
S E
M S M
E S

Proceedings of the

International Congress of Mathematicians

Madrid, August 22–30, 2006

VOLUME I

Plenary Lectures and Ceremonies

Marta Sanz-Solé
Javier Soria
Juan Luis Varona
Joan Verdera

Editors

European Mathematical Society

Editors:

Marta Sanz-Solé
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via 585
08007 Barcelona
Spain

Javier Soria
Departament de Matemàtica Aplicada i Anàlisi
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via 585
08007 Barcelona
Spain

Juan Luis Varona
Departamento de Matemáticas y Computación
Universidad de La Rioja
Edificio J. L. Vives
Calle Luis de Ulloa s/n
26004 Logroño
Spain

Joan Verdera
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra (Barcelona)
Spain

2000 Mathematics Subject Classification: 00Bxx

ISBN 978-3-03719-022-7

Bibliographic information published by Die Deutsche Bibliothek

The Swiss National Library lists this publication in The Swiss Book,
the Swiss national bibliography, and the detailed bibliographic data are
available on the Internet at http://www.helveticat.ch.

Contact address:

European Mathematical Society Publishing House
Seminar for Applied Mathematics
ETH-Zentrum FLI C4
CH-8092 Zürich
Switzerland

Phone: +41 (0)44 632 34 36
Email: info@ems-ph.org
Homepage: www.ems-ph.org

Typeset using the author's TEX files: I. Zimmermann, Freiburg
Printed in Germany

9 8 7 6 5 4 3 2 1

Preface

When we started planning the edition of the Proceedings of the International Congress of Mathematicians 2006 (ICM2006), we considered the possibility of publishing only an electronic version. However, it is pretty difficult to break traditions, particularly for an activity like the ICM with an existence of more than a hundred years. Thus, we finally decided to mimic the model that started in Berlin 98: to publish both, a printed and an electronic version of the Proceedings. However, you may notice the influence of living the Internet Era, where length of files is not really a big issue, by the number of pages, altogether almost 4400, probably a record for the history of ICMs.

These Proceedings consist of three volumes. Volume I is divided into four parts. The first one gathers the speeches at the opening ceremony including the presentation of the Fields Medals, the Rolf Nevanlinna Prize and the newly awarded Gauss Prize for Applications of Mathematics as well as the speeches at the closing ceremony. It also contains information about the organization of the Congress, the committees, sponsors and other collaborators. The second part contains the traditional laudationes for the prizes, that is, an extensive presentation of the work of the awardees. The third part is the main body of the volume and consists of the articles written by the plenary lecturers of the Congress. One of the characteristics of this ICM has been the large number of diverse activities accompanying day by day the program fixed by the IMU Scientific Program Committee. In the fourth part of the volume, you can find articles corresponding to some of them.

Volumes II and III were printed before the Congress and distributed to the participants in Madrid. They gather the articles written by the invited speakers in the different scientific sections of the Congress.

The on-line version of these volumes is accessible at the address http://www.icm2006.org/proceedings

We take this opportunity to express our thanks to the authors of the articles for their effort in the preparation of excellent contributions. We also would like to express our gratitude to the EMS Publishing House for the superb job in the edition of these Proceedings and all the printed material of the ICM2006.

March 2007

Marta Sanz-Solé
Javier Soria
Juan Luis Varona
Joan Verdera

Contents

Special activities

Cultural activities

Past congresses

1897	Zurich	1958	Edinburgh
1900	Paris	1962	Stockholm
1904	Heidelberg	1966	Moscow
1908	Rome	1970	Nice
1912	Cambridge, UK	1974	Vancouver
1920	Strasbourg	1978	Helsinki
1924	Toronto	1982	Warsaw (held in 1983)
1928	Bologna	1986	Berkeley
1932	Zurich	1990	Kyoto
1936	Oslo	1994	Zurich
1950	Cambridge, USA	1998	Berlin
1954	Amsterdam	2002	Beijing

Madrid 2006

Past Fields Medalists and Rolf Nevanlinna Prize Winners

Fields Medalists

1936 Lars V. Ahlfors
Jesse Douglas

1950 Laurent Schwartz
Atle Selberg

1954 Kunihiko Kodaira
Jean-Pierre Serre

1958 Klaus F. Roth
Rene Thom

1962 Lars Hörmander
John W. Milnor

1966 Michael F. Atiyah
Paul J. Cohen
Alexander Grothendieck
Steve Smale

1970 Alan Baker
Heisuke Hironaka
Sergei P. Novikov
John G. Thompson

1974 Enrico Bombieri
David B. Mumford

1978 Pierre R. Deligne
Charles F. Fefferman
Grigorii A. Margulis
Daniel G. Quillen

1982 Alain Connes
William P. Thurston
Shing-Tung Yau

1986 Simon K. Donaldson
Gerd Faltings
Michael H. Freedman

1990 Vladimir G. Drinfeld
Vaughan F. R. Jones
Shigefumi Mori
Edward Witten

1994 Jean Bourgain
Pierre-Louis Lions
Jean-Christophe Yoccoz

1998 Richard E. Borcherds
William T. Gowers
Maxim Kontsevich
Curtis T. McMullen

2002 Laurent Lafforgue
Vladimir Voevodsky

Rolf Nevanlinna Prize Winners

1982 Robert E. Tarjan

1986 Leslie G. Valiant

1990 Alexander A. Razborov

1994 Avi Wigderson

1998 Peter W. Shor

2002 Madhu Sudan

Organization of the Congress

Manuel de León, President of the ICM2006

In 1998, the Real Sociedad Matemática Española, the Societat Catalana de Matemàtiques, the Sociedad Española de Matemática Aplicada and the Sociedad de Estadística e Investigación Operativa got together to reorganize the Spanish Committee of Mathematics (CEMAT) representing Spain at the IMU. This Committee, which includes three other societies (the Federación Española de Sociedades de Profesores de Matemáticas, the Sociedad Española de Investigación en Educación Matemática, and the Sociedad Española de Historia de las Ciencias y de las Técnicas), put forward the Spanish candidacy to host the 25th International Congress of Mathematics in Madrid in 2006, as well as the IMU General Assembly in Santiago de Compostela.

This bid was initially backed by the City of Madrid, the Autonomous Community of Madrid, the Ministry of Education, Culture and Sport, the Ministry of Science and Technology and the Ministry for Foreign Affairs. His Majesty King Juan Carlos I also gave his support to the candidacy with a letter included in the dossier. In addition, backing was forthcoming from the universities in the region (the Universidad Complutense de Madrid, the Universidad Autónoma de Madrid, and the Universidad Carlos III de Madrid) with letters from their respective rectors, as well as from the president of the Consejo Superior de Investigaciones Científicas (CSIC). An association was created to promote the candidacy, which brought together the support of all the above-mentioned bodies and institutions. The candidacy was advocated by the Spanish delegation headed by José Luis Fernández at the 24th General Assembly in Shanghai, and was unanimously approved by vote. The invitation to come to Madrid was formally made on behalf of Spain by Carles Casacuberta at the ICM2002 closing ceremony in Beijing.

The association formed to present the candidacy was dissolved on its return from China, and work began on the organization of the ICM2006 in Madrid and the General Assembly in Santiago. To this end, the ICM2006 Madrid Association was set up, independently of the CEMAT and the societies but in complete co-ordination with all of them. The first president of this association was Carlos Andradas, who was replaced in 2003 by Manuel de León. At the same time, an Organizing Committee responsible for the General Assembly was set up at the Universidad de Santiago. This Committee included the three universities in the region (Santiago de Compostela, La Coruña and Vigo), and was headed by the dean of the Faculty of Mathematics, Juan Manuel Viaño. Both bodies have worked in full co-ordination with each other in recent years.

A further important point is that, although the ICM2006 was to be held in Madrid, the organization of the congress was a joint effort across the whole country. In addition to the General Assembly in Santiago, the Committee was composed of mathematicians from all over Spain, a reflection of the country's historical and cultural wealth and variety. A consultation of the web page will reveal messages of welcome not only in

English, but also Spanish, Catalan, Euskera and Galician; in other words, in all the official languages of the Spanish state.

A major congress with a scope such as that of the ICM also requires strong financial and logistic support from public administration bodies, and as such is subject to political changes. This is precisely what occurred in the city and region of Madrid. The change of government in Spain in 2004 brought about a restructuring of ministries, and with it a corresponding change in our interlocutors, who became the Ministry of Education and Science, the Ministry of Culture, and the Ministry of Foreign Affairs and Cooperation. We are bound to state that the support shown by the previous government for the organization of the ICM was taken up by its successor, both of whom were fully aware of the unique importance of the event.

With regard to financial support, the ICM2006 Executive Committee worked extremely hard to achieve the following goals: 1) To secure the backing for the event from institutions; firstly the Committee of Honour was proud to have His Majesty the King as its president, with representatives of all the public authorities: the Prime Minister, other ministers, the mayor of Madrid, the president of the Regional Government, and the rectors and president of the CSIC; 2) To ensure solid public funding, which came from the Ministry of Education and Science, the Community of Madrid, Madrid City Hall and from the CSIC, and 3) To attract funding from the private sector, which eventually fell short of initial expectations, and which except for organizations such as the Vodafone Foundation, BSCH, the Areces and Enterasys Foundations, as well as Spanish companies and those with their headquarters in Spain, are still a long way from recognizing mathematics as a driving force in research, technological development and innovation. We Spanish mathematicians have also learned that this section on the road to understanding still remains to be covered.

The organization of an ICM requires an important logistical underpinning that cannot be left to voluntary contributions. For that reason we chose a congress agency with great experience in organizing major events, and one with enough flexibility to adapt to our needs. This agency was Unicongress. With their team headed by Paloma Herrero we worked hand in hand as though the ICM2006 were indeed a joint venture, and together we shared the achievements and setbacks which, like all those who have been involved in previous ICMs, we know are part of and parcel of this difficult task. I am happy to say that our choice was the right one, and that the outcome was satisfactory for all concerned. We also believe that for Unicongress, too, this was a new experience, since any ICM amounts to much more than a conventional congress.

The ICM congress logo is something that remains in the mind for years to come. It is not easy to devise a logo that embodies at once the essence of a country and mathematics itself. After many attempts we settled on the one that has since become familiar, and is inspired in the sunflower. One the one hand, the sunflower symbolizes the Spain of sun and light already known to many; on the other, the number of its spirals to right and left are elements of the Fibonacci sequence. The artistic creativity of its devisers led to an image that resembles both a sunflower and the fractal nature of a Romanesco cauliflower. This has given rise to different mathematical interpretations,

and even to different reproductions of the original. The colours of the logo can be fully appreciated on the congress website, where in the logo structure the different themes are associated with the different colours.

The logo formed the basis for one of the official posters designed to promote the ICM2006, together with four others based on well-known pieces of Spanish architecture with a mathematical content. These five posters were sent to mathematical departments the world over and have been very well received internationally.

The target for the ICM2006 budget was 2 500 000 euros, including the attendance fees and specific help from the IMU. The fees could not be set too high, otherwise it would have prevented mathematicians from countries with economic difficulties from attending the congress. Thus following the custom of previous ICMs, it was set at 260 euros, which scarcely covered the expenses generated by each participant in terms of proceedings, coffee, congress bag, materials, etc… As mentioned before, most of the budget was provided by public sources and the fees. On-going work with the General Secretariat of Scientific and Technological Policy enabled us to meet all budget requirements without any final deficit. I would like to mention the outstanding work carried out by the Treasurer, Alberto Ibort, and the vice-Treasurer, Miguel Ángel Rodríguez, thanks to whom the accounts for the ICM2006 remained always on an even keel.

Every ICM is special in some respect, and ours was no exception. The Committee wanted to emphasize three main branches or axes peculiar to the geo-strategic situation of Spain in history and in the world, in particular in relation to Europe.

- The European axis, as a reflection of Spain's position in Europe, symbolized by holding the General Assembly in Santiago de Compostela, the destination of pilgrims along the Road to Santiago, which acted as a channel for culture and science in the Middle Ages.
- The Latin American axis, highlighting the existence of a cultural community by means of which Spain wishes to further its links, including those concerned with mathematics; and
- The Mediterranean axis, with Spain as a bridge between Africa, the Near East and Europe, with the intention of increasing mathematical co-operation in this sphere.

The venue for the congress deserves a section on its own. For a congress such as the ICM, eminently scientific in character, but also with its relevance in social and media terms, with the presentation of the most prestigious prizes awarded in mathematics, an appropriate venue is a crucial factor. The Palacio Municipal de Congresos (PMC) in Madrid is a striking building designed by Ricardo Bofill, one of the most highly recognized Spanish architects on the international scene. This majestic building, equipped with all the latest modern technology, provided everything we could have wished for. But this did not come cheaply, and in fact accounted for a considerable part of the budget. However, thanks to our collaboration with the Convention Bureau

of Madrid, Madrid City Hall, and those in charge at the PMC itself, we were able to secure the building as the venue for the congress. In retrospect, I believe our decision to have been the correct one, and it is true to say that the ICM2006 would not have been the same without these premises.

The opening ceremony is another vital part of any ICM. For several months, we debated with the IMU Executive Committee, and in particular with its president, Sir John Ball, about how the ceremony would be structured. The presence of His Majesty the King at this opening ceremony on August 22nd was decisive for attaining the impact desired, and we are grateful for the extraordinary co-operation extended by the Royal Household from the very beginning. In spite of difficulties with the agenda, to say nothing of the security measures required, everything was in place on time for the event. Not only is financial support from public institutions necessary for a congress of this nature, but also the physical presence of their representatives. In this case, we the organizers would like to express our thanks to the Royal Household, to Madrid City Hall, to the Community of Madrid and the Ministry of Education and Science for all their support in both these respects. The opening ceremony was divided into two parts; the first part consisted of a video produced by the organizers showing the relation of mathematics with art and culture through the ICM2006 official posters. There was also a musical performance by the Ara Malikian Trio that enjoyed great success. The second part consisted of the official speeches and the presentation of the prizes by His Majesty the King. We believe this was an emotive and attractive event befitting the importance of the awards and the prize-winners themselves. Finally, His Majesty the King delivered a speech pointing out the vital role played by mathematics in education, knowledge and development. After his address, the King declared the Madrid ICM2006 officially open. His Majesty also attended the cocktail reception held after the opening ceremony, and delighted everyone with his cordiality and friendly approachability.

After the opening ceremony, the congress unfolded according to plan. The quality of the lectures was a concern of both the Programme Committee and the Local Programme Committee, not only for their content, which was beyond all doubt, but also for the presentations. Noga Alon's work on behalf of the PC, and Marta Sanz-Solé's on behalf of the LPC, were both admirable, and I am sure I am not mistaken when I say that the ICM2006 fully emulated previous ICMs in this respect. There is no doubt that the technological facilities at the Palacio Municipal de Congresos did much to ensure the quality of both invited talks and plenary lectures.

The scientific programme consisted of 20 plenary lectures and 169 invited talks distributed over 20 sections, the same amount as at the ICM2002. With regard to the open programme, the presentation of posters was encouraged by a competition with prizes for the best entries, a measure whose purpose was to make the programme more agreeable and digestible.

Steps are taken at every ICM to encourage the participation of mathematicians from the more disadvantaged countries. Indeed, co-operation in development is a priority of the IMU, as explicitly stated in the resolutions approved at the 25th General

Assembly. On this occasion, the IMU and the ICM2006 established the following five categories for financial support:

1. Young mathematicians from developing and economically disadvantaged countries.
2. Senior mathematicians from developing and economically disadvantaged countries.
3. Senior mathematicians from Latin America.
4. Senior mathematicians from Mediterranean developing countries.
5. Young Spanish mathematicians.

The IMU subsidized the travel expenses of 143 mathematicians selected for Programmes 1 and 2: 80 on Programme 1 and a further 63 on Programme 2, while the Local Organizing Committee covered the registration fee, board and lodging in Madrid for 131 of these 143 participants.

In accordance with the three axes previously described, the ICM2006 Organizing Committee also managed to include Programmes 3, 4 and 5, covering the registration fee, board and lodging in Madrid for 178 mathematicians (Programme 3: 76; Programme 4: 70; Programme 5: 32) and 43 airline tickets (Programme 3: 25; Programme 4: 18). These five programmes were co-ordinated by C. Herbert Clemens, Linda Geraci and Sharon Laurenti (IMU), and also by Marisa Fernández (ICM2006). This task was possible thanks to their efforts and dedication.

The specific funding was provided by the IMU Special Development Fund, the Spanish Agency for International Cooperation (Ministry of Foreign Affairs and Cooperation), the Departments of Mathematics and Deans of the Faculties of Mathematics of the Spanish Universities, and the Carolina Foundation, as well as by a large number of Spanish and non-Spanish mathematical societies.

As regards co-operation, one of the activities undertaken prior to the ICM2006 was the "Mathematics for Peace and Development" School. During the week July 17th-23rd, young mathematicians from Arab countries (including Palestine), Latin America, Europe and Israel attended eight courses given at the Universidad de Córdoba by prestigious mathematicians from different countries. The aim of the School was to draw attention to mathematics as an effective means of contributing to the progress of peoples, as well as its use as a universal language for mutual understanding among different cultures. The choice of Córdoba as the venue was the role of this city as a symbol of the "Spain of the Three Cultures", where Christians, Jews and Muslims lived side by side in an example of tolerance and co-operation.

The Madrid ICM2006 was also complemented by 64 satellite conferences – a record. 36 of them were held in Spain and constituted a demonstration of the organizational powers of Spanish mathematicians and their many international relations. There was no specialized branch of mathematics that was not addressed in any of the satellite conferences. Although at times these satellite conferences can draw

attendance away from the ICM itself, in this case the number and quality of such conferences more than made up for any shortfall and proved to be an excellent scientific accompaniment.

Cultural and dissemination activities were other facets of the ICM that were accorded fundamental importance. In consequence, an ambitious programme was drawn up to cover two fronts: on the one hand, society in general, and on the other the congress participants. Our aim was to draw attention to the role played by mathematics throughout the length and breadth of geography and history and in the culture of humankind, as well as showing how mathematics is an essential part of life. Judging by the results, and by the reactions to these cultural activities, which were praised in King Juan Carlos' opening speech and in the closing speech by the IMU president, they were one of the outstanding successes of the congress. The responsibility for this task fell to a team led by Antonio J. Durán, in collaboration with Raúl Ibáñez, Guillermo Curbera and Antonio Pérez-Sanz.

In relation with the ICM2006 in particular, and in the effort to bring mathematics closer to society at large, the exhibition "The Life of Numbers" was expressly prepared for the occasion, and was organized and financed by the Ministry of Culture and the Spanish National Library. The exhibition was held in Madrid at the Spanish National Library from June 7th to September 10th, and provided an account of the relation of human beings with numbers from the first marks left by human hands in Palaeolithic cave paintings to the Renaissance, a journey through Mesopotamia, Egypt, Greece, Mesoamerica, Rome, India and the Middle Ages. On display at the exhibition were Babylonian tablets, Roman coins, pre-Roman and Mayan manuscripts, an impressive collection of Renaissance mercantile arithmetics, engravings by Leonardo da Vinci and Durer, maps of the Earth and the Stars, all the exhibits coming from different Spanish institutions: the Museum of America and the National Archaeological Museum, the Library of the Monasterio de El Escorial, the Capitular & Colombina Library in Sevilla, the Universidad Complutense de Madrid Library, from Catalonia, and of course from the Spanish National Library itself. The pièce de résistance was the Codex Vigilanus, a manuscript composed in 976 at the Monasterio de San Martín de Albelda (La Rioja), currently conserved at the Monasterio de El Escorial. This manuscript is the oldest written record of its kind in history and includes the Hindu-Arabic numerals which are still the basis of our numbers today. A beautifully illustrated edition of the book "The Life of Numbers" was published for the exhibition with texts by Alberto Manguel, Georges Ifrah and Antonio J. Durán (who was also the curator of the exhibition).

Also with the general public in mind, three exhibitions were organized at the Centro Cultural Conde Duque in Madrid, financed by the Ministry of Education and Science and the Spanish Foundation for Science and Technology. Firstly, the already well-known "Experiencing Mathematics", an exhibition originating at the French Centre des Sciences in Orleáns and sponsored by UNESCO. This exhibition was presented under the Spanish title of "¿Por qué las Matemáticas?" ("Why Mathematics?") and was open at the Conde Duque Cultural Centre from August 17th to

October 20th (the curators being Raúl Ibáñez and Antonio Pérez Sanz). The second exhibition, organized expressly for the occasion, concerned fractal art and went under the title of "Fractal art: Beauty and Mathematics". On display were works by the twenty-eight finalists in an international competition expressly organized for the ICM2006 in Madrid, with a jury of panellists headed by Benoit Mandelbrot. Professor Mandelbrot gave a talk on "The Nature of Roughness in Mathematics, Science, and Art" at the main congress venue, where a replicated version of this exhibition could also be seen. Highly visual catalogues were published for both exhibitions (the first included a notebook of activities for students). The third exhibition was "Demoscene: Mathematics in Movement", held in parallel at the Centro Cultural Conde Duque and the congress venue, and consisted of a selection of computer-aided animated films with live commentary by some of their creators. Desmocene is a powerful source of mathematical algorithms for the creation of graphic and visual effects, whose special digital effects are currently used in feature films and video games.

The success of all these exhibitions, whose purpose was to stimulate interest about mathematics in society at large, together with the celebration of the ICM2006 in itself, can be measured by their repercussion in the media and by the large number of people who came to visit them, to the extent that they frequently had to queue to enter. Those in charge at the Spanish National Library and the Centro Cultural Conde Duque were frankly surprised by the number of visitors, given the subject-matter of the respective exhibitions.

The ICM2006 Executive Committee also mounted an extensive programme of activities for the Congress participants themselves.

The most ambitious of these events was the exhibition entitled "The ICM through History", based on the history of the 25 ICMs held to date, from the first held in Zurich in 1897 to the Madrid congress in 2006. The aim of the exhibition was to provide a visual chronicle of all the ICMs, emphasizing their significance in terms of human endeavour and using the activities of mathematicians at the ICMs as a mirror in which history, culture, technology, fashion and changing attitudes were reflected. Some 500 written and photographic documents provided a twin portrait of the ICMs; on the one hand, a chronological review of the history of the ICM, and on the other a transversal view through the social life of the congresses, the graphic design for the congresses and the buildings where they have been held. The physical and conceptual heart of the exhibition resided in the display of medals, original reproductions of the Fields, Nevanlinna and Gauss awards provided by the Royal Canadian Mint, the University of Helsinki and the Deutsche Mathematiker-Vereinigung. Guillermo Curbera, the curator of the exhibition, was helped in his task by many universities, libraries, archives, museums, mathematical societies and individuals, enabling him to assemble an extraordinary collection of photographs and documents, many of them never available to the public before. The exhibition was entirely financed by the ICM2006 Executive Committee and has remained as an asset of the Spanish mathematical societies.

Another cultural activity that aroused much public and media attention was the Japanese sculptor Keizo Ushio's live sculpting of a square block of black granite weighing various tonnes. From this he fashioned a torus which he split into two curved sections to form a sculpture resembling the symbol for infinity. Ushio began work in early August on the campus of the Consejo Superior de Investigaciones Científicas, from where he moved to the Congress venue on August 22nd. It was there he completed the work in full view of congress participants and passers-by, producing a sculpture that has attracted much attention, especially in Spain and Japan.

This programme of activities was complemented by others which, although not organized directly by the Committee, were included in the general programme. One of the most noteworthy was the exhibition based on classical mathematical texts under the title of the "History of Mathematical Knowledge", which was held at the "Marqués de Valdecilla" Historical Library of the Universidad Complutense de Madrid between June 28th and October 27th (with Ricardo Moreno as curator). Another was the replicated version of the exhibition organized by the University of Vienna, with Karl Sigmund and John Dawson as curators. This exhibition commemorated the centenary of Kurt Gödel and took place at the Botanical Garden of the Universidad Complutense de Madrid from August 22nd to September 8th (with Capi Corrales Rodrigáñez as local co-ordinator). Further exhibitions were: "Singularities", mounted at the Congress venue by professor Herwig Hauser (including a film show); a tribute to the musician Francisco Guerrero (including a concert held at the venue), and the mathematical visit to the Monasterio de El Escorial and its library (tickets for this event were sold out six months before the Congress began).

Pride of place among the cultural events was the official gift presented to all plenary lecturers and invited speakers by the Executive Committee in recognition for their contribution to the Congress. This consisted of a facsimile edition of the works of Archimedes, "On the Sphere and the Cylinder", "On the Measurement of the Circle" and "The Quadrature of the Parabola" (published jointly with the Real Sociedad Matemática Española), in an annotated Spanish translation. This is a luxury edition comprising two volumes presented in a box-set (333×230 mm). The first volume is a facsimile book of a 16th century manuscript from the Library of El Monasterio de El Escorial, a manuscript copied in Venice at the expense of Diego Hurtado de Mendoza (Charles V's ambassador at Venice from 1527 to 1547) from the manuscript CCCV extant in the Marciana Library. The second volume contains the annotated Spanish translation of those Archimedean works, and the following four studies: (1) *Greek Science: Towards a Critical Knowledge* by Carlos García Gual; (2) *Archimedes and His Manuscripts* by Antonio J. Durán (who was also in charge of co-ordination of the edition); (3) *Archimedes: A Legend of Wisdom*, and (4) *The Mathematical Works of Archimedes*, both by Pedro M. González Urbaneja.

Many other special activities were organized, a list of which would be too long to include in this introduction, although we may mention the scientific part of the Emmy Noether Talk, given by Ivonne Choquet-Bruhat, the special talk on Poincaré's Conjecture by John Morgan, and the talk given by Benoit Mandelbrot. A joint scien-

tific activity organized by the London Mathematical Society and the Real Sociedad Matemática Española was also held.

Several round table discussions were also held, among which were those organized by the European Mathematical Society on August 23rd, "Should Mathematicians Care about Communicating to Broad Audiences? Theory and Practice", chaired by Jean Pierre Bourguignon and with the participation of Björn Engquist, Marcus du Sautoy, Alexei Sossinsky, François Tisseyre and Philippe Tondeur, and the ICM2006 Closing Round Table on August 29th, "Are Pure and Applied Mathematics Drifting Apart?", chaired by John Ball and with the participation of Lennart Carleson, Ronald Coifman, Yuri Manin, Helmut Neunzert and Peter Sarnak.

One of the most long-standing traditions in the history of the ICM is the edition of a special commemorative stamp. On this occasion, the design for the stamp included the congress logo and the first known written record of the Hindu-Arabic numbers from the Codex Vigilanus, published in Spain in the 10th century, which is currently conserved at the Library of the Monasterio de El Escorial on the outskirts of Madrid.

The volunteers are a collective who deserve a special mention. We also wanted this group to be composed of representatives from all over Spain, and indeed volunteers came forward from all the Spanish universities. Some 700 pre-graduate and pre-doctoral grant students responded to our call, from which a total of 350 were selected. These volunteers worked hard and enjoyed the experience to such an extent that they were sad to see the ICM2006 come to a close, which in itself stands as a testimony to the success of their efforts. We on the Organizing Committee are indebted to all of them. They worked tirelessly for long hours without complaint, and I hope that many of them will be able to participate in the ICM2010 as fully-fledged mathematicians.

Every ICM at its conclusion is obliged to present statistics providing an account in numbers of all that took place. The final figure of participants reached 3,600, with 400 accompanying persons. The number of countries from which participants came set an all-time record of 108. The number of exhibitors rose to 45. In the scientific part of the congress there were 20 plenary lectures, 169 invited talks and some 1,000 short communications and posters.

There is no doubt that the most outstanding feature of this congress was the extraordinary attention it received from the media. In this regard, some have attributed this interest to the conspicuous absence of Grigory Perelman and his refusal to receive the Fields Medal, but it must be said that one year before the start of the congress the Organizing Committee set up a press office with the "Divulga" agency. Over the 20 weeks immediately prior to August 22nd, a weekly news bulletin providing information about the contents of the coming ICM was published. At the same time, the ICM public presentations and the most important parallel activities were programmed. Our press team headed by Ignacio F. Bayo and Mónica Salomone also collaborated with the IMU Executive Committee at an international level. Indeed, we sent letters to the leading communications media in Spain and abroad inviting their representatives to the opening ceremony. The combination of all these circumstances made the event a media success. For ten days during the summer in Spain the ICM2006 was headline

news, and international repercussion was likewise unprecedented. The lesson to be learned from this is that we mathematicians must work hand in hand with journalists and the media if we wish to emerge from the information ghetto.

Press work culminated in the publication of 7 issues of the "Daily News", often produced against the clock and in spite of permanent pressure on the press office arising from the continuous avalanche of requests for information from the media and its representatives. In addition, press conferences were organized on a daily basis, which sometimes attracted audiences hitherto unconceivable in the world of mathematics.

With regard to diffusion, it is also necessary to mention the series of programmes produced by the UNED Educational Television and provided for the Organizing Committee. These programmes constitute documents of great educational value.

The Closing Ceremony was held on August 30th and featured the expressions of gratitude and acknowledgement from the IMU president to the different committees, my own to the committees who worked on the organization in Spain, the address by the elected president of the IMU, László Lovász, and the invitation from the Indian representative, Rajat Tandon, to attend the ICM2010 to be held in his country, in the city of Hyderabad.

After every ICM there still remains work to be done. In addition to the thick Volumes II and III forming part of the Proceedings, there is the first that the reader now holds in his or her hands. The Publishing House of the European Mathematical Society was charged with the publication of these proceedings, and the result has certainly been impressive. This first volume is accompanied by a DVD with recordings of the opening and closing ceremonies, as well as all the plenary lectures. We believe that it provides an excellent complement to the text and an unforgettable record for all those who shared with us those wonderful ten days in Madrid in August 2006.

This ICM2006 will have a long-lasting effect on Spanish mathematics. It has been a collective effort that has brought us closer together and made us aware of belonging to a national and international community. On a domestic level, it has also led to a self-examination that has given rise to initiatives that are already under way to improve research in the discipline. Furthermore, it has brought mathematics more to the social forefront to an extent never before witnessed in Spain. This is a situation that we must make the most of in the years to come. Moreover, the eyes of the international mathematical collective were fixed on Spain this summer, a fact that will undoubtedly further greater collaboration.

We hope to have fulfilled all the expectations placed in us by the IMU, and leave the mathematical doors of our country open to the future.

The committees of the Congress

Organizing committees

Honorary Committee

President

His Majesty, The King of Spain

Members

The Prime Minister of Spain
The President of the Community of Madrid
The Minister of Education and Science
The Minister of Culture
The Minister of Foreign Affairs
The Minister of Industry, Tourism and Trade
The Mayor of the City of Madrid
The Rector of the Universidad Complutense de Madrid
The Rector of the Universidad Autónoma de Madrid
The Rector of the Universidad Politécnica de Madrid
The Rector of the Universidad de Alcalá de Henares
The Rector of the Universidad Carlos III de Madrid
The Rector of the Universidad Rey Juan Carlos
The Rector of the Universidad Nacional de Educación a Distancia
The President of the Consejo Superior de Investigaciones Científicas

Executive Committee

President

Manuel de León, Instituto de Matemáticas y Física Fundamental, CSIC, Madrid

Vice President General

Carlos Andradas, Universidad Complutense de Madrid

Vice Presidents

Carles Casacuberta, Universitat de Barcelona
Eduardo Casas, Universidad de Cantabria, Santander
Pedro Gil Álvarez, Universidad de Oviedo

Secretary General

José Luis González-Llavona, Universidad Complutense de Madrid

Treasurer

Alberto Ibort Latre, Universidad Carlos III de Madrid

Cultural Activities

Antonio J. Durán, Universidad de Sevilla

Fund Raising & Sponsorship
Emilio Bujalance, Universidad Nacional de Educación a Distancia, Madrid
María Luisa Fernández, Euskal Herriko Unibertsitatea, Bilbao

Infrastructure and Logistics
Emilio Bujalance, Universidad Nacional de Educación a Distancia, Madrid

Local Program Committee
Marta Sanz-Solé, Universitat de Barcelona

Parallel Scientific Activities
Fernando Soria, Universidad Autónoma de Madrid

Publications
Joan Verdera, Universitat Autònoma de Barcelona

Relations with Latin America, Eastern Europe and Developing Countries
María Luisa Fernández, Euskal Herriko Unibertsitatea, Bilbao

Social Activities
Rosa Echevarría, Universidad de Sevilla

Vice Treasurer
Miguel Ángel Rodríguez, Universidad Complutense de Madrid

Web and Electronic Communications
Pablo Pedregal, Universidad de Castilla-La Mancha, Ciudad Real

Cultural Activities

Chair
Antonio J. Durán, Universidad de Sevilla

Members
Antonio F. Costa, Universidad Nacional de Educación a Distancia, Madrid
Guillermo P. Curbera, Universidad de Sevilla
Raúl Ibáñez, Euskal Herriko Unibertsitatea, Bilbao

Infrastructure and Logistics

Chair
Emilio Bujalance, Universidad Nacional de Educación a Distancia, Madrid

Members
Roberto Canogar McKenzie, Universidad Nacional de Educación a Distancia, Madrid
Francisco Javier Cirre Torres, Universidad Nacional de Educación a Distancia, Madrid
Miguel Delgado Pineda, Universidad Nacional de Educación a Distancia, Madrid
M. José Muñoz Bouzo, Universidad Nacional de Educación a Distancia, Madrid
Ana M. Porto F. Silva, Universidad Nacional de Educación a Distancia, Madrid

Local Program Committee

Chair
Marta Sanz-Solé, Universitat de Barcelona

Members
Jesús Bastero, Universidad de Zaragoza
José A. Carrillo, ICREA and Universitat Autònoma de Barcelona
Wenceslao González-Manteiga, Universidade de Santiago de Compostela
Consuelo Martínez, Universidad de Oviedo
Marcel Nicolau, Universitat Autònoma de Barcelona
Tomás Recio, Universidad de Cantabria, Santander
J. Rafael Sendra, Universidad de Alcalá de Henares
Juan M. Viaño, Universidade de Santiago de Compostela

Parallel Scientific Activities

Chair
Fernando Soria, Universidad Autónoma de Madrid

Members
Manuel Barros, Universidad de Granada
Miguel Escobedo, Euskal Herriko Unibertsitatea, Bilbao
Ignacio García Jurado, Universidade de Santiago de Compostela
Luis Narváez Macarro, Universidad de Sevilla

Publications

Editors of the Proceedings
Marta Sanz-Solé, Universitat de Barcelona
Javier Soria, Universitat de Barcelona
Juan Luis Varona, Universidad de La Rioja
Joan Verdera, Universitat Autònoma de Barcelona

The Madrid Intelligencer
Fernando Chamizo, Universidad Autónoma de Madrid
Adolfo Quirós, Universidad Autónoma de Madrid

Relations with Latin America, Eastern Europe and Developing Countries

Chair
María Luisa Fernández, Euskal Herriko Unibertsitatea, Bilbao

Members
Antonio Cuevas, Universidad Autónoma de Madrid
Eugenio Hernández, Universidad Autónoma de Madrid
Ignacio Luengo, Universidad Complutense de Madrid

Marta Macho, Euskal Herriko Unibertsitatea, Bilbao
Raquel Mallavibarrena, Universidad Complutense de Madrid
José Leandro de María, Universidad Nacional de Educación a Distancia, Madrid
Ernesto Martínez, Universidad Nacional de Educación a Distancia, Madrid
Vicente Muñoz, Instituto de Matemáticas y Física Fundamental, CSIC, Madrid
Domingo Pestaña, Universidad Carlos III de Madrid
José Manuel Rodríguez, Universidad Carlos III de Madrid

Web and Electronic Communications

Chair
Pablo Pedregal, Universidad de Castilla-La Mancha, Ciudad Real

Member
Ernesto Aranda Ortega, Universidad de Castilla-La Mancha, Ciudad Real

IMU committees

Program Committee

Chair
Noga Alon, Tel Aviv University, Israel

Members
Douglas N. Arnold, University of Minnesota, USA
Joaquim Bruna, Universitat Autònoma de Barcelona, Spain
Kenji Fukaya, Kyoto University, Japan
Nigel Hitchin, University of Oxford, UK
Vaughan Jones, University of California, Berkeley, USA
Pierre-Louis Lions, Collège de France, France
Gregory Margulis, Yale University, USA
Richard Taylor, Harvard University, USA
S. R. Srinivasa Varadhan, Courant Institute of Mathematical Sciences, USA
Claire Voisin, Institut de Mathématiques de Jussieu, France
Enrique Zuazua, Universidad Autónoma de Madrid, Spain

Panels for the program of ICM 2006

1. Logic and Foundations

Chair. Angus MacIntyre, University of London, UK.

Core Members. Saharon Shelah, Hebrew University, Israel; Hugh Woodin, University of California, Berkeley, USA.

Other Members. Gregory Cherlin, Rutgers University, USA; Alexander Kechris, California Institute of Technology, USA; Richard Shore, Cornell University, USA; Stevo Todorcevic, University of Toronto, Canada and C.N.R.S., France.

2. Algebra

Chair. Alexander Lubotzky, Hebrew University, Israel.

Core Members. Robert Griess, University of Michigan, USA; Vladimir Voevodsky, Institute for Advanced Study, USA.

Other Members. William M. Kantor, University of Oregon, USA; Consuelo Martínez López, Universidad de Oviedo, Spain; Dimitry Orlov, Steklov Mathematical Institute, Russia; Idun Reiten, Norwegian University of Science and Technology, Norway.

3. Number Theory

Chair. Hendrik Lenstra, Universiteit Leiden, The Netherlands.

Core Members. Gerd Faltings, Max-Planck-Institut für Mathematik, Germany; Henryk Iwaniec, Rutgers University, USA; Kazuya Kato, Kyoto University, Japan.

Other Members. Haruzo Hida, University of California, Los Angeles, USA; Shou-Wu Zhang, Columbia University, USA.

4. Algebraic and Complex Geometry

Chair. Miles Reid, University of Warwick, UK.

Core Members. Ngaiming Mok, University of Hong Kong, People's Republic of China; Shigeru Mukai, Kyoto University, Japan.

Other Members. Spencer Bloch, University of Chicago, USA; Fedor Bogomolov, New York University, USA; Rahul Pandharipande, Princeton University, USA; Eckart Viehweg, Universität Duisburg-Essen, Germany.

5. Geometry

Chair. Gang Tian, Princeton University, USA.

Core Members. Frances Kirwan, University of Oxford, UK; François Labourie, Université de Paris-Sud 11, France; Hiraku Nakajima, Kyoto University, Japan; Leonid Polterovich, Tel Aviv University, Israel.

Other Members. Robert Bryant, Duke University, USA; Richard Schoen, Stanford University, USA.

6. Topology

Chair. Andrew Casson, Yale University, USA.

Core Member. Stephan Stolz, University of Notre Dame, USA.

Other Members. Mladen Bestvina, University of Utah, USA; Michael Hopkins, Massachusetts Institute of Technology, USA; Tomotada Ohtsuki, Kyoto University, Japan; Ronald Stern, University of California, Irvine, USA.

7. Lie Groups and Lie Algebras

Chair. Joseph Bernstein, Tel Aviv University, Israel.

Core Members. Marc Burger, ETH Zürich, Switzerland; Alexander Eskin, University of Chicago, USA; Jean-Loup Waldspurger, Institut de Mathématiques de Jussieu, CNRS, France.

Other Members. Pavel Etingof, Massachusetts Institute of Technology, USA; Stephen Kudla, University of Maryland, USA; George Lusztig, Massachusetts Institute of Technology, USA.

8. Analysis

Chair. Pertti Mattila, University of Helsinki, Finland.

Core Members. Boris Kashin, Steklov Institute of Mathematics, Russia; Terence Tao, University of California, Los Angeles, USA.

Other Members. Guy David, Université Paris-Sud 11, France; Ronald De Vore, University of South Carolina, USA; Hans Martin Reimann, Universität Bern, Switzerland; Yum-Tong Siu, Harvard University, USA.

9. Operator Algebras and Functional Analysis

Chair. Gilles Pisier, Texas A&M University, USA.

Core Members. Joachim Cuntz, Universität Münster, Germany; Sorin Popa, University of California, Los Angeles, USA; Nicole Tomczak-Jaegermann, University of Alberta, Canada.

Other Members. Uffe Haagerup, University of Southern Denmark. Denmark.

10. Ordinary Differential Equations and Dynamical Systems

Chair. Yakov Sinai, Princeton University, USA.

Core Members. John Guckenheimer, Cornell University, USA; Shahar Mozes, Hebrew University, Israel; Jean-Christophe Yoccoz, Collège de France, France; Lai-Sang Young, New York University, USA.

Other Members. Giovanni Forni, University of Toronto, Canada; Yulij Ilyashenko, Cornell University, USA; Steklov Mathematical Institute, Russia.

11. Partial Differential Equations

Chair. Gilles Lebeau, Université de Nice Sophia Antipolis, France.

Core Members. Luis Caffarelli, University of Texas, USA; Sun-Yung Alice Chang, Princeton University, USA; Lawrence Craig Evans, University of California, Berkeley, USA; Stefan Müller, Max-Planck-Institut für Mathematik, Germany.

Other Members. Alberto Bressan, Penn State University, USA; Yoshikazu Giga, Hokkaido University, Japan; Benoît Perthame, École Normale Supérieure, France.

12. Mathematical Physics

Chair. Jürg Fröhlich, ETH Zürich, Switzerland.

Core Members. Igor Krichever, Columbia University, USA; Gregory Moore, Rutgers University, USA.

Other Members. Eugene Bogomolny, Université Paris-Sud 11, France; Giovanni Felder, ETH Zürich, Switzerland; Krzysztof Gawedzki, Institut de Physique Théorique, ENS-Lyon, France; Sergiu Klainerman, Princeton University, USA; Israel Michael Sigal, University of Toronto, Canada.

13. Probability and Statistics

Chair. David Nualart, University of Kansas, Lawrence, USA.

Core Members. Terry Lyons, University of Oxford, UK; Terence Speed, University of California, Berkeley, USA.

Other Members. Peter Hall, Australian National University, Canberra, Australia; Shigeo Kusuoka, University of Tokyo, Japan; Michel Ledoux, Université Paul-Sabatier, Toulouse III, France; David Siegmund, Stanford University, USA; Ofer Zeitouni, University of Minnesota, USA.

14. Combinatorics

Chair. Gil Kalai, Hebrew University, Israel.

Core Members. Jirí Matousek, Charles University, Czech Republic; Richard Stanley, Massachusetts Institute of Technology, USA; Günter Ziegler, Technische Universität Berlin, Germany.

Other Members. Peter Cameron, Queen Mary University of London, UK; Andrew Odlyzko, University of Minnesota, USA; Alexander Schrijver, CWI, The Netherlands; Joel Spencer, New York University, USA.

15. Mathematical Aspects of Computer Science

Chair. Shafí Goldwasser, Massachusetts Institute of Technology, USA.

Core Members. Johan Hastad, KTH, Sweden; Richard Karp, University of California, Berkeley, USA; Emo Welzl, ETH Zürich, Switzerland.

Other Members. Michael Kearns, University of Pennsylvania, USA; Peter Shor, Massachusetts Institute of Technology, USA; Éva Tardos, Cornell University, USA.

16. Numerical Analysis and Scientific Computing

Chair. Alfio Quarteroni, EPFL, Switzerland.

Core Members. Wolfgang Dahmen, RWTH Aachen University, Germany; Leslie Greengard, New York University, USA; Eitan Tadmor, University of Maryland, USA.

Other Members. Albert Cohen, Université Pierre et Marie Curie, France; Lisa Fauci, Tulane University, USA; Tang Tao, Hong Kong Baptist University, People's Republic of China.

17. Control Theory and Optimization

Chair. Jean-Pierre Puel, Université de Versailles, France.

Core Members. William Cook, Georgia Institute of Technology, USA; Jorge Nocedal, Northwestern University, USA; Eduardo Sontag, Rutgers University, USA.

Other Members. Ruth F. Curtain, University of Groningen, The Netherlands; Petar V. Kokotovic, University of California, Santa Barbara, USA; Steven I. Marcus, University of Maryland, USA.

18. Applications of Mathematics in the Sciences

Chair. Olivier Pironneau, Université Pierre et Marie Curie, France.

Core Members. Ronald Coifman, Yale University, USA; Karl Sigmund, University of Vienna, Austria.

Other Members. Jennifer Chayes, University of Washington, USA; David McLaughlin, New York University, USA; George C. Papanicolau, Stanford University, USA; Rolf Rannacher, Institut für Angewandte Mathematik, Germany; Endre Süli, University of Oxford, UK; Masahisa Tabata, Kyushu University, Japan.

19. Mathematics Education and Popularization of Mathematics

Chair. Wilfried Schmid, Harvard University, USA.

Core Member. Jill Adler, University of Witwatersrand, South Africa.

Other Members. Dan Amir, Tel Aviv University, Israel; Deborah Ball, University of Michigan, USA; Garth Gaudry, University of Melbourne, Australia; Frederick Leung, University of Hong Kong, People's Republic of China.

20. History of Mathematics

Chair. Karen Parshall, University of Virginia, USA.

Other Members. Craig Fraser, University of Toronto, Canada; Jeremy G. Gray, Open University, UK; Jan P. Hogendijk, University of Utrecht, The Netherlands; Michio Yano, Kyoto Sangyo University, Japan.

Fields Medal Committee for 2006

Chair

John Ball, University of Oxford, UK

Members

Enrico Arbarello, Università di Roma La Sapienza, Italia
Jeff Cheeger, Courant Institute of Mathematical Sciences, USA
Donald Dawson, Carleton University, Canada
Gerhard Huisken, Max Planck Institute for Gravitational Physics, Germany
Curtis T. McMullen, Harvard University, USA
Aleksei N. Parshin, Steklov Mathematical Institute, Russia
Tom Spencer, Institute for Advanced Study, USA
Michèle Vergne, École Polytechnique, France

Rolf Nevanlinna Prize Committee for 2006

Chair

Margaret Wright, Courant Institute of Mathematical Sciences, USA

Members

Samson Abramsky, University of Oxford, UK
Franco Brezzi, Istituto di Matematica Applicata e Tecnologie Informatiche, Italy
Gert-Martin Greuel, University of Kaiserslautern, Germany
Johan Håstad, KTH Stockholm, Sweden

Carl Friedrich Gauss Prize Committee for 2006

Chair

Martin Grötschel, Konrad-Zuse-Zentrum für Informationstechnik, Germany

Members

Robert E. Bixby, Rice University, USA
Frank den Hollander, Eindhoven University of Technology, The Netherlands
Stéphane Mallat, École Polytechnique, France
Ian Sloan, The University of New South Wales, Australia

Emmy Noether Lecture Committee for 2006

Chair

Ragni Piene, Oslo University, Norway

Members

Christopher Deninger, Westfälische Wilhelms-Universität, Germany
Hesheng Hu, Fudan University, China
Cathleen Morawetz, Courant Institute of Mathematical Sciences, USA
María Eulalia Vares, CBPF, Brazil

Travel Grants Committee

Chair

John Ball, University of Oxford, United Kingdom

Members

Hajer Bahouri, Université de Tunis, Tunisia
Zhiming Ma, Chinese Academy of Science, Beijing, China
Madabusi S. Raghunathan, Tata Institute, India
Michael Tsfasman, Russian Academy of Sciences, Moscow, Russia
Marcelo Viana, IMPA, Brazil

Authorities and members of the IMU Executive Committee and the organizing committees

Other collaborators of the ICM2006

e-program
Maria Julià, Rafael Serra Fuster (Agilgroup).

ICM2006 Madrid Official Suppliers
Audiovisual equipment: AV Medios
Building of exhibition and poster boards: DIP Proyectos
Catering: MONICO Gourmet
Catering at the ICM2006 party: Mariano e Isabel
WiFi: Enterasys

Press office
Clemente Alvárez, Sherezade Álvarez, Álvaro Antón Sancho. Ignacio F. Bayo, Pablo Francescutti, Mario García, Pilar Gil, Lula Gómez, Abelardo Hernández, Concha Muro, Jeff Palmer, Roberto Rubio, Mónica Salomone (Director), Laura Sánchez.

Secretariat
Teresa López Rodríguez, Itziar Prats Fernández, Magaly Roldán Plumey.

Technical secretariat

Rocío Aranda, Mireya Arnoso, José Casero, Ana Belén Córdoba, Belén Gómez Aróstegui, Irene Gutiérrez, Paloma Herrero (Director), Antonio Ortiz, Silvia Recio, Carine Sainte-Rose, Celia Teves, Jordi Traveset.

List of sponsors

The ICM 2006 is held under the auspices of the *International Mathematical Union* and the sponsorship of the following public and academic bodies and private companies and foundations.

Public bodies

Ministerio de Educación y Ciencia
Ministerio de Asuntos Exteriores y de Cooperación
    Agencia Española de Cooperación Internacional
Ministerio de Cultura
    Biblioteca Nacional
    Dirección General de Comunicación y Cooperación Cultural
    Sociedad Estatal de Conmemoraciones Culturales
Comunidad de Madrid
    Consejería de Educación
    Instituto Madrileño de Desarrollo
  Ayuntamiento de Madrid
      Madrid-Convention Bureau
      Concejalía de las Artes
      Centro Cultural Conde Duque
  Consejo Superior de Investigaciones Científicas
  Correos
  Fundación Carolina
  Fundación Española para la Ciencia y la Tecnología

Academic bodies

Universidad Autónoma de Madrid
Universitat de Barcelona
Universitat Autònoma de Barcelona
Universidad de Castilla-La Mancha
Universidad Complutense de Madrid
Universidad Nacional de Educación a Distancia
Universidad de Sevilla

Association for Women in Mathematics
Canadian Mathematical Society
Real Sociedad Matemática Española
Royal Dutch Mathematical Society
Sociedad de Estadística e Investigación Operativa
Sociedad Española de Matemática Aplicada

Societat Catalana de Matemàtiques
Société Mathématique de France
Irish Mathematical Society
Mathematical Society of Japan
National Council of Teachers of Mathematics, USA
Sociedad Española de Investigación en Educación Matemática
Federación Española de Sociedades de Profesores de Matemáticas
Sociedad Española de Historia de las Ciencias y de las Técnicas

Private companies and foundations

Enterasys
Fundación Pedro Barrié de la Maza
Fundación Ramón Areces
Fundación Vodafone
Grupo SM, Editorial SM
ONCE
Springer
The King Juan Carlos I of Spain Center of N. Y. University in Madrid

Opening ceremony

Sir John Ball, President of the International Mathematical Union

Your Majesty,
Señor Ruiz Gallardón,
Señora Cabrera,
Señora Aguirre,
Professor Manuel de León,
Distinguished guests,
Ladies and gentlemen,

¡Bienvenidos al ICM dos mil seis! Welcome to ICM 2006, the 25th International Congress of Mathematicians, and the first ICM to be held in Spain. We offer our heartfelt thanks to the Spanish nation, so rich in history and culture, for its invitation to Madrid.

We greatly appreciate that His Majesty King Juan Carlos is honouring mathematics by His presence here today.

While celebrating this feast of mathematics, with the many talking-points that it will provide, it is worth reflecting on the ways in which our community functions.

Mathematics is a profession of high standards and integrity. We freely discuss our work with others without fear of it being stolen, and research is communicated openly prior to formal publication. Editorial procedures are fair and proper, and work gains its reputation through merit and not by how it is promoted. These are the norms operated by the vast majority of mathematicians. The exceptions are rare, and they are noticed.

Mathematics has a strong record of service, freely given. We see this in the time and care spent in the refereeing of papers and other forms of peer review. We see it in the running of mathematical societies and journals, in the provision of free mathematical software and teaching resources, and in the various projects world-wide to improve electronic access to the mathematical literature, old and new. We see it in the nurturing of students beyond the call of duty.

This service is exemplified by the tremendous efforts made over the last four years by Spanish mathematicians to bring this Congress to fruition. I propose that we formally record our appreciation of their splendid work through electing by acclamation the President of the Local Organizing Committee, Manuel de León, as President of this International Congress.

The Scientific Program of the Congress was in the capable hands of an international Program Committee consisting of Noga Alon (Israel, Chair), Douglas Arnold (USA), Joaquim Bruna (Spain), Kenji Fukaya (Japan), Nigel Hitchin (UK), Vaughan Jones (USA), Pierre-Louis Lions (France), Gregory Margulis (USA), Richard Taylor (USA),

S. R. Srinivasa Varadhan (USA), Claire Voisin (France), Enrique Zuazua (Spain). The International Mathematical Union is most grateful to the members of this committee, and to the many other mathematicians who served on the sectional panels, for their work in putting together a fine program of lectures.

Mathematicians do not own mathematics. But among the many millions who use mathematics daily they are distinguished by their constant search for deeper understanding based on an appreciation of beauty, simplicity, structure and the power of generalization. Yet the lesson of past centuries is that these vital elements in the development of mathematics require constant invigoration by new questions that come from the world about us.

There is no object, large or small, and almost no aspect of human existence, to which mathematics cannot contribute understanding. In particular, the great questions facing the planet, such as how to model and manage the climate, pose profound mathematical challenges. The need for an understanding of mathematics, of the mathematical way of thinking, and of the role mathematics can play in society, is no longer confined to scientists and engineers, but is increasingly important for those who work in industry, finance, the social sciences, and in many other walks of life, and thus also for all involved in education, for the media, opinion-formers and politicians. As subjects become better understood, they become more mathematical. Thus in the life sciences, for example, we see a rapid increase in the use of mathematical models, a trend that promises to profoundly influence medicine in the future.

In contemplating the importance of mathematics for the world, we see the importance of supporting the development of mathematics throughout the world. Mathematical talent does not respect geographical boundaries, but the opportunities, working conditions and tradition necessary for such talent to flourish depend heavily on geography, economic conditions and politics. Each country and region has its own needs for science and mathematics, its own problems as regards its mathematical development.

It is for these reasons that the IMU has made a special effort over the last four years to increase its support for mathematicians in developing countries. It has established an office for developing countries at the International Centre for Theoretical Physics in Trieste, and has cooperated with ICTP and the Abel Fund in the founding of the Ramanujan Prize for young mathematicians working in developing countries. At the IMU General Assembly held in Santiago de Compostela last weekend, a new class of Associate Membership was created to encourage more countries to join the Union. The IMU has augmented its developing countries programmes, particularly in Africa, helped by generous support from the following sponsors:

Niels Henrik Abel Memorial Fund (annual grant),

Nuffield Foundation and the Leverhulme Trust (linked grants to support mathematics in sub-Saharan Africa, in conjunction with the London Mathematical Society and the African Mathematics Millennium Science Initiative),

David and Lucile Packard Foundation,

Andrew W. Mellon Foundation,

American Mathematical Society,

London Mathematical Society.

Other sponsors, including those of the ICM itself, have made it possible for some 400 mathematicians from developing and economically disadvantaged countries, particularly younger researchers, to attend this Congress:

ICM sponsors,
American Mathematical Society,

Mathematical Society of Japan,

USA Committee for Mathematics,

London Mathematical Society,

Het Wiskundig Genootschap Netherlands,

Italian Mathematical Union (UMI),

German Mathematical Society (DMV),

European Mathematical Society.

Despite these initiatives, a dramatic increase in both funding and scientific interchange is required to address the global imbalances in mathematical education and research. In sharing mathematical knowledge and experience with those who work around the world, it is the whole mathematical community that benefits, and we make our own contribution to peace and stability through the binding together of peoples by a common language independent of politics, religion and culture.

I wish you all a rewarding and exciting Congress.

Manuel de León, President of the ICM2006 Organizing Committee

Your Majesty,
President of the Community of Madrid,
Minister of Education and Science,
Mayor of Madrid,
Professors John Ball and Phillip Griffiths,
Dear Colleagues, ladies and gentlemen,

On behalf of the Organizing Committee I would like to welcome you all to the ICM2006, and in particular to this opening ceremony.

First of all, I want to express our gratitude to the King Juan Carlos for His continuous support.

¡Muchas gracias, Majestad!

The ICM is a congress of great importance. Every four years, mathematicians from all over the world meet to celebrate mathematics, to inform each other of our latest results, to honour the most outstanding achievements during this period, to debate the present and future state of the discipline, to discuss how best to transfer new knowledge, and to bring mathematics closer to society and to improve public appreciation.

We Spanish mathematicians feel very honoured to have been entrusted by the IMU with the organization of this ICM. The constant support of the IMU Executive Committee and its president, Professor John Ball, has been essential for this task.

Furthermore, an event of this magnitude requires a great financial commitment, which on this occasion in Madrid has amounted to approximately two and a half million euros. Much of this funding has been provided by the Ministry of Education and Science, the Ministry of Foreign Affairs, the Ministry of Culture, the Community and the City of Madrid, and many others that you can see listed below; we are grateful for that support.

In addition to the scientific activities, an interesting series of round-table discussions has been organized, as well as an extensive programme of cultural and parallel activities. The fact that the entire process of registration and communication has been carried out electronically is also worthy of mention. Both this opening ceremony

and all the plenary lectures will be transmitted online throughout the world, and the congress records will be available on the website. This is a reflection of the importance of mathematics in today's Information Society.

The logo deserves a special mention because it is an essential part of every ICM, and on this occasion in Madrid it is the basis on which we have built the image of the Congress. It depicts a sunflower consisting of optimum growth mathematics and the golden mean representing a Spain of sunlight and optimism.

Our wish and our aim is for this ICM2006 to provide a platform for making the presence of mathematics felt in society, a process in which the media must inevitably play its part. To this end, the ICM2006 set up a Press Office that has worked together with the IMU to issue a weekly bulletin in English and Spanish aimed at both the media and the public at large.

Allow me also to explain how Spain has prepared itself for this day. Ten years ago, Spanish mathematicians set about reorganizing the social structure of our community, and in particular the Committee that liaises with the International Mathematical Union. At the same time, we began working on the organization of the World Mathematical Year in Spain. This collective project has had one important consequence: Spanish mathematicians came to the realization that we are a community, a community which, perhaps more than any other scientific discipline in this country, has subjected its strengths and weaknesses to an ongoing process of examination.

We have learned that mathematical research in Spain has made great progress in recent years. We now need to raise the standard of quality and encourage the interdisciplinary nature of mathematics, and are presently taking steps to achieve these aims.

We all agree on the vital role of mathematics in education, but it still remains to convince everyone of its equally important role as key technology for development. The new schemes for mathematical research currently being set up in Spain will undoubtedly help to increase qualitative and quantitatively the presence of Mathematics in science, technology and innovation. For a country like ours, this is the basis for a prosperous future.

The celebration of the ICM2006 in Madrid constitutes a landmark on this road. It also underlines our sense of belonging to an international community to whose organization and activities we are eager to make a contribution, continuing the process of internationalization that is already under way in Spain.

On behalf of the Organizing Committee, I would like to thank all the participants for coming to Madrid, some of them from very distant places, and I apologize if at any time we have been unable to meet all their demands. We would like you to know that in these coming days we are about to share, we are at your complete disposal.

Welcome to the ICM2006, welcome to Madrid! We wish you a successful conference and a very pleasant stay. Thank you all very much!

Alberto Ruiz Gallardón, Mayor of Madrid

Your Majesty,

Under the auspices of the Crown, and in keeping with the scientific and cultural progress that this Institution has enabled in Spain, Madrid bears today the honour and the responsibility of being the world capital of mathematical science. This has been made possible by the International Mathematical Union's choice of our city to host its twenty-fifth Congress, responding not only to the efforts made by Madrid City Council during its candidacy for the most prestigious mathematical event of our age, but also to the very nature of the capital of Spain as a crossroads of knowledge.

Over the next few days, the Congress promoters will witness this city's unquestionable capability regarding the organisation of significant events, with international impact, in the fields of science, culture, sports or economics. Madrid's excellent infrastructures for the staging of fairs and exhibitions and the wide range of services it offers are factors which explain the city's increasingly consolidated position at the forefront in terms of the hosting of conferences and congresses. However, the hospitality of the inhabitants of Madrid – on whose behalf I take this opportunity to extend a warm welcome to the participants of the Congress – and their interest in the intellectual progress of this century, are elements that have proved even more decisive in choosing Madrid for a gathering of the brightest minds of our age.

Madrid's long-standing relationship with mathematics can be traced back to at least 1582, when Phillip II founded the Royal Academy of Mathematics. Madrid also provided the stage upon which Agustín de Pedrayes, one of Spain's most celebrated mathematicians, who achieved fame in the International Congress of 1799 in Paris via his crucial contribution to the creation of the decimal metric system, carried out his professional activity between the 18th and 19th centuries. Nevertheless, Madrid's confidence in the success of this Congress is focused more on the future than on the past.

In a world where political systems appear faced with terrible challenges, where technology is hampered by uncompromising materialism, where the humanities seem overwhelmed by the challenge of providing an answer, you, as mathematicians, have the great privilege of speaking a different and eternally youthful language, wherein conjectures can be tested or refuted, whilst the language itself remains untainted by despair and its universality undiminished by disagreement. Laymen have difficulty

understanding the terms of the debate centred around Fermat's Last Theorem or those used to describe the essential humility of the mathematical possibilities surrounding Gödel's Theorem. Nevertheless, we believe that certain equations are as beautiful as the Iliad, as stated by the philosopher Edgar Quinet, and therefore we can find motives for consolation and hope. Indeed, beyond the specific applications of mathematical science, this discipline provides proof that the human need for understanding and for creativity remain intact. In these turbulent and yet complacent times, the inherent difficulty of mathematics – where, in the words of Plato, beauty and truth coincide – constitutes an intellectual stimulus, an invitation to better ourselves and a bastion of purity. The thinker George Steiner quoted Kepler to explain this phenomenon: "amidst massacres [and war], the laws of elliptical motion belong to no man and to no principality".

Therefore, Sire, perhaps it is not only mathematicians who need to come closer to society, by descending to the details of everyday life and explaining the usefulness of their science to the people, but it is all of us who are obliged to make the ethical and aesthetical effort to reach the same level of excellence, rigour and beauty that they inhabit.

In this two-fold hope and trust, it is a great pleasure for me to welcome the world's best mathematicians to Madrid.

Mercedes Cabrera, Minister for Education and Science

Your Majesty,

When the International Mathematical Union chose the City of Madrid to host the 25th International Congress of Mathematicians and for the presentation of the prestigious Fields Medals, the Spanish Government Ministry of Education and Science understood that it had to give its full support to the Organizing Committee of the event. In this way, our support for the Congress became an important part of the Scientific Policy Programme of Complementary Measures.

Given that more than 8,000 Spanish mathematicians are represented at the International Mathematical Union, we feel that at this time and together with them all the citizens of Spain are likewise represented, since we recognize the importance of mathematics in the development of thought, in the shaping and management of reality, and in the progress of Culture.

This Congress will serve to pave the way to new avenues of research, and to the exchange of new advances and opinions among all the different fields of knowledge, whether related directly or indirectly with mathematics. Furthermore, it will assist in advising public bodies, the Ministry of Education and Science among them, on the means of support it should adopt in the future.

We therefore celebrate this meeting as a great event of concern to everyone, and with our best wishes for its success we greet the members of the International Mathematical Union; the Organizing Committee of the Congress; the scientists who will be honoured for their achievements, and all the participants, especially all our guests from abroad.

We do not know what some of the pioneers in the history of mathematical research in Spain would have said if they had known about the congress we inaugurate today.

However, we know what we, as scientists, teachers or holders of public office, are obliged to offer both for them and for society in the matter of teaching and research. For them, in recognition and in tribute to their work and their memory; for society at large, because it is the proper task of public bodies, and in particular of the Ministry I represent, to make scientific achievement and discovery available to all in the interests of progress. That is why the Spanish Ministry of Education and Science is currently developing different projects in support of research in the fields of Mathematical Science.

As a basic policy, it is our aim to improve the role of mathematics in Education. To that end, the restructuring of the Spanish educational system as laid out in the new Organic Law of Education will enable us establish specific areas in which the acquisition of logic-mathematical skills and the development of mathematical learning at school level will accorded the status of basic abilities.

It is also our aim to pursue a new teaching methodology, encouraging practical experience in the classroom and furthering ongoing teacher training to meet our educational goals.

With regard to the situation of research in our country, Spain occupies the 9th position in the world in terms of scientific production in mathematics. This constitutes a considerable improvement over the last twenty-five years, and we expect the plans that are now being developed to improve this performance even further, by consolidating quality research teams and strengthening relations with researchers working on projects in other fields connected with technological innovation and development.

To achieve these goals, the National Programme for Mathematics has been set up within the framework of the R+D+I National Plan. In addition, the Consolider Mathematica Programme is being carried out as part of the broader Consolider Ingenio 2010, which will enable us to fund research work by top level groups in the field of Mathematics. In fact, the Consolider Mathematica programme has been chosen by the relevant Scientific Committee as a worthy recipient of immediate support.

We trust that these and other complementary measures, aimed at the training and mobility of research personnel and the creation of research institutions, will strengthen

Mathematical Science, both at an international level and in the Spanish System of Science, Technology and Business.

But today we are also here to celebrate the presentation of the Fields Medals and the Nevanlinna and Gauss Prizes. The Ministry of Education and Science of the Spanish Government congratulates the award-winners and expresses its gratitude for their generous contribution to society through Science. They are an example to us all, and especially to the many young people who are laying the foundations for their future professional careers.

Finally, I would like to express our gratitude to the members of Executive Committee of the Congress for all their efforts, and to all those involved in the organization of the many accompanying events and activities, as well as the scientists who by their work will enrich discussion and extend common understanding.

Your Majesty, we are aware of Your interest in seeing Spain occupy an important place in the society of knowledge and in the International Scientific Community, and of Your wish that all citizens acquire a solid education and training in preparation for the modern world. The Ministry of Education and Science is currently working on numerous schemes and projects to achieve this aim. If we are successful, we will have fulfilled one of the main purposes of our existence. Support for this International Congress of Mathematicians constitutes a further step along this road.

Many thanks and welcome to you all.

Esperanza Aguirre, President of the Community of Madrid

Your Majesty,

It is an honour and a source of great satisfaction for Madrid to welcome from today over 4,000 of the best mathematicians from all over the world who have gathered here to share their latest studies and discoveries, to explain the state of their researches, and to reward the most outstanding achievements of their colleagues with the Fields Medals and the Rolf Nevanlinna and Carl Friedrich Gauss Prizes.

In the 19th century, the German mathematician Gustav Jacobi stated that those who devoted themselves to study and research in Mathematics did so above all to “honour the human spirit”". This is how it has always been since the origins of mathematical thought, and the greatest achievements in this Science figure among the finest creations of humanity as a whole.

This is a good opportunity to recall that mathematical thought dates back to classical Greece, and lies at the source of all Western thought and civilization. From these brilliant beginnings, the essence of mathematical thought has consisted in finding an exact formulation for what we see, what we experience and what we perceive. That is why, whether we realize it or not, we are all descendants of Pythagoras.

To these words of greeting and welcome to Madrid I would also like to add my sincere congratulations to all the Congress participants for their efforts, for their researches, and for the knowledge they impart to their students, initiating them into the mysteries of their science. The intrinsic difficulties of their studies sometimes deprive them of recognition by society at large. That is why, with my congratulations, I would like to encourage them to continue with their fine work.

In the mid-19th century, the leading Spanish mathematician of the period, José Echegaray, stated that unfortunately there were few Spaniards of world status in mathematical research at that time. Happily today that is no longer the case, and the presence of the most outstanding mathematicians here in Madrid is the best demonstration of what I mean. I am sure that the celebration of this Congress in Madrid will act as a stimulus to all those young people in Spain who have discovered the pleasures of studying mathematics, and have begun to appreciate the beauty of its reasoning and its proofs. I likewise trust that the choice of Madrid as host city for this Congress will also be a source of pride and encouragement for all the Faculties of Mathematics at Madrid Universities.

With my very best wishes for the success of the Congress, and for the personal future and professional scientific career of all those concerned, I once again most cordially welcome you all to Madrid.

Many thanks.

Presentation of the new IMU logo by Phillip Griffiths, Secretary of IMU

The International Mathematical Union (IMU) has adopted a new logo. It was the winner of an international open competition announced by the IMU in 2004 that attracted over 80 submissions. The final selection was made by the Executive Committee of IMU.

The logo was designed by John Sullivan, Professor of Mathematical Visualization at the Technical University of Berlin (TU Berlin) and at the DFG Research Center MATHEON, and adjunct professor at the University of Illinois, Urbana (UIUC), with help from Prof. Nancy Wrinkle of Northeastern Illinois University.

The logo design is based on the Borromean rings, a famous topological link of three components. The rings have the surprising property that if any one component is removed, the other two can fall apart (while all three together remain linked). This so-called Brunnian property has led the rings to be used over many centuries in many cultures as a symbol of interconnectedness, or of strength in unity.

Although the Borromean rings are most often drawn as if made from three round circles, such a construction is mathematically impossible.

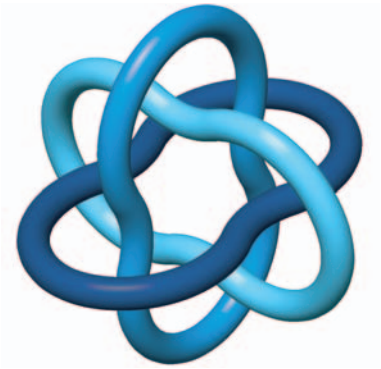
The IMU logo instead uses the tight shape of the Borromean rings, as would be obtained by tying them in rope pulled as tight as possible. Mathematically, this is the length-minimizing configuration of the link subject to the constraint that unit-diameter tubes around the three components stay disjoint. This problem and its solution are described in the paper *Criticality for the Gehring Link Problem* by J. Cantarella, J. Fu, R. Kusner, J. Sullivan, N. Wrinkle, Geometry and Topology 10 (2006), pp. 2055–2115, also available at arXiv.org/math/0402212.

Although this critical configuration is quite close to one made of convex and concave circular arcs, its actual geometry is surprisingly intricate. Each component is planar and piecewise smooth, with the shapes of many of the 14 pieces described by elliptic integrals. The improvement over the similar piecewise circular configuration leads to a savings of length of less than one tenth of one percent!

(The paper cited above first noticed a similar surprise in the simple clasp: one rope attached to the floor clasped around another attached to the ceiling. There as well, the minimizing shapes for the ropes are quite complicated, leaving a small gap between the thick tubes right at the tip.)

The tight configuration of the Borromean rings has pyritohedral symmetry (3*2 in the Conway/Thurston orbifold notation), and the IMU logo uses a view along a three-fold axis of rotation symmetry. Instead of the thick tubes, which would touch one another all along their lengths, thinner tubes are drawn, allowing a better view of the link.

Sullivan says the new logo "represents the interconnectedness not only of the various fields of mathematics, but also of the mathematical community around the world." Together with Charles Gunn of TU Berlin, he has made a 5-minute computer-graphics video The Borromean Rings: a new logo for the IMU that was shown at the ICM opening ceremony.



Presentation of the Fields Medals by John Ball, Chairman of the Fields Medal Committee

The 2006 Fields Medal Committee consisted of:

– Enrico Arbarello (Italy)

– John Ball (UK, Chair)

– Jeff Cheeger (USA)

– Donald Dawson (Canada)

– Gerhard Huisken (Germany)

– Curtis McMullen (USA)

– Alexey Parshin (Russia)

– Tom Spencer (USA)

– Michèle Vergne (France)

The instructions to the Committee are: to choose at least two, with a strong preference for four, Fields Medallists, to have regard in its choice to representing a diversity of mathematical fields, and to respect the age limit that a candidate's 40th birthday must not occur before January 1st of the year of the Congress at which the Fields Medals are awarded.

The Committee was privileged to consider a number of remarkable young mathematicians. Although the choice was a difficult one, the Committee was unanimous in selecting four medallists whose wonderful work demonstrates the breadth and richness of the subject. I will announce the names of the winners in alphabetical order.

A Fields Medal is awarded to Andrei Okounkov, of the Department of Mathematics, Princeton University, for his contributions bridging probability, representation theory and algebraic geometry.

A Fields Medal is awarded to Grigory Perelman, of St Petersburg, for his contributions to geometry and his revolutionary insights into the analytical and geometric structure of the Ricci flow. I regret that Dr. Perelman has declined to accept the medal.

A Fields Medal is awarded to Terence Tao, of the Department of Mathematics, University of California at Los Angeles (UCLA), for his contributions to partial differential equations, combinatorics, harmonic analysis and additive number theory.

A Fields Medal is awarded to Wendelin Werner, of the Laboratoire de Mathématiques, Université Paris-Sud, for his contributions to the development of stochastic Loewner evolution, the geometry of two-dimensional Brownian motion, and conformal field theory.

Presentation of the Nevanlinna Prize by Margaret H. Wright, Chair of the 2006 Nevanlinna Prize Committee

It is a privilege to announce the winner of the 2006 Rolf Nevanlinna Prize, which is awarded by the International Mathematical Union for outstanding contributions in mathematical aspects of information sciences.

The Nevanlinna Prize was first awarded in 1982. A requirement is that the winner's 40th birthday must occur on or after January 1 of the year in which the award is made.

The members of the 2006 Nevanlinna Prize Committee are:

– Samson Abramsky (United Kingdom)

– Franco Brezzi (Italy)

– Gert-Martin Greuel (Germany)

– Johan Håstad (Sweden)

– Margaret Wright, Chair (United States).

The International Mathematical Union awards the 2006 Nevanlinna Prize to Professor Jon M. Kleinberg of the Computer Science Department, Cornell University, Ithaca, New York, USA. Professor Kleinberg's date of birth is October 1971.

The Nevanlinna Prize citation for Jon Kleinberg is:

For deep, creative and insightful contributions to the mathematical theory of the global information environment, including

the influential "hubs and authorities" algorithm;

methods for discovering short chains in large social networks;

techniques for modeling, identifying and analyzing bursts in data streams;

theoretical models of community growth in social networks; and

contributions to the mathematical theory of clustering.

Jon Kleinberg's combination of mathematical ability, superb taste in interesting problems, breadth of interests and sense of strategy is both dazzling and unmatched. His work has had a fundamental impact on the effectiveness of today's most advanced Web search engines, and his mathematical insights have had applications to Internet routing, data mining, discrete optimization, and the sociology of the World Wide Web.

Presentation of the Gauss Prize by Martin Grötschel, Chair of the Gauss Prize Committee

Today we celebrate the first award of the Carl Friedrich Gauss Prize for applications of mathematics. Since this is a new IMU distinction, it is appropriate to say a few words about the scope of the prize in the beginning.

The Gauss Prize is awarded jointly by the Deutsche Mathematiker-Vereinigung (DMV, the German Mathematical Society) and the International Mathematical Union (IMU), and is administered by the DMV. The prize consists of a medal and a monetary award (currently EUR 10,000). The source of the prize fund is a small surplus from the International Congress of Mathematicians (ICM'98) held in Berlin eight years ago.

The statutes stipulate that the Gauss Prize is awarded for outstanding mathematical contributions that have found significant practical applications outside of mathematics, or for achievements that made the application of mathematical methods to areas outside of mathematics possible in an innovative way, e.g., via new modelling techniques or the design and implementation of algorithms. In a nutshell, the Carl Friedrich Gauss Prize is given for the impact the work of the prize winner has had in practice.

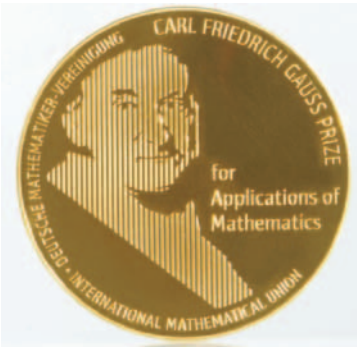
Since the practical usefulness of mathematical results is often not immediately visible, and as their applicability and importance for practice may only be realized after a long time lag – in contrast to the Fields Medal and the Rolf Nevanlinna Prize – no age limit restricts the choice of a prize winner.

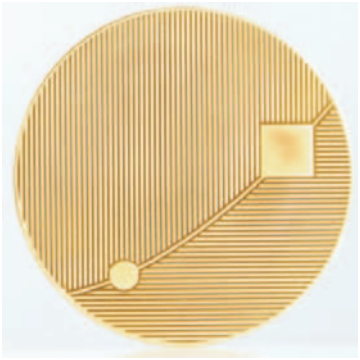
Scientific awards gain reputation through the choice of outstanding winners. The Fields Medal, e.g., is a prime example for this fact. The Gauss Prize jury hopes to mark the beginning of a similar tradition today by presenting an awardee whose research has influenced the world at large and whose contributions are highly respected by the mathematical community.

Why has the prize been given Gauss' name? Carl Friedrich Gauss (1777–1855) was one of the greatest mathematicians of all time. Gauss combined scientific theory and practice like no other before him or since. His *Disquisitiones Arithmeticae*, published in 1801, stand to this day as a true masterpiece of scientific investigation. In the same year, Gauss gained fame in wider circles for his prediction, using very few observations, of when and where the asteroid Ceres would next appear. The method of least squares, developed by Gauss as an aid in his mapping of the state of Hannover, is still an indispensable tool for analyzing data. His sextant is pictured on the last series of the German 10-Mark bills, honoring his considerable contributions to surveying.

On the front side of the bill, one also finds a bell curve, which is the graphical representation of the Gaussian normal distribution in probability. Together with Wilhelm Weber, Gauss invented the first electric telegraph. In recognition of his contributions to the theory of electromagnetism, the international unit of magnetic induction is the gauss. These few examples show that the impact of Gauss' mathematics can be experienced every day everywhere. With this new prize, IMU and DMV would like the world to recognize the importance of mathematics for our society; and Carl Friedrich Gauss is a prime example for the role mathematicians can play in this respect.

The medal, designed by Jan Arnold, that comes along with the award is displayed below. It shows on the front a familiar Gauss portrait dissolved into a linear pattern, the least squares method as well as the discovery of Ceres' orbit are symbolized on the back.





Following the prize statutes, the IMU Executive Committee appointed a Gauss Prize Committee for the 2006 award. The members were Bob Bixby, Martin Grötschel (chair), Frank den Hollander, Stéphane Mallat, and Ian Sloan. The establishment of the Gauss Prize was announced on April 30, 2002, Gauss' 225th birthday, and at the same time, nominations were invited. About thirty highly deserving mathematicians from all over the world were suggested for this prize by colleagues from pure and applied mathematics.

And now, I would like to announce the winner and read the citation.

The International Mathematical Union and the Deutsche Mathematiker-Vereinigung jointly award the Carl Friedrich Gauss Prize for Applications of Mathematics to Professor Kiyosi Itô for laying the foundations of the theory of stochastic differential equations and stochastic analysis. Itô's work has emerged as one of the major mathematical innovations of the 20th century and has found a wide range of applications outside of mathematics. Itô calculus has become a key tool in areas such as engineering (e.g., filtering, stability, and control in the presence of noise), physics (e.g., turbulence and conformal field theory), and biology (e.g., population dynamics). It is at present of particular importance in economics and finance with option pricing as a prime example.

The document is signed by John Ball, President of IMU, and Günter M. Ziegler, President of DMV.

A side remark, at this moment in time, a new application-oriented research institute called Quantitative Products Laboratory, is being founded in Berlin. It will be sponsored by a big German bank donating at least three million Euros annually. This new institute would not have been founded without the foundations laid by Kiyosi Itô.

The details of Itô's work will be explained tomorrow, August 23, in the Gauss Prize lecture presented by Hans Föllmer.

Kiyosi Itô was born in Japan in 1915. He received his Doctor of Science degree from the Imperial University in Tokyo and is now professor emeritus at Kyoto University. He has honorary doctoral degrees from Université Paris VI, ETH Zürich, and the University of Warwick. Itô is a member of the Académie des Sciences, France,

the Japan Academy, and the National Academy of Sciences, USA, to mention just a few of his many honors and distinctions.

For health reasons, Kiyosi Itô is unfortunately unable to be present at today's award ceremony.

The IMU President, John Ball, will personally take the Gauss Medal to Kyoto after this meeting and present it to Professor Itô in a special ceremony[1]. I am very happy to be able to announce that the Itô family has decided to send a representative to Madrid. Kiyosi Itô's youngest daughter, Junko Itô, who is professor and chair of linguistics at the University of California in Santa Cruz, is here to accept the Gauss Prize on behalf of her father.

[1] Photograph by Armin Mester. It shows John Ball and Kiyosi Itô on September 14, 2007 in Kyoto during the presentation of the Gauss Medal.

His Majesty the King of Spain, Juan Carlos

I am greatly pleased to preside over the opening of this Twenty-Fifth International Congress of Mathematicians, an outstanding scientific event which, in addition to its tradition of over a century, enjoys unquestionable prestige and significance on a global scale.

I extend my greetings to all the participants, my warm welcome to Spain to those from other countries, and my most heartfelt congratulations to the organizers of this Congress in Madrid.

You will understand that it is a very special pleasure for me that this Congress, which has brought together nearly four thousand scientists from over one hundred countries, is being held for the first time in our country.

Therefore, I wish to convey my greatest recognition and appreciation to the Spanish mathematical community, whose well-deserved prestige, proven effort and cohesion, have made Spain – and more specifically Madrid – the focus of attention of the international mathematical community this year.

This Congress enables us to learn about the main progress made by research in this discipline, and to highlight and promote in our respective societies the enormous importance of Mathematics. Importance because it is a basic instrument to understand the world, because it constitutes an unquestionable pillar of education, and because it is an indispensable tool to ensure progress for the benefit of Humanity.

Galileo told us that the world is written in mathematical language; to understand it, nothing can rival this discipline that has brought us together today in Madrid.

Improved understanding of the world we live in, by using the universality of Mathematics, is, in addition, a task which reinforces cooperation between diverse countries, societies and cultures.

It is equally evident that the high value of Mathematics in education requires our attention and dedication.

Mathematics is rightly considered the key technology. This is stated in the Declaration made public in 2000 by the International Mathematical Union and UNESCO, on the occasion of the World Mathematical Year.

We depend on, and we will increasingly depend on, the indispensable foundation that research, technology and innovation constitute for the future of our economic development and our social well-being.

For this reason, we must promote mathematical development as an essential element for progress that will enable sustainable development for all Humanity.

The business world must also join, with increasing efforts, a discipline which has been essential to our development, as it is, for example, the basic foundation to achieve the Information Society we currently enjoy.

Spain has been making a particular effort, and will continue to do so in the future, to promote its technological development.

Projects such as the Ingenio 2010 Programme are aimed at such a goal. We are pleased to see that Spanish mathematicians have not missed the opportunity to participate in such an ambitious R+D+I programme.

But this Congress also includes other aspects that I would like to highlight. With 108 countries represented, the largest number in its history, it aims to achieve universal representation and participation.

This has been made possible thanks to grant programmes for the participation of mathematicians from economically disadvantaged countries, following a long-standing tradition of the International Mathematical Union to which Spain is especially sensitive.

Furthermore, this Congress has made an enormous effort to bring Mathematics closer to society, striving to make it more wide-spread and well-known in public opinion.

All of this is being done through exhibitions, various cultural events and by reinforcing its presence in the media.

This effort to make Mathematics more well-known is particularly significant, as it is fundamental to encourage new scientific vocations all over the world.

In addition, these Congresses enable the mathematical community to award, every four years, and with well-deserved solemnity, its most highly prized and valued distinctions.

I am referring to the Fields Medal, the Rolf Nevanlinna Prize and the Carl Friedrich Gauss Prize, all of which are indisputably prestigious awards which have just been granted to this year's winners.

The Fields Medal has been awarded for 70 years to mathematicians under the age of 40 for outstanding achievement in the basic aspects of the discipline; the Rolf Nevanlinna Prize has been awarded since 1982 for the best mathematical contributions to the Information Society; and the Carl Friedrich Gauss Prize, awarded for the first time this year in Madrid, aims to honour outstanding achievement in contributing to improve our everyday lives.

I extend my most enthusiastic congratulations to all this year's winners.

Their work, professional career and scientific merits, as well as their contribution to our societies' development and well-being, deserve everyone's recognition and constitute an example and encouragement for the whole of the international mathematical

community.

To conclude, I would like to reiterate my most sincere support for the significant work done by the International Mathematical Union. I wish you every success for the next Congress to be held in India, just as I trust this one in Madrid will be successful.

I declare open the 25th International Congress of Mathematicians of 2006.

Thank you very much.

The King of Spain, Juan Carlos. On his left, Jon Kleinberg and Terence Tao; on his right Andrei Okounkov and Wendelin Werner.

Closing ceremony

The closing ceremony was held on Wednesday, August 30, starting at 18:00 in Auditorium A of the Palacio Municipal de Congresos de Madrid.

Sir John Ball, President of the International Mathematical Union

Welcome to the Closing Ceremony of ICM 2006!

You just saw a longer version of the video that was shown at the Opening Ceremony, concerning the new IMU logo, designed by John Sullivan.

It has been a marvellous International Congress, and we begin by a retrospective look at some of the highlights.

(Showing of video montage of scenes from the ICM.)

Before saying a few words about this Congress, I want to go back to before King Juan Carlos opened ICM 2006, and present a brief report about the IMU General Assembly held in Santiago de Compostela on 19 and 20 August. This was a very successful meeting, which owed much to the care and consideration of the local organizing committee in Santiago chaired by Juan Viaño.

The General Assembly voted to make various changes to the Statutes and the Procedures for Election of IMU. In particular a new independent Nominating Committee structure for the construction of slates for elections was approved. In future the Executive Committee of the International Commission on Mathematical Instruction, concerned with mathematics education, will be elected by the ICMI General Assembly rather than the IMU General Assembly. The number of members-at-large on the IMU Executive Committee is increased from five to six, and a new category of Associate Membership of IMU, with no dues, no votes and limited duration, was introduced to encourage full membership.

Turning to the elections themselves, the new Executive Committee of IMU to serve for the period 2007–2010 will be:

President. László Lovász (Hungary)

Secretary. Martin Grötschel (Germany)

Vice Presidents. Zhiming Ma (China), Claudio Procesi (Italy)

Members at Large. Salah Baouendi (USA), Manuel de León (Spain), Ragni Piene (Norway), Cheryl Praeger (Australia), Victor Vassiliev (Russia), Marcelo Viana (Brazil)

I would like to pay tribute to the work of this committee, and especially to the retiring members: Phillip Griffiths, who has completed two terms as Secretary of IMU, Jean-Michel Bismut (Vice-President), Masaki Kashiwara (Vice-President), Jacob Palis (Past-President and Past Secretary of IMU), and M. S. Raghunathan.

And we also will say farewell to Linda Geraci, who has served admirably as the IMU Administrator.

The membership of the Commission on Development and Exchanges, concerned with developing countries, for 2007–2010 will be:

President. S.G. Dani (India)

Secretary. Gérard González-Sprinberg (France)

Members at Large. Graciela Boente (Argentina), Paulo Cordaro (Brazil), Jean-Pierre Gossez (Belgium), Mary Teuw Niane (Sénégal), Marta Sanz-Solé (Spain), Jiping Zhang (China)

CDE will be unified with the recently formed Developing Countries Strategy Group (DCSG) to form a new IMU Commission for Developing Countries which will both consider strategy and administer the IMU grants programmes. I would like to thank the members of CDE and in particular Herb Clemens, the outgoing CDE Secretary and the Chair of DCSG, for their excellent work, in which they have been ably assisted by the Developing Countries Administrator Sharon Laurenti.

The new Executive Committee of ICMI for 2007–2009 will be:

President. Michèle Artigue (France)

Secretary-General. Bernard Hodgson (Canada)

Vice Presidents. Jill Adler (South Africa), Bill Barton (New Zealand)

Members at Large. Maria Bartolini Bussi (Italy), Jaime Carvalho e Silva (Portugal), Celia Hoyles (UK), S. Kumaresan (India), Alexei Semenov (Russia)

The fact that this Executive Committee will hold office for three rather than four years is related to the transition process towards the new electoral system for ICMI.

The General Assembly also elected two members to the International Commission for the History of Mathematics, Christian Houzel (France) and Peter Neumann (UK).

Although it is appointed rather than elected, I want to show you the membership of the Committee for Electronic Information and Communication (CEIC) for the next two years:

Chair. Jonathan Borwein (Canada)

Members at Large. Michael Doob (Canada), David Eisenbud (USA), John Ewing (USA), Ulf Rehmann (Germany), Alf van der Poorten (Australia) and one member from the IMU Executive Committee.

This is one of IMU's most important committees. Examples of its fine work are the new Electronic and Federated World Directories of Mathematicians. If you have not used these important resources you can learn about them on the IMU webpages. IMU is very grateful to this committee and in particular to its Chair Jonathan Borwein.

An important discussion in Santiago concerned IMU's finances. As well as a 5% increase in dues for each of the next 4 years, an increase in the number of units paid by the generally wealthier countries in groups IV and V was agreed. These increases,

though painful, are essential to pay for IMU's increased activities, especially with respect to developing countries.

A further important discussion concerned a new set of guidelines for the scientific programme of future ICMs. This is a quite lengthy and detailed document, that after revision will be made available on the IMU webpages. The new guidelines begin with a description of the purpose of the ICM:

Every ICM should reflect the current activity of mathematics in the world, present the best work being carried out in all mathematical subfields and different regions of the world, and thus point to the future of mathematics. The invited speakers at an ICM should be mathematicians of the highest quality who are able to present current research to a broad mathematical audience.

I think that this is an important statement which should help future Program Committees in the difficult job of choosing a geographically balanced list of speakers of the highest quality.

The General Assembly passed 11 resolutions. I want to show you the four resolutions over which there was some discussion. Resolution 8 concerned mathematical education:

The General Assembly of the IMU reaffirms the importance of the issues treated by ICMI (*the International Commission on Mathematical Instruction*). *It recognizes the importance of continuing and strengthening the relationship of IMU with ICMI and urges the increased involvement of research mathematicians in mathematical education at all levels.*

Resolution 9 concerns CEIC:

With the ultimate goal of creating an enduring network of digital mathematical literature, the General Assembly of the IMU endorses the new version of the "Best practices" document of its Committee on Electronic Information and Communication (*CEIC*), *posted June* 2005 *at http://www.ceic.math.ca, as well as the March* 2005 *draft of "Digital Mathematical Library: a vision for the Future".*

The digital mathematical library is a very important project that we need to do as much as we can to further.

Resolution 10 concerns the freedom of movement of scientists and mathematicians:

The General Assembly of the IMU continues to endorse the principle of universality expressed in the International Council for Science (*ICSU*) *ARTICLE* 5 *of the STATUTES, as adopted by the* 1998 *General Assembly, and endorses the additional ICSU Statement on the Universality of Science* (2004). *Notwithstanding heightened tensions, security concerns, etc., the General Assembly urges free exchange of scientific ideas and free circulation of scientists and mathematicians across international borders. The IMU opposes efforts by governments to restrict contacts, interactions, access and travel in the world mathematical community, particularly when such restrictions penalize individual mathematicians for the actions of governments.*

Resolution 7 concerns the finances of IMU:

The General Assembly recommends that the incoming Executive Committee of the IMU studies the establishment of stable administrative structure and funding mechanisms, including possible fund-raising, for the support of the expanding IMU activities, and report to the 2010 *General Assembly with concrete proposals.*

Finally, the General Assembly decided that the location of ICM2010 will be Hyderabad in India.

If you want to learn more about IMU, you can consult the IMU webpages, where a detailed report of the General Assembly will appear, and read the new electronic newsletter IMU-Net. Mireille Chaleyat-Maurel has done a splendid job in the production of the newsletter – can we express our thanks to her.

The planning and bringing together of the many elements that make up the International Congress is a daunting undertaking. In several respects, such as online internet transmission of the plenary lectures and the management of relations with the media, of which I will have more to say in a moment, ICM 2006 has set standards for the future. In addition, the local organizing committee complemented the scientific programme with a tapestry of interesting events and exhibitions, expressing the richness of mathematics through discourse, history and art.

To all those who have lived the Congress over the last few years, and to those who have helped during the Congress itself, together making it such a great occasion, we say that your hard work has really been worth it, and how very much it is appreciated by all who have spent these days in Madrid.

In his closing address, Manuel de León will give us the opportunity to recognize the many individuals who have contributed to the success of this Congress. But with his permission I want to say a few words about the ICM and the media. This was a cooperative effort between IMU and the ICM Press Office. The Congress turned out to be a remarkable news story, and it was remarkably told. I wish to thank Allyn Jackson and Christof Poeppe, who wrote the initial press releases for the prizes, Marcus du Sautoy, who gave invaluable advice, and through articles and interviews contributed greatly to generating media interest, and Anne-Marie Astad for making available distribution lists developed for the Abel Prize. But no praise is too great for the accomplishments of the ICM Press Office itself, which consisted of Monica Salomone and Ignacio Fernandez Bayo of DIVULGA, supported by the splendid team that you see listed in a section of this volume. The result of their untiring and professional work was unprecedented national and international press coverage of the Congress and of mathematics.

Let me end by saying that it has been a great privilege to serve as President of IMU, and to work with my colleagues on the Executive Committee and with the Local Organizing Committee of the Congress. The IMU is very fortunate to have László Lovász as its next President. I wish him every success for his term of office, and thank you all for your participation in the Congress.

I now invite László Lovász to address the Congress.

László Lovász, Elected President of the International Mathematical Union

Ladies and gentlemen,

Let me start with joining John Ball in expressing my sincere thanks and most heartfelt congratulations to the Organizers of the Congress. They have done a tremendous job, and we all benefited from this a lot: not only the participants, but also those colleagues and students to whom we go back and to whom we'll communicate what we have learned here.

I would also like to extend these thanks and congratulations to the Program Committee and the Executive Committee, who also worked very hard over the last 4 years. In particular, I express my thanks to John Ball for his devout, selfless, and I must say, very successful job he did as the President of IMU. It will very difficult to measure up to his work; one fact that helps me face this task is that as Past President, he'll be a member of the Executive Committee, and I'll count on his advice and help. I'd also extend these thanks to the retiring members of the Executive Committee: Vice Presidents Jean-Michel Bismut and Masaki Kashiwara, Secretary Phillip Griffiths, Madabusi Raghunathan and Past President Jacob Palis. To those members of the Executive Committee who stayed on to serve a second term, Vice president Zhi-Ming Ma, Secretary Martin Grötschel, Ragni Piene and Victor Vassiliev, I am thankful for their willingness to do so, and I am looking forward to working with them.

I also want to express my thanks to the speakers. To be invited to the Congress is a great honor but also a great responsibility. Some areas are easier to talk about to a general mathematical audience than others; but I feel that all our speakers made a great afford to convey the main ideas and results to us.

Let me add a few more personal thoughts. When one arrives at a Congress, one cannot feel but overwhelmed by the number of people and by the variety of mathematics that is presented here. One could walk the corridors for minutes without seeing a familiar face, and one could browse the abstracts long before seeing a topic that one, say, did research in. This is so even for a senior person who attended many previous Congresses, and obviously a young person who has not been to previous Congresses must feel this even more.

It is perhaps because of this feeling that people repeatedly bring up the idea of abandoning these International Congresses. I feel this would be a serious mistake. I talked to scientists working in other fields, and they expressed their envy for the fact that we have a meeting where the best mathematicians tell to all of us what are the main problems, trends, or paradigms of their fields; where we honor the recipients of major prizes, and hear and discuss their work; where we have panel discussions and also corridor discussions about important issues facing our science or our community.

I hope that now, 9 days after the opening, all participants, in particular our young colleagues, go home with a feeling that mathematics is a vibrant, live, beautiful and fruitful science, and this will help them in their research, teaching and popularization of mathematics. And I hope that you'll come back to the next congress. See you at ICM 2010!

Manuel de León, President of the ICM2006 Organizing Committee

Dear colleagues,

Ten days ago in this same auditorium, we opened the 25th International Congress of Mathematicians. Since then we have been meeting here in this impressive Palacio Municipal de Congresos. We hope that this time together has been fruitful, and that you have met old friends and made new ones.

The best way of knowing if an ICM has been successful is if the participants are sorry to depart. If that is the case, then remember that it is not "Goodbye" but "See you soon!", because the great mathematical family will continue to meet at other congresses all over the World, and in four years time we will all be together again in Hyderabad, India, to enjoy the hospitality of our Indian friends.

No ICM would be possible without the effort of many people, and now is the moment to acknowledge them.

First, those in the different committees:

– Local Program Committee
– Satellite conferences
– Web
– Grants
– Cultural activities
– Social activities
– Infrastructure and logistics
– Publications

The efforts of the Secretariat, under the direction of our General Secretary José Luis González-Llavona, has been fundamental. I hope they will forgive us for any moments of impatience or bad moods during the run-up to the Congress.

The work of our congress agency, UNICONGRESS, has also been essential. We have worked together through thick and thin, but the final result has made it all worthwhile. Our thanks to them, to all our suppliers, and to all the staff at the Palacio Municipal de Congresos.

I believe that if one thing stands out in this ICM2006, it is the extraordinary coverage provided by the press, and for that we have mainly to thank our friends at DIVULGA, led by Ignacio F. Bayo and Mónica Salomone. Their example is one to be followed, to continue the effort of putting mathematics across to the people.

Another crucial help was provided by our over 350 volunteers. Their patient and enthusiasm have contributed to do this ICM unforgettable for all of us. Thank you very much to all of you!

Finally, we express our thanks to all the participants for taking the trouble to come to Madrid in such difficult times, to set this great example of tolerance and peaceful co-existence. Thanks to all of you. Have a safe journey home, and see you again in India in 2010!

See you all soon!

¡Hasta pronto!

Rajat Tandon, University of Hyderabad, India

Sir John Ball,

Professor Lovász,

Professor Manuel de Léon,

Ladies and gentleman,

Let me first take this opportunity to express my appreciation of the innumerable number of people who have worked so tirelessly for this Congress in Madrid. Let me say 'Gracias' to our Spanish hosts and the local organizing committee under the chairmanship of Prof. Manuel de Léon whose monumental effort has ensured the unqualified success of this ICM. I say 'Gracias' to the hundreds of volunteers who have been so gracious in rendering their assistance to us. And finally I thank the various committees of the IMU who have presented us with such a strong and exciting academic programme. We recognize that we have our work cut out for us if we are to emulate the success of this Congress in Hyderabad.

We in India feel very privileged to have the honour of hosting the next International Congress of Mathematicians. It gives us enormous pleasure to invite the mathematical community from all six continents to Hyderabad for the ICM2010, to be held from the 19th to the 27th of August.

Hyderabad, like Madrid, is a wonderful composition of the old and the new. This city, founded more than 400 years ago, houses teeming bazaars, old jewelry and fine craftsmen, old forts and mausoleums. Cosmopolitan in its population you find people of all faiths living and learning together here.

Two hundred years ago this city expanded to the twin cities of Hyderabad and Secunderabad with the addition of a cantonment area and today greater Hyderabad is a conglomeration of three cities in one with the modern Cyberabad area which is second only to Bangalore as the information technology heart of India. Here you find not only large research and development centres of the top Indian IT companies like the Tata Consultancy Services or Infosys but also the large multinationals like IBM, Microsoft and Google.

This is the charm of Hyderabad – whilst you will find computer scientists at an international institute of information technology grapple with the intricacies of P = NP, you will also find the finest pearl craftsmen in the world – their craft inherited from their forefathers over hundreds of years. Hyderabad is known as the pearl capital of India and perhaps of the world.

The organizing committee for the ICM2010 will be pushing for several satellite conferences in different parts of India – north, south, east and west. So those who wish to visit the Taj Mahal or the Pink city of Jaipur or the temples of Mahabalipuram will always be able to find a satellite conference of their choice near the place they want to visit. We are urging other South Asian countries to hold satellite conferences as well.

It will be our pleasure to host a meeting of the General Assembly of the IMU in Bangalore on the 16th and 17th of August just prior to the ICM.

I urge all delegates here to let it be known to the mathematical community of their countries that an open and democratic India, the home of Ramanujan, with a vibrant community of scholars of its own warmly welcomes them all and urges them to mix mathematics with pleasure and flavour the traditional hospitality of India in the August of 2010. We assure you that it will be a memorable experience.

The granite sculpture created by Keizo Ushio – a beautiful infinity, and the special stamp of the Congress.

The work of the Fields Medalists, the Rolf Nevanlinna Prize Winner and the Gauss Prize Winner

Wendelin Werner, Andrei Okounkov, Terence Tao, Jon Kleinberg, and Junko Itô, youngest daughter of Kiyosi Itô.

Andrei Okounkov

B.S. in Mathematics, Moscow State University, 1993

Ph.D. in Mathematics, Moscow State University, 1995

Positions until today

1994–1995	Research Fellow in the Dobrushin Mathematical Laboratory at the Institute for Problems of Information Transmission, Russian Academy of Sciences
1996	Member in the Institute of Advanced Study in Princeton
1997	Member in the Mathematical Sciences Research Institute in Berkeley, on leave from University of Chicago
1996–1999	L. E. Dickson instructor in Mathematics, University of Chicago
1998–2001	Assistant Professor of Mathematics, University of California at Berkeley
2001–2002	Professor of Mathematics, University of California at Berkeley
Present position	Professor of Mathematics, Princeton University

The work of Andrei Okounkov

Giovanni Felder

Andrei Okounkov's initial area of research is group representation theory, with particular emphasis on combinatorial and asymptotic aspects. He used this subject as a starting point to obtain spectacular results in many different areas of mathematics and mathematical physics, from complex and real algebraic geometry to statistical mechanics, dynamical systems, probability theory and topological string theory. The research of Okounkov has its roots in very basic notions such as partitions, which form a recurrent theme in his work. A partition λ of a natural number n is a non-increasing sequence of integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ adding up to n. Partitions are a basic combinatorial notion at the heart of the representation theory. Okounkov started his career in this field in Moscow where he worked with G. Olshanski, through whom he came in contact with A. Vershik and his school in St. Petersburg, in particular S. Kerov. The research programme of these mathematicians, to which Okounkov made substantial contributions, has at its core the idea that partitions and other notions of representation theory should be considered as random objects with respect to natural probability measures. This idea was further developed by Okounkov, who showed that, together with insights from geometry and ideas of high energy physics, it can be applied to the most diverse areas of mathematics.

This is an account of some of the highlights mostly of his recent research.

I am grateful to Enrico Arbarello for explanations and for providing me with very useful notes on Okounkov's work in algebraic geometry and its context.

1. Gromov–Witten invariants

The context of several results of Okounkov and collaborators is the theory of Gromov–Witten (GW) invariants. This section is a short account of this theory. GW invariants originate from classical questions of enumerative geometry, such as: how many rational curves of degree d in the plane go through $3d-1$ points in general position? A completely new point of view on this kind of problems appeared at the end of the eighties, when string theorists, working on the idea that space-time is the product of four-dimensional Minkowski space with a Ricci-flat compact complex three-fold, came up with a prediction for the number of rational curves of given degree in the quintic $x_1^5 + \cdots + x_5^5 = 0$ in $\mathbb{C}P^4$. Roughly speaking, physics gives predictions for differential equations obeyed by generating functions of numbers of curves. Solving these equations in power series gives recursion relations for the numbers. In particular a recursion relation of Kontsevich gave a complete answer to the above question on rational curves in the plane.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

In general, Gromov–Witten theory deals with intersection numbers on moduli spaces of maps from curves to complex manifolds. Let V be a nonsingular projective variety over the complex numbers. Following Kontsevich, the compact moduli space $\overline{M}_{g,n}(V,\beta)$ (a Deligne–Mumford stack) of *stable maps* of class $\beta \in H_2(V)$ is the space of isomorphism classes of data $(C, p_1, \dots, p_n, f)$ where C is a complex projective connected nodal curve of genus g with n marked smooth points $p_1, \dots, p_n$ and $f: C \to V$ is a stable map such that $[f(C)] = \beta$. Stable means that if f maps an irreducible component to a point then this component should have a finite automorphism group. For each $j = 1, \dots, n$ two natural sets of cohomology classes can be defined on these moduli space: 1) pull-backs $\mathrm{ev}_j^*\alpha \in H^*(\overline{M}_{g,n}(V,\beta))$ of cohomology classes $\alpha \in H^*(V)$ on the target V by the evaluation map $\mathrm{ev}_j: (C, p_1, \dots, p_n, f) \mapsto f(p_j)$; 2) the powers of the first Chern class $\psi_j = c_1(L_j) \in H^2(\overline{M}_{g,n}(V,\beta))$ of the line bundle L_j whose fiber at $(C, p_1, \dots, p_n, f)$ is the cotangent space $T^*_{p_j}C$ to C at p_j. The *Gromov–Witten invariants* of V are the intersection numbers

$$\langle \tau_{k_1}(\alpha_1) \dots \tau_{k_n}(\alpha_n) \rangle^V_{\beta,g} = \int_{\overline{M}_{g,n}(V,\beta)} \prod \psi_j^{k_j} \mathrm{ev}_j^* \alpha_j.$$

If all k_i are zero and the α_i are Poincaré duals of subvarieties, the Gromov–Witten invariants have the interpretation of counting the number of curves intersecting these subvarieties. As indicated by Kontsevich, to define the integral one needs to construct a *virtual fundamental class*, a homology class of degree equal to the "expected dimension"

$$\mathrm{vir\,dim}\, \overline{M}_{g,n}(V,\beta) = -\beta \cdot K_V + (g-1)(3 - \dim V) + n, \tag{1}$$

where K_V is the canonical class of V. This class was constructed in works of Behrend–Fantechi and Li–Tian.

The theory of Gromov–Witten invariants is already non-trivial and deep in the case where V is a point. In this case $\overline{M}_{g,n} = \overline{M}_{g,n}(\{\mathrm{pt}\})$ is the Deligne–Mumford moduli space of stable curves of genus g with n marked points. Witten conjectured and Kontsevich proved that the generating function

$$F(t_0, t_1, \dots) = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k_1+\dots+k_n = 3g-3+n} \langle \tau_{k_1} \dots \tau_{k_n} \rangle^{\mathrm{pt}}_g \prod_{j=1}^{n} t_{k_j},$$

involving simultaneously all genera and numbers of marked points, obeys an infinite set of partial differential equations (it is a tau-function of the Korteweg–de Vries integrable hierarchy obeying the "string equation") which are sufficient to compute all the intersection numbers explicitly. One way to write the equations is as Virasoro conditions

$$L_k(e^F) = 0, \quad k = -1, 0, 1, 2 \dots,$$

for certain differential operators L_k of order at most 2 obeying the commutation relations $[L_j, L_k] = (j-k)L_{j+k}$ of the Lie algebra of polynomial vector fields.

Before Okounkov few results were available for general projective varieties V and they were mostly restricted to genus $g = 0$ Gromov–Witten invariants (quantum cohomology). For our purpose the conjecture of Eguchi, Hori and Xiong is relevant here. Again, Gromov–Witten invariants of V can be encoded into a generating function F_V depending on variables $t_{j,a}$ where a labels a basis of the cohomology of V. Eguchi, Hori and Xiong extended Witten's definition of the differential operators L_k and conjectured that F_V obeys the Virasoro conditions $L_k(e^{F_V}) = 0$ with these operators.

2. Gromov–Witten invariants of curves

In a remarkable series of papers ([10], [11], [12]), Okounkov and Pandharipande give an exhaustive description of the Gromov–Witten invariants of curves. They prove the Eguchi–Hori–Xiong conjecture for general projective curves V, give explicit descriptions in the case of genus 0 and 1, show that the generating function for $V = \mathbb{P}^1$ is a tau-function of the Toda hierarchy and consider also in this case the $\mathbb{C}^\times$-equivariant theory, which is shown to be governed by the 2D-Toda hierarchy. They also show that GW invariants of $V = \mathbb{P}^1$ are unexpectedly simple and more basic than the GW invariants of a point, in the sense that the latter can be obtained as a limit, giving thus a more transparent proof of Kontsevich's theorem.

A key ingredient is the *Gromov–Witten/Hurwitz correspondence* relating GW invariants of a curve V to *Hurwitz numbers*, the numbers of branched covering of V with given ramification type at given points. A basic beautiful formula of Okounkov and Pandharipande is the formula for the *stationary* GW invariants of a curve V of genus $g(V)$, namely those for the Poincaré dual ω of a point:

$$\langle \tau_{k_1}(\omega) \dots \tau_{k_n}(\omega) \rangle^{\bullet\, V}_{\beta=d\cdot[V],g} = \sum_{|\lambda|=d} \left(\frac{\dim \lambda}{d!} \right)^{2-2g(V)} \prod_{i=1}^{n} \frac{p_{k_i+1}(\lambda)}{(k_i+1)!}. \tag{2}$$

The (finite!) summation is over all partitions λ of the degree d and $\dim \lambda$ is the dimension of the corresponding irreducible representation of S_d. The genus g of the domain is fixed by the condition that the cohomological degree of the integrand is equal to the dimension of the virtual fundamental class. It is convenient here to include also stable maps with possibly disconnected domains and this is indicated by the bullet. The functions $p_k(\lambda)$ on partitions are described below.

Hurwitz numbers can be computed combinatorially and are given in terms of representation theory of the symmetric group by an explicit formula of Burnside. If the covering map at the ith point looks like $z \to z^{k_i+1}$, i.e., if the monodromy at the ith point is a cycle of length $k_i + 1$, the formula is

$$H^V_d(k_1+1, \dots, k_n+1) = \sum_{|\lambda|=d} \left(\frac{\dim \lambda}{d!} \right)^{2-2g(V)} \prod_{i=1}^{n} f_{k_i+1}(\lambda).$$

Thus in this case the GW/Hurwitz correspondence is given by the substitution rule $f_{k+1}(\lambda) \to p_{k+1}(\lambda)/(k+1)!$. The functions f_k and p_k are basic examples of *shifted symmetric functions*, a theory initiated by Kerov and Olshanski, and the results of Okounkov and Pandharipande offer a geometric realization of this theory. A shifted symmetric polynomial of n variables $\lambda_1, \dots, \lambda_n$ is a polynomial invariant under the action of the symmetric group given by permuting $\lambda_j - j$. A shifted symmetric function is a function of infinitely many variables $\lambda_1, \lambda_2 \dots$, restricting for each n to a shifted symmetric polynomial of n variables if all but the first n variables are set to zero. Shifted symmetric functions form an algebra $\Lambda^* = \mathbb{Q}[p_1, p_2, \dots]$ freely generated by the *regularized shifted power sums*, appearing in the GW invariants:

$$p_k(\lambda) = \sum_j \left(\left(\lambda_j - j + \tfrac{1}{2}\right)^k - \left(-j + \tfrac{1}{2}\right)^k \right) + (1 - 2^{-k})\zeta(-k)$$

The second term and the Riemann zeta value "cancel out" in the spirit of Ramanujan's second letter to Hardy: $1+2+3+\cdots = -\frac{1}{12}$. The shifted symmetric functions $f_k(\lambda)$ appearing in the Hurwitz numbers are central characters of the symmetric groups S_n: $f_1 = |\lambda| = \sum \lambda_i$ and the sum of the elements of the conjugacy class of a cycle of length $k \geq 2$ in the symmetric group S_n is a central element acting as $f_k(\lambda)$ times the identity in the irreducible representation corresponding to λ. The functions p_k and f_k are two natural shifted versions of Newton power sums.

In the case of genus $g(V) = 0, 1$, Okounkov and Pandharipande reformulate (2) in terms of expectation values and traces in fermionic Fock spaces and get more explicit descriptions and recursion relations. In particular if $V = E$ is an elliptic curve the generating function of GW invariants reduces to the formula of Bloch and Okounkov [1] for the character of the infinite wedge projective representation of the algebra of polynomial differential operators, which is expressed in terms of Jacobi theta functions. As a corollary, one obtains that

$$\sum_d q^d \langle \tau_{k_1}(\omega) \dots \tau_{k_n}(\omega) \rangle_d^{\bullet E}$$

belongs to the ring $\mathbb{Q}[E_2, E_4, E_6]$ of *quasimodular forms*.

A shown by Eskin and Okounkov [2], one can use quasimodularity to compute the asymptotics as $d \to \infty$ of the number of connected ramified degree d coverings of a torus with given monodromy at the ramification points. By a theorem of Kontsevich–Zorich and Eskin–Mazur, this asymptotics gives the volume of the moduli space of holomorphic differentials on a curve with given orders of zeros, which is in turn related to the dynamics of billiards in rational polygons. Eskin and Okounkov give explicit formulae for these volumes and prove in particular the Kontsevich–Zorich conjecture that they belong to $\pi^{-2g}\mathbb{Q}$ for curves of genus g.

3. Donaldson–Thomas invariants

As is clear from the dimension formula (1) the case of three-dimensional varieties V plays a very special role. In this case, which in the Calabi–Yau case $K_V = 0$ is the original context studied in string theory, it is possible to define invariants counting curves by describing curves by equations rather than in parametric form. Curves in V of genus g and class $\beta \in H_2(V)$ given by equations are parametrized by Grothendieck's Hilbert schemes $\mathrm{Hilb}(V; \beta, \chi)$ of subschemes of V with given Hilbert polynomial of degree 1. The invariants β, $\chi = 2 - g$ are encoded in the coefficients of the Hilbert polynomial. R. Thomas constructed a virtual fundamental class of $\mathrm{Hilb}(V; \beta, \chi)$ for three-folds V of dimension $-\beta \cdot K_V$, the same as the dimension of $\bar{M}_{g,0}(V, \beta)$. Thus one can define Donaldson–Thomas (DT) invariants as intersection numbers on this Hilbert scheme. There is no direct geometric relation between $\mathrm{Hilb}(V; \beta, \chi)$ and $\bar{M}_{g,0}(V, \beta)$, and indeed the (conjectural) relation between Gromov–Witten invariants and Donaldson–Thomas invariants is quite subtle. In its simplest form, it relates the GW invariants $\int_{\bar{M}^\bullet_{g,n}(V,\beta)} \prod \mathrm{ev}_i^* \gamma_i$ to the DT invariants $\int_{\mathrm{Hilb}(V;\beta,\chi)} \prod c_2(\gamma_i)$. The class $c_2(\gamma)$ is the coefficient of $\gamma \in H^*(V)$ in the Künneth decomposition of the second Chern class of the ideal sheaf of the universal family $\mathcal{V} \subset \mathrm{Hilb}(V; \beta, \chi) \times V$.

The conjecture of Maulik, Nekrasov, Okounkov and Pandharipande [6], [7], inspired by ideas of string theory [14] states that suitably normalized generating functions $Z'_{GW}(\gamma; u)_\beta$, $Z'_{DT}(\gamma; q)_\beta$ are essentially related by a coordinate transformation:

$$(-iu)^{-d} Z'_{GW}(\gamma_1, \ldots, \gamma_n; u)_\beta = q^{-d/2} Z'_{DT}(\gamma_1, \ldots, \gamma_n; q)_\beta, \quad \text{if } q = -e^{iu}, \beta \neq 0.$$

Here $d = -\beta \cdot K_V$ is the virtual dimension. Moreover these authors conjecture that there $Z'_{DT}(\gamma; q)_\beta$ is a *rational* function of q. This has the important consequence that all (infinitely many) GW invariants are determined in principle by finitely many DT invariants. Versions of these conjectures are proven for local curves and the total space of the canonical bundle of a toric surface. The GW/DT correspondence can be viewed as a far-reaching generalization of formula (2), to which it reduces in the case where V is the product of a curve with $\mathbb{C}^2$.

4. Other uses of partitions

Here is a short account of other results of Okounkov based on the occurrence of partitions.

One early result of Okounkov [9] is his first proof of the Baik–Deift–Johansson conjecture (two further different proofs followed, one by Borodin, Okounkov and Olshanski and one by Johansson). This conjecture states that, as $n \to \infty$, the joint distribution of the first few rows of a random partition of n with the Plancherel measure $P(\lambda) = (\dim \lambda)^2/|\lambda|!$, natural from representation theory, is the same, after proper shift and rescaling, as the distribution of the first few eigenvalues of a Gaussian random

hermitian matrix of size n. The proof involves comparing random surfaces given by Feynman diagrams and by ramified coverings and contains many ideas that anticipate Okounkov's later work on Gromov–Witten invariants.

Random partitions also play a key role in the work [8] of Nekrasov and Okounkov on $N = 2$ supersymmetric gauge theory in four dimensions. Seiberg and Witten gave a formula for the effective "prepotential", postulating a duality with a theory of monopoles. The Seiberg–Witten formula is given in terms of periods on a family of algebraic curves, closely connected with classical integrable systems. Nekrasov showed how to rigorously define the prepotential of the gauge theory as a regularized instanton sum given by a localization integral on the moduli space of antiselfdual connections on $\mathbb{R}^4$. Nekrasov and Okounkov show that this localization integral can be written in terms of a measure on partitions with periodic potential and identify the Seiberg–Witten prepotential with the surface tension of the limit shape.

Partitions of n also label $(\mathbb{C}^\times)^2$-invariant ideals of codimension n in $\mathbb{C}[x, y]$ and thus appear in localization integrals on the Hilbert scheme of points in the plane. Okounkov and Pandharipande [13] describe the ring structure of the equivariant quantum cohomology (genus zero GW invariants) of this Hilbert scheme in terms of a time-dependent version of the Calogero–Moser operator from integrable systems.

5. Dimers

Dimers are a much studied classical subject in statistical mechanics and graph combinatorics. Recent spectacular progress in this subject is due to the discovery by Okounkov and collaborators of a close connection of planar dimer models with real algebraic geometry.

A *dimer configuration* (or perfect matching) on a bipartite graph G is a subset of the set of edges of G meeting every vertex exactly once. For example if G is a square grid we may visualize a dimer configuration as a tiling of a checkerboard by dominoes. In statistical mechanics one assigns positive weights (Boltzmann weights) to edges of G and defines the weight of a dimer configuration as the product of the weights of its edges. The basic tool is the Kasteleyn matrix of G, which is up to certain signs the weighted adjacency matrix of G. For finite G Kasteleyn proved that the partition function (i.e., the sum of the weights of all dimer configurations) is the absolute value of the determinant of the Kasteleyn matrix.

Kenyon, Okounkov and Sheffield consider a doubly periodic bipartite graph G embedded in the plane with doubly periodic weights. For each natural number n one then has a probability measure on dimer configurations on $G_n = G/n\mathbb{Z}^2$ and statistical mechanics of dimers is essentially the study of the asymptotics of these probability measures in the thermodynamic limit $n \to \infty$. One key observation is the Kasteleyn matrix on G_1 can be twisted by a character $(z, w) \in (\mathbb{C}^\times)^2$ of $\mathbb{Z}^2$ and thus one defines the *spectral curve* as the zero set $P(z, w) = 0$ of the determinant of the

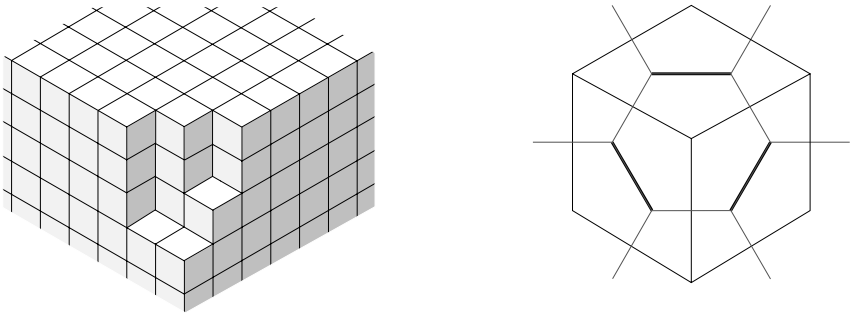
twisted Kasteleyn matrix $P(z, w) = \det K(z, w)$. This determinant is a polynomial in $z^{\pm 1}$, $w^{\pm 1}$ with real coefficients and thus defines a real plane curve.

The main observation of Kenyon, Okounkov and Sheffield [3] is that the spectral curve belongs to the very special class of (simple) Harnack curves, which were studied in the 19th century and have reappeared recently in real algebraic geometry. Kenyon, Okounkov and Sheffield show that in the thermodynamic limit, three different *phases* (called gaseous, liquid and frozen) arise. These phases are characterized by qualitatively different long-distance behaviour of pair correlation functions. One can see these phases by varying two real parameters (B_1, B_2) (the "magnetic field") in the weights, so that the spectral curve varies by rescaling the variables. The regions in the (B_1, B_2)-plane corresponding to different phases are described in terms of the *amoeba* of the spectral curve, namely the image of the curve by the map $\mathrm{Log}\colon (z, w) \mapsto (\log|z|, \log|w|)$. The amoeba of a curve is a closed subset of the plane which looks a bit like the microorganism with the same name. The amoeba itself corresponds to the liquid phase, the bounded components of its complement to the gaseous phase and the unbounded components to the frozen phase. This insight has a lot of consequences for the statistics of dimer models and lead Okounkov and collaborators to beautiful results on interfaces with various boundary conditions [3], [5].

Such a precise and complete description of phase diagrams and shapes of interfaces is unprecedented in statistical mechanics.

6. Random surfaces

One useful interpretation of dimers is as models for random surfaces in three-dimensional space. In the simplest case one considers a model for a melting or dissolving cubic crystal in which at a corner some atoms are missing (see figure).



A melting crystal corner (left) and the relation between tilings and dimers (right).

Viewing the corner from the (1,1,1) direction one sees a tiling of the plane by 60° rhombi, which is the same as a dimer configuration on a honeycomb lattice (each tile

covers one dimer of the dimer configuration). In this simple model one gives the same probability for every configuration with given missing volume. If one lets the size of the cubes go to zero keeping the missing volume fixed, the probability measure concentrates on an a surface, the limit shape. More generally, every planar dimer model can be rephrased as a random surface model and limit shapes for more general crystal corner geometries can be defined. Kenyon, Okounkov and Sheffield show that the limit shape is given by the graph of (minus) the *Ronkin function* $R(x, y) = (2\pi i)^{-2} \int_{|z|=|w|=1} \log(P(e^x z, e^y w)) dz dw/zw$ of the spectral curve (in the case of the honeycomb lattice with equal weights, $P(z, w) = z + w + 1$). This function is affine on the complement of the amoeba and strictly convex on the amoeba. So the connected components of the complement of the amoeba are the projections of the facets of the melting crystal.

In addition to this surprising connection with real algebraic geometry, random surfaces of this type are essential in the GW/DT correspondence, see Section 3, as they arise in localization integrals for DT invariants of toric varieties.

7. The moduli space of Harnack curves

The notions used by Okounkov and collaborators in their study of dimer models arose in an independent recent development in real algebraic geometry. Their result bring a new probabilistic point of view in this classical subject.

In real algebraic geometry, unsurmountable difficulties already appear when one consider curves. The basic open question is the first part of Hilbert's 16th problem: what are the possible topological types of a smooth curve in the plane given by a polynomial equation $P(z, w) = 0$ of degree d? Topological types up to degree 7 are known but very few general results are available. In a recent development in real algebraic geometry in the context of toric varieties the class of Harnack curves plays an important role and can be characterized in many equivalent way. In one definition, due to Mikhalkin, a Harnack curve is a curve such that the map to its amoeba is 2:1 over the interior, except at possible nodal points; equivalently, by a theorem of Mikhalkin and Rullgård, a Harnack curve is a curve whose amoeba has area equal to the area of the Newton polygon of the polynomial P. These equivalent properties determine the topological type completely.

Kenyon and Okounkov prove [4] that *every* Harnack curve is the spectral curve of some dimer model. They obtain an explicit parametrization of the moduli space of Harnack curves with fixed Newton polygon by weights of dimer models, and deduce in particular that the moduli spaces are connected.

8. Concluding remarks

Andrei Okounkov is a highly creative mathematician with both an exceptional breadth and a sense of unity of mathematics, allowing him to use and develop, with perfect ease, techniques and ideas from all branches of mathematics to reach his research objectives. His results not only settle important questions and open new avenues of research in several fields of mathematics, but they have the distinctive feature of mathematics of the very best quality: they give simple complete answers to important natural questions, they reveal hidden structures and new connections between mathematical objects and they involve new ideas and techniques with wide applicability.

Moreover, in addition to obtaining several results of this quality representing significant progress in different fields, Okounokov is able to create the ground, made of visions, intuitive ideas and techniques, where new mathematics appears. A striking example for this concerns the relation to physics: many important developments in mathematics of the last few decades have been inspired by high energy physics, whose intuition is based on notions often inaccessible to mathematics. Okounkov's way of proceeding is to develop a mathematical intuition alternative to the intuition of high energy physics, allowing him and his collaborators to go beyond the mere verification of predictions of physicists. Thus, for example, in approaching the topological vertex of string theory, instead of stacks of D-branes and low energy effective actions we find mathematically more familiar notions such as localization and asymptotics of probability measures. As a consequence, the scope of Okounkov's research programme goes beyond the context suggested by physics: for example the Maulik–Nekrasov–Okounkov–Pandharipande conjecture is formulated (and proved in many cases) in a setting which is much more general than the Calabi–Yau case arising in string theory.

References

[1] Bloch, Spencer, and Okounkov, Andrei, The character of the infinite wedge representation. *Adv. Math.* **149** (1) (2000), 1–60.

[2] Eskin, Alex, and Okounkov, Andrei, Asymptotics of numbers of branched coverings of a torus and volumes of moduli spaces of holomorphic differentials. *Invent. Math.* **145** (1) (2001), 59–103.

[3] Kenyon, Richard, Okounkov, Andrei, and Sheffield, Scott, Dimers and amoebae. *Ann. of Math.* (2) **163** (3) (2006), 1019–1056.

[4] Kenyon, Richard, and Okounkov, Andrei, Planar dimers and Harnack curves. *Duke Math. J.* **131** (3) (2006), 499–524.

[5] Kenyon, Richard, and Okounkov, Andrei, Limit shapes and the complex burgers equation. Preprint; arXiv:math-ph/0507007.

[6] Maulik, D., Nekrasov, N., Okounkov, A., and Pandharipande, R., Gromov-Witten theory and Donaldson-Thomas theory, I. Preprint; arXiv:math.AG/0312059.

[7] Maulik, D., Nekrasov, N., Okounkov, A., and Pandharipande, R., Gromov-Witten theory and Donaldson-Thomas theory, II. Preprint; arXiv:math. AG/0406092.

[8] Nekrasov, Nikita A., and Okounkov, Andrei, Seiberg-Witten theory and random partitions. In *The unity of mathematics*, Progr. Math. 244, Birkhäuser, Boston, MA, 2006, 525–596.

[9] Okounkov, Andrei, Random matrices and random permutations. *Internat. Math. Res. Notices* **2000** (20) (2000), 1043–1095.

[10] Okounkov, Andrei, and Pandharipande, Rahul, Gromov-Witten theory, Hurwitz theory, and completed cycles. *Ann. of Math.* (2) **163** (2) (2006), 517–560.

[11] Okounkov, Andrei, and Pandharipande, Rahul, The equivariant Gromov-Witten theory of $\mathbf{P}^1$. *Ann. of Math.* (2) **163** (2) (2006), 561–605.

[12] Okounkov, Andrei, and Pandharipande, Rahul, Virasoro constraints for target curves. *Invent. Math.* **163** (1) (2006), 47–108.

[13] Okounkov, Andrei, and Pandharipande, Rahul, Quantum cohomology of the Hilbert scheme of points in the plane. Preprint; arXiv:math.AG/0411210.

[14] Okounkov, Andrei, Reshetikhin, Nikolai, and Vafa, Cumrun, Quantum Calabi-Yau and classical crystals. In *The unity of mathematics*, Progr. Math. 244, Birkhäuser, Boston, MA, 2006, 597–618.

Department of Mathematics, ETH Zurich, 8092 Zurich, Switzerland
E-mail: felder@math.ethz.ch

Grigory Perelman

Ph.D. Leningrad State University, November 1990

Positions until today

December 1990–November 1992	Junior researcher at St. Petersburg Department of the V. A. Steklov Institute of the Russian Academy of Sciences (PDMI)
December 1992–December 1998	Researcher at PDMI Computer Science Department
January 1999–May 2004	Senior researcher at PDMI
June 2004–December 2005	Leading researcher at PDMI

The work of Grigory Perelman

John Lott

Grigory Perelman has been awarded the Fields Medal for his contributions to geometry and his revolutionary insights into the analytical and geometric structure of the Ricci flow.

Perelman was born in 1966 and received his doctorate from St. Petersburg State University. He quickly became renowned for his work in Riemannian geometry and Alexandrov geometry, the latter being a form of Riemannian geometry for metric spaces. Some of Perelman's results in Alexandrov geometry are summarized in his 1994 ICM talk [20]. We state one of his results in Riemannian geometry. In a short and striking article, Perelman proved the so-called Soul Conjecture.

Soul Conjecture (conjectured by Cheeger–Gromoll [2] in 1972, proved by Perelman [19] in 1994). Let M be a complete connected noncompact Riemannian manifold with nonnegative sectional curvatures. If there is a point where all of the sectional curvatures are positive then M is diffeomorphic to Euclidean space.

In the 1990s, Perelman shifted the focus of his research to the Ricci flow and its applications to the geometrization of three-dimensional manifolds. In three preprints [21], [22], [23] posted on the arXiv in 2002–2003, Perelman presented proofs of the Poincaré conjecture and the geometrization conjecture.

The Poincaré conjecture dates back to 1904 [24]. The version stated by Poincaré is equivalent to the following.

Poincaré conjecture. A simply-connected closed (= compact boundaryless) smooth 3-dimensional manifold is diffeomorphic to the 3-sphere.

Thurston's geometrization conjecture is a far-reaching generalization of the Poincaré conjecture. It says that any closed orientable 3-dimensional manifold can be canonically cut along 2-spheres and 2-tori into "geometric pieces" [27]. There are various equivalent ways to state the conjecture. We give the version that is used in Perelman's work.

Geometrization conjecture. If M is a connected closed orientable 3-dimensional manifold then there is a connected sum decomposition $M = M_1 \# M_2 \# \cdots \# M_N$ such that each M_i contains a 3-dimensional compact submanifold-with-boundary $G_i \subset M_i$ with the following properties:

1. G_i is a graph manifold.
2. The boundary of G_i, if nonempty, consists of 2-tori that are incompressible in M_i.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

3. $M_i - G_i$ admits a complete finite-volume Riemannian metric of constant negative curvature.

In the statement of the geometrization conjecture, G_i is allowed to be $\emptyset$ or M_i. (For example, if $M = S^3$ then we can take $M_1 = G_1 = S^3$.) The geometrization conjecture implies the Poincaré conjecture. Thurston proved that the geometrization conjecture holds for Haken 3-manifolds [27]. Background information on the Poincaré and geometrization conjectures is in [17].

Perelman's papers have been scrutinized in various seminars around the world. At the time of this writing, the work is still being examined. Detailed expositions of Perelman's work have appeared in [1], [16], [18].

1. The Ricci flow approach to geometrization

Perelman's approach to the geometrization conjecture is along the lines of the Ricci flow strategy developed by Richard Hamilton. In order to put Perelman's results in context, we give a brief summary of some of the earlier work. A 1995 survey of the field is in [12].

If M is a manifold and $\{g(t)\}$ is a smooth one-parameter family of Riemannian metrics on M then the Ricci flow equation is

$$\frac{dg}{dt} = -2\,\mathrm{Ric}. \tag{1}$$

It describes the time evolution of the Riemannian metric. The right-hand side of the equation involves the Ricci tensor Ric of $g(t)$. We will write $(M, g(\cdot))$ for a Ricci flow solution.

Ricci flow was introduced by Hamilton in 1982 in order to prove the following landmark theorem.

Positive Ricci curvature ([7]). Any connected closed 3-manifold M that admits a Riemannian metric of positive Ricci curvature also admits a Riemannian metric of constant positive sectional curvature.

A connected closed 3-dimensional Riemannian manifold with constant positive sectional curvature is isometric, up to scaling, to the quotient of the standard round 3-sphere by a finite group that acts freely and isometrically on S^3. In particular, if M is simply-connected and admits a Riemannian metric of positive Ricci curvature then M is diffeomorphic to S^3. The idea of the proof of the theorem is to run the Ricci flow, starting with the initial metric $g(0)$ of positive Ricci curvature. The Ricci flow will go singular at some finite time T, caused by the shrinking of M to a point. As time approaches T, if one continually rescales M to have constant volume then the rescaled sectional curvatures become closer and closer to being constant on M.

In the limit, one obtains a Riemannian metric on M with constant positive sectional curvature.

Based on Hamilton's result, Hamilton and S.-T. Yau developed a program to attack the Poincaré conjecture using Ricci flow. The basic idea was to put an arbitrary initial Riemannian metric on the closed 3-manifold, run the Ricci flow and analyze the evolution of the metric.

Profound results about Ricci flow were obtained over the years by Hamilton and others. Among these results are the Hamilton–DeTurck work on the existence and uniqueness of Ricci flow solutions [6], [7], Hamilton's maximum principle for Ricci flow solutions [8], the Hamilton–Chow analysis of Ricci flow on surfaces [4], [9], Shi's local derivative estimates [25], Hamilton's differential Harnack inequality for Ricci flow solutions with nonnegative curvature operator [10], Hamilton's compactness theorem for Ricci flow solutions [11] and the Hamilton–Ivey curvature pinching estimate for three-dimensional Ricci flow solutions [12, Theorem 24.4],[15]. We state one more milestone result of Hamilton, from 1999.

Nonsingular flows ([14]). *Suppose that the normalized Ricci flow on a connected closed orientable* 3*-manifold* M *has a smooth solution that exists for all positive time and has uniformly bounded sectional curvatures. Then* M *satisfies the geometrization conjecture.*

The normalized Ricci flow is a variant of the Ricci flow in which the volume is kept constant. The above result clearly showed that Ricci flow was a promising approach to the geometrization conjecture. The remaining issues were to remove the assumption that the Ricci flow solution is smooth for all positive time, and the *a priori* bound on the sectional curvature.

Regarding the smoothness issue, many 3-dimensional solutions of the Ricci flow equation (1) encounter a singularity within a finite time. One example of a singularity is a standard neckpinch, in which a cross-sectional 2-sphere $\{0\} \times S^2$ in a topological neck $((-1, 1) \times S^2) \subset M$ shrinks to a point in a finite time. Hamilton introduced the idea of performing a surgery on a neckpinch [13]. At some time, one removes a neighborhood $(-c, c) \times S^2$ of the shrinking 2-sphere and glues three-dimensional balls onto the ensuing boundary 2-spheres $\{-c\} \times S^2$ and $\{c\} \times S^2$. After the surgery operation the topology of the manifold has changed, but in a controllable way, since the presurgery manifold can be recovered from the postsurgery manifold by connected sums. One then lets the postsurgery manifold evolve by Ricci flow. If one encounters another neckpinch singularity then one performs a new surgery, lets the new manifold evolve, etc.

One basic issue was to show that if the Ricci flow on a closed 3-manifold M encounters a singularity then an entire connected component disappears or there are nearby 2-spheres on which to do surgery. To attack this, Hamilton initiated a blowup analysis for Ricci flow [12, Section 16]. It is known that singularities arise from curvature blowups [7]. That is, if a Ricci flow solution exists on a maximal time interval $[0, T)$, with $T < \infty$, then $\lim_{t \to T^-} \sup_{x \in M} |\mathrm{Riem}(x, t)| = \infty$, where Riem

denotes the sectional curvatures. Suppose that $\{(x_i, t_i)\}_{i=1}^{\infty}$ is a sequence of spacetime points with $\lim_{i\to\infty} |\operatorname{Riem}(x_i, t_i)| = \infty$. In order to understand the geometry of the Ricci flow solution as one approaches the singularity time, one would like to spatially expand around (x_i, t_i) by a factor of $|\operatorname{Riem}(x_i, t_i)|^{\frac{1}{2}}$ and take a convergent subsequence of the ensuing geometries as $i \to \infty$. In fact, if one also expands the time coordinate by $|\operatorname{Riem}(x_i, t_i)|$ then one can consider taking a subsequence of rescaled Ricci flow solutions, that converges to a limit Ricci flow solution $(M_\infty, g_\infty(\cdot))$.

Hamilton's compactness theorem [11] gives sufficient conditions to extract a convergent subsequence. Roughly speaking, on the rescaled solutions one needs uniform curvature bounds on balls and a uniform lower bound on the injectivity radius at (x_i, t_i). One can get the needed curvature bounds by carefully choosing the blowup points (x_i, t_i). However, before Perelman's work, the needed injectivity radius bound was not available in full generality.

If the blowup limit $(M_\infty, g_\infty(\cdot))$ exists then it is a nonflat ancient solution, meaning that it is defined for $t \in (-\infty, 0]$. The manifold M_∞ may be compact or noncompact. In the three-dimensional case, Hamilton–Ivey pinching implies that for each $t \in (-\infty, 0]$, the time-t slice $(M_\infty, g_\infty(t))$ has nonnegative sectional curvature. Thus the possible blowup limits are very special. Hamilton gave detailed analyses of various singularity models [12, Section 26]. One troublesome possibility, the so-called $\mathbb{R} \times$ *cigar soliton* ancient solution, could not be excluded. If this particular solution occurred in a blowup limit then it would be problematic for the surgery program, as there would be no evident 2-spheres along which to do surgery. Hamilton conjectured [12, Section 26] that the $\mathbb{R} \times$ *cigar soliton* solution could be excluded by means of a suitable generalization of the "little loop lemma" [12, Section 15].

In addition, there was the issue of showing that any point of high curvature in the original Ricci flow solution on $[0, T)$ has a neighborhood that is indeed modeled by a blowup limit.

2. No local collapsing theorem

Perelman's first breakthrough in Ricci flow, the no local collapsing theorem, removed two major stumbling blocks in the program to prove the geometrization of three-dimensional manifolds using Ricci flow. It allows one to take blowup limits of finite time singularities and it shows that the $\mathbb{R} \times$ *cigar soliton* solution cannot arise as a blowup limit.

No local collapsing theorem ([21]). *Let M be a closed n-dimensional manifold. If $(M, g(\cdot))$ is a given Ricci flow solution that exists on a time interval $[0, T)$, with $T < \infty$, then for any $\rho > 0$ there is a number $\kappa > 0$ with the following property. Suppose that $r \in (0, \rho)$ and let $B_t(x, r)$ be a metric r-ball in a time-t slice. If the sectional curvatures on $B_t(x, r)$ are bounded in absolute value by $\frac{1}{r^2}$ then the volume of $B_t(x, r)$ is bounded below by κr^n.*

Perelman expresses the conclusion of the no local collapsing theorem by saying that the Ricci flow solution is "κ-noncollapsed at scales less than ρ". The theorem says that after rescaling the metric ball to have radius one, if the sectional curvatures of the rescaled ball are bounded in absolute value by one then the volume of the rescaled ball is bounded below by κ. This lower bound on the volume is a form of noncollapsing. The theorem is scale-invariant, except for the condition that r should be less than the scale ρ.

Perelman proves his no local collapsing theorem using new monotonic quantities for Ricci flows, which he calls the $\mathcal{W}$-functional and the reduced volume $\tilde{V}$. Expressions that are time-nondecreasing under the Ricci flow, loosely known as entropies, were known to be potentially useful tools; for example, such an entropy was used in the two-dimensional case in [9]. However, no relevant entropies were previously known in higher dimensions. Perelman's entropy functionals arise from a new and profound understanding of the underlying structure of the Ricci flow equation. The method of proof of the no local collapsing theorem is to show that a local collapsing contradicts the monotonicity of the entropy.

The significance of the no local collapsing theorem is that under a curvature assumption, it implies a lower bound on the injectivity radius at x, using [3]. This is what one needs in order to extract blowup limits. Any blowup limit $(M_\infty, g_\infty(t))$ will be a nonflat ancient solution which, from the no local collapsing theorem, is κ-noncollapsed at all scales. If such an ancient solution additionally has nonnegative curvature operator and bounded curvature (which will be the case for three-dimensional blowup limits) then Perelman calls it a *κ-solution*.

Hereafter we assume that M is an orientable three-dimensional manifold. Perelman gives the following classification of κ-solutions.

Three-dimensional κ-solutions ([21], [22]). *Any three-dimensional orientable κ-solution $(M_\infty, g_\infty(\cdot))$ falls into one of the following types:*

(a) *$(M_\infty, g_\infty(\cdot))$ is a finite isometric quotient of the round shrinking 3-sphere.*

(b) *M_∞ is diffeomorphic to S^3 or $\mathbb{R}P^3$.*

(c) *$(M_\infty, g_\infty(\cdot))$ is the standard shrinking $\mathbb{R} \times S^2$ or its $\mathbb{Z}_2$-quotient $\mathbb{R} \times_{\mathbb{Z}_2} S^2$.*

(d) *M_∞ is diffeomorphic to $\mathbb{R}^3$ and, after rescaling, each time slice is asymptotically necklike at infinity.*

In particular, Perelman shows that the $\mathbb{R} \times$ *cigar soliton* ancient solution cannot arise as a blowup limit (as there is no $\kappa > 0$ for which it is κ-noncollapsed at all scales), thereby realizing Hamilton's conjecture.

Perelman's main use of κ-solutions is to model the high-curvature regions of a Ricci flow solution. By means of a sophisticated version of the blowup analysis, he proves the following result, which we state in a qualitative form.

Canonical neighborhoods ([21]). *Given $T < \infty$, if $(M, g(\cdot))$ is a nonsingular Ricci flow on a closed orientable 3-manifold M that is defined for $t \in [0, T)$ then any region*

of high scalar curvature is modeled, after rescaling, by the corresponding region in a three-dimensional κ-solution.

Perelman's first Ricci flow paper [21] concludes by showing that if the Ricci flow on a closed orientable 3-manifold M has a smooth solution that exists for all positive time then M satisfies the geometrization conjecture. There is no *a priori* curvature assumption. The proof of this result uses the long-time analysis described in Section 4.

3. Ricci flow with surgery

Perelman's second Ricci flow paper [22] is a technical tour de force. He constructs a surgery algorithm to handle Ricci flow singularities. There are several issues involved in setting up a surgery algorithm. The most basic issue is to know that if the Ricci flow encounters a singularity then a connected component disappears or there are 2-spheres along which one can perform surgery, with control on the topology of the excised regions. This is an issue about the geometry of the Ricci flow near a singularity. For the first singularity time, it is handled by the above canonical neighborhood theorem. A second issue is to perform the surgery so as to not ruin the Hamilton–Ivey pinching condition on the curvature. A third issue is to show that surgery times do not accumulate. If surgery times accumulate then one may never get to a sufficiently large time to draw any topological conclusions.

Hereafter we consider a Ricci flow $(M, g(\cdot))$ on a connected closed oriented 3-manifold. With T being the first singularity time (if there is one), Perelman defines Ω to be the points in M where the scalar curvature R stays bounded up to time T, i.e. $M - \Omega = \{x \in M : \lim_{t\to T^-} R(x,t) = \infty\}$. Here Ω is an open subset of M. The next result gives the topology of M if the scalar curvature blows up everywhere.

Components that go extinct ([22]). *If $\Omega = \emptyset$ then M is diffeomorphic to a finite isometric quotient S^3/Γ of the round 3-sphere, to $S^1 \times S^2$ or to $S^1 \times_{\mathbb{Z}_2} S^2 = \mathbb{R}P^3 \# \mathbb{R}P^3$.*

Now suppose that the scalar curvature blows up somewhere but not everywhere, i.e. $\Omega \neq \emptyset$. Perelman's surgery procedure involves going up to the singularity time T and then trimming off horns. More precisely, there is a limiting time-T metric $\bar{g}$ on Ω, with scalar curvature function $\bar{R}$. For a small number $\rho > 0$, the part of Ω where the scalar curvature is not too big is $\Omega_\rho = \{x \in \Omega : \bar{R}(x) \leq \rho^{-2}\}$, a compact subset of M. The connected components of Ω can be divided into those that intersect Ω_ρ and those that do not. The connected components of Ω that do not intersect Ω_ρ have uniformly large scalar curvature and are discarded. Using the canonical neighborhood theorem, Perelman shows that if a connected component of Ω intersects Ω_ρ then it has a finite number of ends, each being a so-called "ε-horn". The latter statement means that the scalar curvature goes to infinity as one exits the end, and in addition if x is a point in the ε-horn then after expanding the metric to make the scalar curvature

at x equal to one, there is a neighborhood of x in Ω that is geometrically close to a cylinder $(-\varepsilon^{-1}, \varepsilon^{-1}) \times S^2$. (Here ε is a fixed small number.) The surgery procedure consists of cutting each such ε-horn along one of these cross-sectional 2-spheres and gluing in a 3-ball.

If one does the surgery in this way then one has control on how the topology changes. Indeed, the presurgery manifold is recovered from the postsurgery manifold by taking connected sums of components, along with some possible additional connected sums with a finite number of $S^1 \times S^2$ or $\mathbb{R}P^3$ factors. (The $S^1 \times S^2$ factors come from surgeries that do not disconnect M. The $\mathbb{R}P^3$ factors can arise from connected components of Ω that were thrown away.) One can guarantee that the surgery preserves the Hamilton–Ivey curvature pinching condition by carefully prescribing the geometric way that the 3-ball is glued, following [13].

One can then run the Ricci flow, starting from the postsurgery manifold, up to the next singularity time T' (if there is one). However, if one wants to do surgery at time T' then one must find the 2-spheres along which to cut. The main problem is that the earlier surgeries could invalidate the conclusion of the canonical neighborhood theorem on $[0, T')$. The proof of the canonical neighborhood theorem in turn relied on the no local collapsing theorem.

One ingredient of Perelman's resolution of this problem is to perform surgery sufficiently far down in the ε-horns. In effect, there is a self-improvement phenomenon as one goes down the horn. Perelman shows that for any $\delta > 0$, if a point x is in an ε-horn as before, and is sufficiently deep within the horn, then after rescaling to make the scalar curvature at x equal to one, there is a neighborhood of x that is geometrically close to a cylinder $(-\delta^{-1}, \delta^{-1}) \times S^2$. Hence one can ensure that the surgeries are done within cylinders that are very long relative to the cross-section. This turns out to be a key to extending the no local collapsing theorem to the case when there are intervening surgeries within the time interval. To summarize, Perelman proves the following technically difficult theorem.

Surgery algorithm ([22]). *The surgery parameters can be chosen so that there is a well-defined Ricci-flow-with-surgery.*

The statement means that the Ricci-flow-with-surgery exists for all time. (It is not excluded that at some finite time the remaining manifold becomes the empty set.) Perelman's proof is quite intricate and uses an induction on the time interval. In addition, for a given induction step, i.e. on a given time interval, he uses a contradiction argument to show that the surgery parameters can be chosen so as to ensure that versions of the no local collapsing theorem and the canonical neighborhood theorem hold on the time interval, despite possible intervening surgeries.

Volume considerations show that only a finite number of surgeries occur on a finite time interval; any surgery within the time interval removes a definite amount of volume, but there is only so much volume available for removal.

4. Long-time behavior

Once one has the Ricci-flow-with-surgery, in order to obtain topological information about the original manifold one needs to analyze the long-time behavior. One special case is when there is a finite extinction time, i.e. the manifold in the Ricci-flow-with-surgery becomes the empty set at some finite time. Using his characterization of components that go extinct and analyzing the topology change caused by surgeries, Perelman gives the possible topology of a manifold whose Ricci flow has a finite extinction time.

Finite extinction time ([22]). *If a Ricci-flow-with-surgery starting from M has a finite extinction time then M is diffeomorphic to a connected sum of finite isometric quotients of the round S^3 and copies of $S^1 \times S^2$.*

In his third Ricci flow paper [23], Perelman goes further and uses minimal disk arguments to give a condition that ensures a finite extinction time; see also [5].

No aspherical factors ([23]). *If the Kneser–Milnor prime decomposition of M does not have any aspherical factors then a Ricci-flow-with-surgery starting with any initial Riemannian metric on M has a finite extinction time.*

When put together, the above two steps give the topological possibilities for a connected closed orientable 3-manifold M whose prime decomposition does not have any aspherical factors. In particular, if M is simply-connected then the above two steps say that M is diffeomorphic to a connected sum of 3-spheres, and hence is diffeomorphic to the 3-sphere.

In the general case when the Ricci-flow-with-surgery may not have a finite extinction time, the goal is to show that as time goes on, one sees the desired decomposition of the geometrization conjecture. There could be an infinite number of total surgeries. At the time of this writing it is not known whether this actually happens. Perelman had the insight that one can draw topological conclusions nevertheless.

Let M_t be a connected component of the time-t manifold. (If t is a surgery time then we consider the postsurgery manifold.) If M_t admitted any metric with nonnegative scalar curvature then it would be flat or the corresponding Ricci flow would have finite extinction time, in which case the topology is understood. So we can assume that M_t carries no metric with nonnegative scalar curvature. Consider hereafter the metric $\hat{g}(t) = \frac{1}{t}g(t)$ on M_t. Perelman defines the "thick" part of M_t as follows. Given $x \in M_t$, let the intrinsic scale $\rho(x, t)$ be the radius ρ such that $\inf_{B(x,\rho)} \mathrm{Riem} = -\rho^{-2}$, where Riem is the sectional curvature of $\hat{g}(t)$. For any $w > 0$, the *w-thick part* of M_t is given by $M^+(w, t) = \{x \in M_t : \mathrm{vol}(B(x, \rho(x, t))) > w\rho(x, t)^3\}$. It is not excluded that $M^+(w, t) = \emptyset$ or $M^+(w, t) = M_t$.

By definition, one has a lower curvature bound on the ball $B(x, \rho(x, t))$. Perelman shows by a subtle argument that for large t, if x is in the w-thick part $M^+(w, t)$ then $B(x, \rho(x, t))$ actually has an effective upper curvature bound. Adapting arguments from [13], he then shows that for any $w > 0$, as time goes on, $M^+(w, t)$ approaches the

w-thick part of a hyperbolic manifold whose cuspidal tori, if any, are incompressible in M_t. On the other hand, if w is small and x is not in the w-thick part then the ball $B(x, \rho(x,t))$ has a lower curvature bound and a relatively small volume compared to $\rho(x,t)^3$. From Perelman's earlier work in collapsing theory, he knew that 3-manifolds which are locally volume collapsed, with respect to a lower curvature bound, are graph manifolds. Putting this together, Perelman is able to achieve the remarkable feat of realizing the hyperbolic/graph dichotomy, without making any *a priori* curvature assumptions.

Hyperbolic pieces ([22]). *Given the Ricci-flow-with-surgery, there are a finite collection $\{(H_i, x_i)\}_{i=1}^k$ of complete pointed finite-volume Riemannian 3-manifolds of constant sectional curvature $-\frac{1}{4}$, a decreasing function $\alpha(t)$ tending to zero and a family of maps $f_t \colon \bigcup_{i=1}^k B\left(x_i, \frac{1}{\alpha(t)}\right) \to M_t$ such that for large t,*

1. *f_t is $\alpha(t)$-close to being an isometry.*
2. *The image of f_t contains $M^+(\alpha(t), t)$.*
3. *The image under f_t of a cuspidal torus of $\{H_i\}_{i=1}^k$ is incompressible in M_t.*

That is, for large t, the $\alpha(t)$-thick part of M_t is well approximated by the corresponding subset of $\bigcup_{i=1}^k H_i$. The remainder of M_t is highly collapsed with respect to a local lower curvature bound.

Graph manifold pieces ([22], [26]). *Let Y_t be the truncation of $\bigcup_{i=1}^k H_i$ obtained by removing horoballs at distance approximately $\frac{1}{2\alpha(t)}$ from the basepoints x_i. Then for large t, $M_t - f_t(Y_t)$ is a graph manifold.*

The above two steps, along with the fact that the components that go extinct are graph manifolds, and the fact that presurgery manifolds can be reconstructed from postsurgery manifolds via connected sums, imply the geometrization conjecture.

Grigory Perelman has revolutionized the fields of geometry and topology. His work on Ricci flow is a spectacular achievement in geometric analysis. Perelman's papers show profound originality and enormous technical skill. We will certainly be exploring Perelman's ideas for many years to come.

References

[1] Cao, H.-D., and Zhu, X.-P., A complete proof of the Poincaré and Geometrization Conjectures – application of the Hamilton-Perelman theory of the Ricci flow. *Asian J. Math.* **10** (2006), 165–492.

[2] Cheeger, J., and Gromoll, D., On the structure of complete manifolds of nonnegative curvature. *Ann. of Math.* **96** (1972), 413–443.

[3] Cheeger, J., Gromov, M., and Taylor, M., Finite propagation speed, kernel estimates for functions of the Laplace operator, and the geometry of complete Riemannian manifolds. *J. Differential Geom.* **17** (1982), 15–53.

[4] Chow, B., The Ricci flow on the 2-sphere. *J. Differential Geom.* **33** (1991), 325–334.

[5] Colding, T., and Minicozzi, W., Estimates for the extinction time for the Ricci flow on certain 3-manifolds and a question of Perelman. *J. Amer. Math. Soc.* **18** (2005), 561–569.

[6] DeTurck, D., Deforming metrics in the direction of their Ricci tensors. *J. Differential Geom.* **18** (1983), 157–162.

[7] Hamilton, R., Three-manifolds with positive Ricci curvature. *J. Differential Geom.* **17** (1982), 255–306.

[8] Hamilton, R., Four-manifolds with positive curvature operator. *J. Differential Geom.* **24** (1986), 153–179.

[9] Hamilton, R., The Ricci flow on surfaces. In *Mathematics and general relativity* (Santa Cruz, CA, 1986), Contemp. Math. 71, Amer. Math. Soc., Providence, RI, 1988, 237–262.

[10] Hamilton, R., The Harnack estimate for the Ricci flow. *J. Differential Geom.* **37** (1993), 225–243.

[11] Hamilton, R., A compactness property for solutions of the Ricci flow. *Amer. J. Math.* **117** (1995), 545–572.

[12] Hamilton, R., The formation of singularities in the Ricci flow. In *Surveys in differential geometry* (Cambridge, MA, 1993), Vol. II, Internat. Press, Cambridge, MA, 1995, 7–136.

[13] Hamilton, R., Four-manifolds with positive isotropic curvature. *Comm. Anal. Geom.* **5** (1997), 1–92.

[14] Hamilton, R., Non-singular solutions of the Ricci flow on three-manifolds. *Comm. Anal. Geom.* **7** (1999), 695–729.

[15] Ivey, T., Ricci solitons on compact three-manifolds. *Differential Geom. Appl.* **3** (1993), 301–307.

[16] Kleiner, B., and Lott, J., Notes on Perelman's papers. http://www.arxiv.org/abs/math.DG/0605667 (2006), based on earlier versions posted at http://www.math.lsa.umich.edu/research/ricciflow/perelman.html.

[17] Milnor, J., Towards the Poincaré conjecture and the classification of 3-manifolds. *Notices Amer. Math. Soc.* **50** (2003), 1226–1233.

[18] Morgan, J., and Tian, G., Ricci flow and the Poincaré conjecture. http://www.arxiv.org/abs/math.DG/0607607 (2006).

[19] Perelman, G., Proof of the soul conjecture of Cheeger and Gromoll. *J. Differential Geom.* **40** (1994), 209–212.

[20] Perelman, G., Spaces with curvature bounded below. in *Proceedings of the International Congress of Mathematicians* (Zürich, 1994), Vol. 1, Birkhäuser, Basel 1995, 517–525.

[21] Perelman, G., The entropy formula for the Ricci flow and its geometric applications. http://arxiv.org/abs/math.DG/0211159 (2002).

[22] Perelman, G., Ricci flow with surgery on three-manifolds. http://www.arxiv.org/abs/math.DG/0303109 (2003).

[23] Perelman, G., Finite extinction time for the solutions to the Ricci flow on certain three-manifolds. http://www.arxiv.org/abs/math.DG/0307245 (2003).

[24] Poincaré, H., Cinquième complément à l'analysis situs. *Rend. Circ. Math. Palermo* **18** (1904), 45–110.

[25] Shi, W.-X., Deforming the metric on complete Riemannian manifolds. *J. Differential Geom.* **30** (1989), 223–301.

[26] Shioya, T., and Yamaguchi, T., Volume collapsed three-manifolds with a lower curvature bound. *Math. Ann.* **333** (2005), 131–155.

[27] Thurston, W., Three-dimensional manifolds, Kleinian groups and hyperbolic geometry. *Bull. Amer. Math. Soc.* **6** (1982), 357–381.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1109, U.S.A.
E-mail: lott@umich.edu

Terence Tao

B.Sc. Flinders University, December 1991

Ph.D. Princeton University, June 1996

Positions until today

1996–present	University of California, Los Angeles (first as assistant professor, now full professor)
1999 and 2000	University of New South Wales
2001–2003	Clay Mathematical Institute
2001–2003	Australian National University

The work of Terence Tao

Charles Fefferman

Mathematics at the highest level has several flavors. On seeing it, one might say:

(A) What amazing technical power!

(B) What a grand synthesis!

(C) How could anyone not have seen this before?

(D) Where on earth did this come from?

The work of Terence Tao encompasses all of the above. One cannot hope to capture its extraordinary range in a few pages. My goal here is simply to exhibit a few contributions by Tao and his collaborators, sufficient to produce all the reactions (A)... (D). I shall discuss the Kakeya problem, nonlinear Schrödinger equations and arithmetic progressions of primes.

Let me start with a vignette from Tao's work on the Kakeya problem, a beautiful and fundamental question at the intersection of geometry and combinatorics. I shall state the problem, comment briefly on its significance and history, and then single out my own personal favorite result, by Nets Katz and Tao.

The original Kakeya problem was to determine the least possible area of a plane region inside which a needle of length 1 can be turned a full 360 degrees. Besicovitch and Pál showed that the area can be taken arbitrarily small.

In its modern form, the Kakeya problem is to estimate the fractal dimension of a "Besicovitch set" $E \subset \mathbb{R}^n$, i.e., a set containing line segments of length 1 in all directions.

There are several relevant notions of "fractal dimension". Here, let us use the Minkowski dimension, defined in terms of coverings of E by small balls of a fixed radius δ. The Minkowski dimension is the infimum of all β such that, for small δ, E can be covered by $\delta^{-\beta}$ balls of radius δ. We want to prove that any Besicovitch set $E \subset \mathbb{R}^n$ has Minkowski dimension at least $\beta(n)$, with $\beta(n)$ as large as possible. (Perhaps $\beta(n) = n$.)

Regarding the central importance of this problem, perhaps it is enough to say that it is intimately connected with the multiplier problem for Fourier transforms, and with the restriction of Fourier transforms to hypersurfaces; these in turn are closely connected with non-linear PDE via Strichartz estimates and their variants. There are also connections with other hard, interesting problems in combinatorics.

Let me sketch some of the history of the problem over the last 30 years. The basic result of the 1970s is that $\beta(2) = 2$. (This is due to Davies, and is closely related

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

to the early work of A. Córdoba. See [7], [8].) In the 1980s, Drury [9] showed that $\beta(n) \geq \frac{n+1}{2}$ for $n \geq 3$. (See also Christ et al [4].)

Then, about 1990, J. Bourgain and, shortly afterwards, T. Wolff discovered that Besicovitch sets of small fractal dimension have geometric structure (they contain "bouquets" and "hairbrushes"). During the 1990s, Bourgain also discovered a connection between the Kakeya problem and Gowers' work on the Balog–Szemerédi theorem from combinatorics. These insights led to small, hard-won improvements in the value of $\beta(n)$. The work looks deep and forbidding. See [1], [2], [24].

The connection with Gowers' work arises in the following result. (We write $\#(S)$ for the number of elements of a set S.)

Deep Theorem (Bourgain, using ideas from Gowers' improvement of Balog–Szemerédi). *Let A, B be subsets of an abelian group, and let $G \subset A \times B$. Assume that $\#(A)$, $\#(B)$, and $\#\{a+b : (a,b) \in G\}$ are at most N. Then $\#\{a-b : (a,b) \in G\} \leq CN^{2-1/13}$, for a universal constant C.*

The point is that one improves on the trivial bound N^2. From the Deep Theorem, one quickly obtains a result on $\beta(n)$ by slicing the set E with three parallel hyperplanes H, H', H'', with H'' halfway between H and H'.

Enter Nets Katz and Terence Tao, who proved the following result in 1999.

Little Lemma. *Under the assumptions of the Deep Theorem, we have $\#\{a-b : (a,b) \in G\} \leq CN^{2-1/6}$, for a universal constant C.*

Note that the Little Lemma is strictly sharper than the Deep Theorem, Nevertheless, its proof takes only a few pages, and can be understood by a bright high-school student. After reading the proof, one has not the faintest clue where the idea came from (see (D)).

The Little Lemma and its refinements led to the estimate $\beta(n) \geq \frac{4n+3}{7}$ for the Kakeya problem, which at the time was the best result known for $n > 8$. In high dimensions, the high-school accessible paper [18] went further than all the deep, forbidding work that came before it. Since then, there has been further progress, with Nets Katz, Izabella Łaba, and Terence Tao playing a leading rôle. The subject still looks deep and forbidding. In particular, regarding (A), let me refer the reader to the tour-de-force [17] by these authors.

Unfortunately, the complete solution to the Kakeya problem still seems far away.

Next, I shall discuss "interaction Morawetz estimates". This simple idea, with profound consequences for PDE, was discovered by the "I-Team": J. Colliander, M. Keel, G. Staffilani, H. Takaoka, and Terence Tao. Let me start with the 3D nonlinear Schrödinger equation (NLS):

$$i\partial_t u + \Delta_x u = \pm |u|^{p-1}u, \quad u(x,0) = u_0(x) \text{ given}, \tag{1}$$

where u is a complex-valued function of $(x,t) \in \mathbb{R}^3 \times \mathbb{R}$, and $p > 1$ is given.

This equation is important in physics and engineering. For instance, it describes the propagation of light in a fiber-optic cable. The behavior of solutions of (1) depends strongly on the $\pm$ sign and on the value of p. In particular, the minus sign is "focussing", and we may expect solutions of (1) to develop singularities; while the plus sign is "defocussing", and we expect solutions of (1) to spread out over large regions of space, as $t \longrightarrow \pm\infty$. In the defocussing case, the non-linear term in (1) should eventually become negligibly small, and the solution of (1) ought to behave like a solution of the (linear) free Schrödinger equation $(i\,\partial_t + \Delta_x)u = 0$. From now on, we restrict attention to the defocussing case.

We note two obvious conserved quantities for (1): the "mass" $\int_{\mathbb{R}^3} |u(x,t)|^2 dx$, and the energy,

$$E = \frac{1}{2}\int\limits_{\mathbb{R}^3} |\nabla_x u(x,t)|^2\,dx \;+\; \frac{1}{p+1}\int\limits_{\mathbb{R}^3} |u(x,t)|^{p+1}\,dx.$$

How can we prove that solutions of (1) spread out for large time? A fundamental tool is the Morawetz estimate. C. Morawetz first discovered this wonderful, simple idea for the non-linear Klein–Gordon equation. Let me describe it here for cubic 3D NLS, i.e., for equation (1) with $p = 3$. There, the Morawetz estimate asserts that

$$\int\limits_0^T \int\limits_{\mathbb{R}^3} \frac{|u(x,t)|^4}{|x|}\,dx\,dt \le C \sup_{0\le t\le T} \;\| \,(-\Delta_x)^{1/4}\,u(\cdot,\,t)\,\|^2_{L^2(\mathbb{R}^3)}, \tag{2}$$

for any $T > 0$ and any solution of (1).

The good news is that (2) instantly shows that u must eventually become small in any given bounded region of space. (If not, then the left-hand side of (2) grows linearly in T as $T \longrightarrow \infty$, while the right-hand side of (2) remains bounded, thanks to conservation of mass and energy.)

The bad news is that (2) does not rule out a scenario in which $u(x,t)$ remains concentrated near a moving center $x = x_0(t)$. The trouble is that the weight function $\frac{1}{|x|}$ is concentrated near $x = 0$, whereas $u(\cdot,t)$ may be concentrated somewhere else.

The I-Team found an amazingly simple and straightforward way to overcome the bad news. Let me sketch the idea, starting with the classic proof of (2). To derive (2), we start with the quantity

$$M_0(t) = \mathrm{Im}\int\limits_{\mathbb{R}^3} \bar{u}(x,t)\cdot\left[\frac{x}{|x|}\cdot\nabla_x\,u(x,t)\right]dx. \tag{3}$$

On one hand, $M_0(t)$ is controlled by the right-hand side of (2), when $0 \le t \le T$. On the other hand, a computation using (1) shows that

$$\frac{d}{dt}\,M_0(t) = 4\pi^2|u(0,t)|^2 + 2\int\limits_{\mathbb{R}^3} |\nabla_\Omega u(x,t)|^2\,\frac{dx}{|x|} + \int\limits_{\mathbb{R}^3}\frac{|u(x,t)|^4}{|x|}\,dx, \tag{4}$$

where ∇_Ω denotes the angular part of the gradient.

The Morawetz estimate (2) follows at once.

The I-Team simply replaced $M_0(t)$ by a weighted average of translates,

$$M(t) = \int_{\mathbb{R}^3} M_y(t)\, |u(y,t)|^2\, dy,$$

where

$$M_y(t) = \mathrm{Im} \int_{\mathbb{R}^3} \bar{u}(x,t) \cdot \left[\frac{x-y}{|x-y|} \cdot \nabla_x\, u(x,t) \right] dx.$$

This puts the greatest weight on those $y \in \mathbb{R}^3$ where $u(y,t)$ lives – an eminently sensible idea.

Starting with $M(t)$ and proceeding more or less as in the proof of the Morawetz estimate, one obtains easily the

Interaction Morawetz Estimate.

$$\int_0^T \int_{\mathbb{R}^3} |u(x,t)|^4\, dx\, dt \le C \parallel u(\cdot,0) \parallel^2_{L^2(\mathbb{R}^3)} \cdot \sup_{0 \le t \le T} \parallel (-\Delta_x)^{1/4} u(\cdot,t) \parallel^2_{L^2(\mathbb{R}^3)}. \tag{5}$$

Again, the right-hand side is bounded for large T, thanks to conservation of mass and energy. This time however, the left-hand side grows linearly in T, even if our solution is concentrated in a moving ball. The I-Team has overcome the bad news. They made it look effortless. Why did no one think of it before? (See (C).)

Observe that the right-hand side of (5) is much weaker than the energy; we need only half an x-derivative, as opposed to a full gradient. The original purpose of the interaction Morawetz estimate was to derive global existence for cubic defocussing 3D NLS in Sobolev spaces in which the energy may be infinite. That is a big achievement (see [6]), but I will not discuss it further here, except to point out that the proof involves additional ideas and formidable work.

Instead, let me say a few words about the defocussing quintic 3D NLS, i.e., the case $p = 5$ of equation (1). This equation is particularly natural and deep, because it is critical for the energy. One knows that finite-energy initial data lead to solutions for a short time, and that small-energy initial data lead to global solutions. The challenge is to prove global existence for initial data with large, finite energy.

To appreciate the difficulty of the problem, we have only to turn to the tour-de-force [3] by J. Bourgain, solving the problem in the radially symmetric case. The general case is an order of magnitude harder; a singularity can form only at the origin in the radial case, but it may form anywhere in the general case. The I-Team settled the general case using a version of the interaction Morawetz estimate for quintic NLS (with cutoffs, which unfortunately greatly complicate the analysis). This is natural, since in a sense one must overcome the same bad news as before. Their result [5] is as follows.

Theorem. *Take $p = 5$ in the defocussing case in* (1). *Then, for any finite-energy initial data u_0, there is a global solution $u(x,t)$ of NLS. If u_0 belongs to H^s with $s > 1$, then $u(\cdot, t)$ also belongs to H^s for all t. Moreover, there exist solutions $u_\pm$ of the free Schrödinger equation, such that*

$$\int_{\mathbb{R}^3} |\nabla_x (u(x,t) - u_\pm(x,t))|^2 \, dx$$

tends to zero as t tends to $\pm\infty$.

I will not try to describe their proof, except to say that they use an interaction Morawetz estimate with cutoffs, along with ideas from Bourgain [3], especially the "induction on energy", as well as other ideas that I cannot begin to describe here. The details are highly formidable; see (A).

We come now to Tao's great joint paper ([16]; see also Green [15]) with Ben Green, in which they prove the following result. Here again, $\#(S)$ denotes the number of elements of a set S.

Theorem GT. *There exist arbitrarily long arithmetic progressions of primes. More precisely, given $k \geq 3$, there exist constants $c(k) > 0$ and $N_0(k) \geq 1$, such that for any $N > N_0(k)$, we have $\#\{k$-term arithmetic progressions among the primes less than $N\} > \frac{c(k)N^2}{(\log N)^k}$.*

The lower bound here agrees in order of magnitude with a natural guess. (Green and Tao are currently working on a more precise result, with an optimal $c(k)$.)

To convey something of the range and depth of the ideas in the proof, let me start with the classic theorem of Szemerédi on sets of positive density. Here, $\mathbb{Z}_N$ denotes the cyclic group of order N.

Theorem Sz 1. *Given k and δ, we have for large enough N that any subset $E \subset \mathbb{Z}_N$ with $\#(E) > \delta \cdot N$ contains an arithmetic progression of length k.*

Szemerédi's theorem also gives a lower bound for the number of k-term progressions in E. (See [23].) It is convenient to speak of functions f rather than sets E. (One obtains Theorem Sz 1 from Theorem Sz 2 below, simply by taking f to be the indicator function of E.) Thus, Szemerédi's theorem may be rephrased as follows.

Theorem Sz 2. *Given k, δ, the following holds for large enough N. Let $f : \mathbb{Z}_N \to \mathbb{R}$, with $0 \leq f(x) \leq 1$ for all x, and with*

(1) $Av_{x \in \mathbb{Z}_N} f(x) > \delta$.

Then

(2) $Av_{x,r \in \mathbb{Z}_N} \{f(x) \cdot f(x+r) \ldots f(x+(k-1)r)\} \geq c(k,\delta) > 0$, *where $c(k,\delta)$ depends only on k, δ (and not on N or f).*

(In (1), (2) and similar formulas, "Av" denotes the mean.)

In Theorems Sz 1 and 2, δ stays fixed as N grows. If instead we could take $\delta \sim 1/\log N$, then the Green–Tao theorem would follow. However, such an improvement of Theorems Sz 1, 2 seems utterly out of reach, and may be false.

There are three very different proofs of Theorems Sz 1, 2; they are due to Szemerédi [21], Furstenberg [10], and Gowers [14]. Without doing justice to the remarkable ideas in these arguments, let me just say that Szemerédi used combinatorics, Furstenberg used ergodic theory, and Gowers used (non-linear) Fourier analysis. It is hard to see anything in common in these three proofs. In a sense, the Green–Tao paper synthesizes them all, by quoting Theorem Sz 2 and using ideas that go back to the proofs of Furstenberg and Gowers. See (B).

Green and Tao prove a powerful extension of Theorem Sz 2, in which the hypothesis $0 \le f(x) \le 1$ is replaced by $0 \le f(x) \le \nu(x)$ for a suitable non-negative weight function $\nu(x)$. The function $\nu(x)$ is assumed to satisfy three conditions, which we describe crudely here.

- $Av_{x\in\mathbb{Z}_N}\, \nu(x) = 1$.
- We assume an upper bound on the quantity

$$Av_{\vec{x}=(x_1,\ldots,x_t)\,\in\,(\mathbb{Z}_N)^t} \left\{ \prod_{i=1}^{m} \nu\left(\lambda_i(\vec{x})\right) \right\}$$

  for certain affine functions $\lambda_1, \ldots, \lambda_m : (\mathbb{Z}_N)^t \longrightarrow \mathbb{Z}_N$.
- For any $h_1, \ldots, h_m \in \mathbb{Z}_N$, we assume that

$$Av_{x\in\mathbb{Z}_N} \{\nu(x+h_1)\ldots\nu(x+h_m)\} \le \sum_{i\neq j} \tau_m(h_i - h_j),$$

  for a function $\tau_m : \mathbb{Z}_N \longrightarrow \mathbb{R}$ that satisfies

$$Av_{h\in\mathbb{Z}_N} \left\{(\tau_m(h)^q\right\} \le C(m,q)$$

  for any q.

Such a function $\nu(x)$ is called a "pseudo-random measure" by Green and Tao. Their extension of Szemerédi's theorem is as follows.

Theorem GTS (Green–Tao–Szemerédi). *Let $k, \delta > 0$, suppose N is large enough and let ν be a pseudo-random measure. Let $f : \mathbb{Z}_N \longrightarrow \mathbb{R}$, with $0 \le f(x) \le \nu(x)$, and with $Av_{x\in\mathbb{Z}_N} f(x) \ge \delta$.*

Then $Av_{x,r\in\mathbb{Z}_N} \{f(x)\cdot f(x+r)\ldots f(x+(k-1)r)\} \ge c(k,\delta) > 0$, where $c(k,\delta)$ depends on k, δ, but not on N or f.

The point is that there are pseudo-random measures $\nu(x)$ that are large on sparse subsets of $\mathbb{Z}_N$ (e.g., the primes up to N). We will return to this point.

Let me say a few words about the proof of Theorem GTS, and then afterwards describe how it applies to the primes.

It is in the proof of Theorem GTS that Szemerédi's theorem is combined with ideas from Furstenberg and Gowers.

Green and Tao break up the function f into a "uniform" and an "anti-uniform" part, $f = f_U + f_{U^\perp}$.

They expand out $Av_{x,r\in\mathbb{Z}_N}\{f(x)\cdot f(x+r)\dots f(x+(k-1)r)\}$ into a sum of terms

(3) $Av_{x,r\in\mathbb{Z}_N}\{f_0(x)\cdot f_1(x+r)\dots f_{k-1}(x+(k-1)r)\}$, where each f_i is either f_U or $f_{U^\perp}$.

The terms (3) that contain any factor f_U are $o(1)$, thanks to ideas that go back to Gowers' proof.

This leaves us with the term (3) in which each f_i is $f_{U^\perp}$. Let us call this the "critical term".

To control that term, Green and Tao partition $\mathbb{Z}_N$ into subsets $E_1, E_2, \dots, E_A$, and then define a function $\bar{f}_{U^\perp}$ on $\mathbb{Z}_N$ by averaging $f_{U^\perp}$ over each E_α. Green and Tao then prove that

(4) replacing $f_{U^\perp}$ by $\bar{f}_{U^\perp}$ makes a difference $o(1)$ in the critical term,

and moreover,

(5) $0 \le \bar{f}_{U^\perp} \le 1$ and $Av_{x\in\mathbb{Z}_N}\,\bar{f}_{U^\perp}(x) \ge \delta$.

Consequently, the classic Szemerédi theorem (Theorem Sz 2) applies to $\bar{f}_{U^\perp}$, completing the proof of the Green–Tao–Szemerédi theorem.

The proof of (4) and (5) is based on ideas that go back to Furstenberg's proof of Szemerédi's theorem.

Once the Green–Tao–Szemerédi theorem is established, one can take $f(x) = \log x$ for x prime, $f(x) = 0$ otherwise. If we can find a pseudo-random measure ν such that

(6) $0 \le f(x) \le \nu(x)$ for all x,

then Theorem GTS applies, and it yields arbitrarily long arithmetic progressions of primes as in Theorem GT. A first guess for $\nu(x)$ is the standard Von Mangoldt function $\Lambda(x) = \log p$ for $x = p^k$, p prime; $\Lambda(x) = 0$ otherwise. Λ may indeed be a pseudo-random measure, but that would be very hard to prove. Fortunately, another function ν can be seen to be a pseudo-random measure satisfying (6), thanks to important work of Goldston–Yıldırım [11], [12], [13], using not-so-hard analytic number theory.

Thus, in the end, a great theorem on the prime numbers is proven without hard analytic number theory. The difficulty lies elsewhere.

I have repeatedly used the phrase "tour-de-force"; I promise that I am not exaggerating.

There are additional first-rate achievements by Tao that I have not mentioned at all. For instance, he has set forth a program [22] for proving the global existence and regularity of wave maps, by using the heat flow for harmonic maps. This has an excellent chance to work, and it may well have important applications in general relativity. I should also mention Tao's joint work with Knutson [19] on the saturation conjecture in representation theory. It is most unusual for an analyst to solve an outstanding problem in algebra.

Tao seems to be getting stronger year by year. It is hard to imagine what can top the work he has already done, but we await Tao's future contributions with eager anticipation.

References

[1] Bourgain, J., Besicovitch-type maximal operators and applications to Fourier analysis. *Geom. Funct. Anal.* **1** (2) (1991), 147–187.

[2] Bourgain, J., On the dimension of Kakeya sets and related maximal inequalities. *Geom. Funct. Anal.* **9** (2) (1999), 256–282.

[3] Bourgain, J., Global well-posedness of defocusing 3D critical NLS in the radial case. *J. Amer. Math. Soc.* **12** (1999), 145–171.

[4] Christ, M., Duoandikoetxea, J., Rubio de Francia, J. L., Maximal operators associated to the Radon transform and the Calderón-Zygmund method of rotations. *Duke Math. J.* **53** (1986), 189–209.

[5] Colliander, J., Keel, M., Staffilani, G., Takaoka, H., Tao, T., Global well-posedness and scattering for the energy-critical nonlinear Schrödinger equation in $\mathbb{R}^3$. *Ann. of Math.*, to appear.

[6] Colliander, J., Keel, M., Staffilani, G., Takaoka, H., Tao, T., Global existence and scattering for rough solutions of a nonlinear Schrödinger equation in $\mathbb{R}^3$. *Comm. Pure Appl. Math.* **57** (8) (2004), 987–1014.

[7] Córdoba, A., The Kakeya maximal function and the spherical summation multipliers. *Amer. J. Math.* **99** (1977), 1–22.

[8] Davies, R., Some remarks on the Kakeya problem. *Proc. Cambridge Philos. Soc.* **69** (1971), 417–421.

[9] Drury, S., L^p estimates for the x-ray transform. *Illinois J. Math.* **27** (1983), 125–129.

[10] Furstenberg, H., Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.* **31** (1977), 204–256.

[11] Goldston, D., and Yıldırım, C. Y., Higher correlations of divisor sums related to primes, I: Triple correlations. *Integers* **3** (2003), A5 (electronic).

[12] Goldston, D., and Yıldırım, C. Y., Higher correlations of divisor sums related to primes, III: k-correlations. Preprint, September 2002; arXiv: math.NT/0209102.

[13] Goldston, D., and Yıldırım, C. Y., Small gaps between primes, I. Preprint, April 2005; arXiv:math.NT/0504336.

[14] Gowers, T., A new proof of Szemerédi's theorem. *Geom. Funct. Anal* **11** (2001), 465–588.

[15] Green, B., Roth's theorem in the primes. *Ann. of Math.* **161** (2005), 1609–1636.

[16] Green, B., and Tao, T., The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.*, to appear.

[17] Katz, N. H., Łaba, I., Tao, T., An improved bound on the Minkowski dimension of Besicovitch sets in $\mathbb{R}^3$. *Ann. of Math.* **152** (2000), 383–446.

[18] Katz, N. H., and Tao, T., Bounds on arithmetic projections, and applications to the Kakeya conjecture. *Math. Res. Lett.* **6** (1999), 625–630.

[19] Knutson, A., and Tao, T., The honeycomb model of $\mathrm{GL}_n(\mathbb{C})$ tensor products I: Proof of the saturation conjecture. *J. Amer. Math. Soc.* **12** (4) (1999), 1055–1090.

[20] Morawetz, C., Time decay for the nonliner Klein-Gordon equation. *Proc. Roy. Soc. Ser. A* **306** (1968), 291–296.

[21] Szemerédi, E., On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* **27** (1975), 299–345.

[22] Tao, T., Geometric renormalization of large energy wave maps. Preprint, November 2004; arXiv:math.AP/0411354.

[23] Varnavides, P., On certain sets of positive density. *J. London Math. Soc.* **34** (1959), 358–360.

[24] Wolff, T., Recent work connected with the Kakeya problem. In *Prospects in mathematics* (Princeton, NJ, 1996), Amer. Math. Soc., Providence, RI, 1999, 129–162.

Department of Mathematics, Fine Hall, Washington Road, Princeton, NJ 08544-1000, U.S.A.
E-mail: cf@math.princeton.edu

Wendelin Werner

Ph.D. Université Paris-Sud, 1993

Positions until today

1991–1993	Charge de recherche CNRS
1993–1995	European postdoctoral fellowship, University of Cambridge
1995–1997	Charge de recherche CNRS
Since 1997	Professor at the Université Paris-Sud (Orsay)

The work of Wendelin Werner

Charles M. Newman*

1. Introduction

It is my great pleasure to briefly report on some of Wendelin Werner's research accomplishments that have led to his being awarded a Fields Medal at this International Congress of Mathematicians of 2006. There are a number of aspects of Werner's work that add to my pleasure in this event. One is that he was trained as a probabilist, receiving his Ph.D. in 1993 under the supervision of Jean-François Le Gall in Paris with a dissertation concerning planar Brownian Motion – which, as we shall see, plays a major role in his later work as well. Until now, Probability Theory had not been represented among Fields Medals and so I am enormously pleased to be here to witness a change in that history.

I myself was originally trained, not in Probability Theory, but in Mathematical Physics. Werner's work, together with his collaborators such as Greg Lawler, Oded Schramm and Stas Smirnov, involves applications of Probablity and Conformal Mapping Theory to fundamental issues in Statistical Physics, as we shall discuss. A second source of pleasure is my belief that this, together with other work of recent years, represents a watershed in the interaction between Mathematics and Physics generally. Namely, mathematicians such as Werner are not only providing rigorous proofs of already existing claims in the Physics literature, but beyond that are providing quite new conceptual understanding of basic phenomena – in this case, a direct geometric picture of the intrinsically random structure of physical systems at their critical points (at least in two dimensions). One simple but important example is percolation – see Figure 1.

Permit me a somewhat more personal remark as director of the Courant Institute for the past four years. We have a scientific viewpoint, as did our predecessor institute in Göttingen – namely, that an important goal should be the elimination of artificial distinctions between the Mathematical Sciences and their applications in other Sciences – I believe Wendelin Werner's work brilliantly lives up to that philosophy.

Yet a third source of pleasure concerns the collaborative nature of much of Werner's work. Beautiful and productive mathematics can be the result of many different personal workstyles. But the highly interactive style, of which Werner, together with Lawler, Schramm and his other collaborators, is a leading exemplar, appeals to many of us as simultaneously good for the soul while leading to work stronger than the sum of its parts. It is a promising sign to see Fields Medals awarded for this style of work.

*Research partially supported by the U.S. NSF under grants DMS-01-04278 and DMS-0606696.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

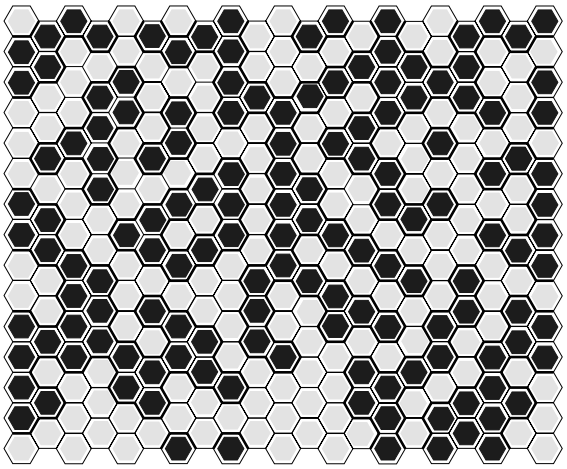


Figure 1. Finite portion of a (site) percolation configuration on the triangular lattice. Each hexagon represents a site and is assigned one of two colors. In the critical percolation model, colors are assigned randomly with equal probability. The cluster interfaces are indicated by heavy lines.

2. Brownian paths and intersection exponents

The area of Probability Theory which most strongly interacts with Statistical Physics is that involving stochastic processes with nontrivial spatial structure. This area, which also interacts with Finance, Communication Theory, Theoretical Computer Science and other fields, has long combined interesting applications with first-class Mathematics. Recent developments however have raised the perceived mathematical status of the best work from "merely" first-class to outstanding. Let me mention two pieces of Werner's work from 1998–2000. These are not only of intrinsic significance, but also were precursors to the breakthroughs about to happen in the understanding of two-dimensional critical systems with (natural) conformal invariance. (There were of course other significant precursors, such as Aizenman's path approach to scaling limits – see, e.g., [1], [2] – and Kenyon's work on loop-erased walks and domino tilings – see, e.g., [13].)

The first of these two pieces of work is a 1998 paper of Bálint Tóth and Werner [36]. The motivation was to construct a continuum version of Tóth's earlier lattice "true self-repelling walk" and this led to a quite beautiful mathematical structure (an extended version of a mostly unpublished and nearly forgotten construction done almost 20 years earlier by Arratia) of coalescing and "reflecting" one-dimensional Brownian paths, running forward and backward in time and filling up all of two-dimensional space-time. There is a (random) plane-filling curve within this structure that is analogous to one that arises in scaling limits of uniformly random spanning trees and was

one of Schramm's motivations in his 2000 paper introducing SLE [33]. SLE is an acronym for what was originally called the Stochastic Loewner Evolution and is now often called the Schramm–Loewner Evolution; more about SLE shortly.

The second piece of work consists of two papers with Lawler in 1999 and 2000 involving planar Brownian intersection exponents [25], [26]. In the second of these, it was shown that the same set of exponents must occur providing only that certain locality and conformal invariance properties are valid. This was a key idea which, combined with the introduction of SLE for the analysis of two-dimensional critical phenomena, led to a remarkable series of three papers in 2001–2002 by Lawler, Schramm and Werner [17], [18], [20] which yielded a whole series of intersection exponents.

For example, let $W^1(t)$, $W^2(t)$, ... be independent planar Brownian motions starting from distinct points at $t = 0$. Then the probability that the random curve segments $W^1([0,t]), \ldots, W^n([0,t])$ are all disjoint is $t^{-\zeta_n + o(1)}$ as $t \to \infty$ for some constant ζ_n.

Theorem 1 ([18]). *The intersection exponents ζ_n, for $n \geq 2$, are given by*

$$\zeta_n = \frac{4n^2 - 1}{24}. \tag{1}$$

This formula had been conjectured earlier by Duplantier and Kwon [12] and derived later by Duplantier [11] in a nonrigorous calculation based on two-dimensional quantum gravity. Despite the simplicity of the formula, prior to the introduction of SLE-based methods, its derivation by conventional stochastic calculus techniques appeared to be quite out of reach.

3. Conformal probability theory

The period from 2001 until the present has seen an explosion of interest in and applications of the SLE approach. To discuss this, we first give a very brief introduction to SLE; some good general references are [32], [38], [16]. For, say, a Jordan domain D in the complex plane with distinct points a, b on its boundary ∂D, and κ a positive parameter, (chordal) SLE with parameter κ, denoted SLE_κ, is a certain random continuous path (a curve, modulo monotonic reparametrization) in the closure $\overline{D}$, starting at a and ending at b. When $\kappa \leq 4$, SLE_κ is (with probability one) a simple path that only touches ∂D at a and b. Loewner, in work dating back to the 1920s [28], studied the evolution from a to b of nonrandom curves in terms of a real-valued "driving function." By conformally mapping D to the upper half plane $\mathbb{H}$ and suitably reparametrizing, one obtains (for say $\kappa \leq 4$) a simple curve $\gamma(t)$ in $\mathbb{H}$ for $t \in (0, \infty)$ and conformal mappings g_t from $\mathbb{H} \backslash \gamma([0,t])$ to $\mathbb{H}$ with g_t satisfying Loewner's evolution equation,

$$\partial_t g_t(z) = \frac{2}{g_t(z) - U(t)}, \tag{2}$$

with driving function $U(t) = g_t(\gamma(t))$. SLE_κ corresponds to the choice of $U(t)$ as the random function $B(\kappa t)$ where B is standard one-dimensional Brownian motion. When $\kappa > 4$, some modifications are necessary, but (2) remains valid – even for $\kappa \geq 8$ when the curves become plane-filling.

Now back to the SLE-based advances of the recent past. Many of these concern or were motivated by (nonrigorous) results in the Statistical Physics literature about two-dimensional critical phenomena. Critical points of physical systems typically happen at very specific values of physical parameters, such as where the vapor pressure curve in a liquid/gas system ends. Critical systems have many remarkable properties, such as random fluctuations that normally are observable only on microscopic scales manifesting themselves macroscopically. A related feature is that many quantities at or approaching the critical point have power law behavior, with the non-integer powers, known as *critical exponents* (as well as other macroscopic features, such as the scaling limits we will discuss later), believed to satisfy "universality", i.e., microscopically distinct models in the same spatial dimension should have the same exponents at their respective critical points. Two-dimensional critical systems turn out to have an additional remarkable property, which is at the heart of both the SLE approach and its predecessors in the physics literature – that is conformal invariance on the macroscopic scale.

As in the case of Brownian intersection exponents, many of the SLE-based results in two dimensions were rigorous proofs of exponent values that had been derived earlier by nonrigorous arguments – primarily those of what is known in the Physics literature as "Conformal Field Theory", which dates back to the work of Polyakov and collaborators in the 1970s and 1980s [31], [4], [5] – see also [10], [30], [9]. Other results were brand new. I'll discuss a few of these in more detail, but, as noted before, what is particularly exciting is that the SLE-based approach is not solely a rigorization of what already had existed in the physics literature but also a conceptually quite complementary approach to that of Conformal Field Theory. Werner in particular has emphasized the need to understand that complementary relationship; this has led, e.g., to a focus on the "restriction property", as in his paper about the conformally invariant measure on self-avoiding loops [39]. That paper is one example of a burgeoning interest in extending the original SLE focus on random curves to the case of random *loops*, but still with conformal invariance properties, both in the specific case of percolation scaling limits [6], [7] and in the more general contexts of Brownian "loop soups" [27], [37] and Conformal Loop Ensembles as currently being studied by Scott Sheffield and Werner.

Next are some more examples of the results obtained in the last six years or so.

4. Brownian frontier

Let $W(t)$ be a planar Brownian motion. The complement in the plane of the curve segment $W([0, t])$ is a countable union of open sets, one of which is infinite; the

boundary of that infinite component is called the Brownian frontier. As a consequence of deep relations that planar Brownian motion and its intersection exponents have with SLE_6 and its exponents (see [19], [23]), Lawler, Schramm and Werner obtained the following, proving a celebrated conjecture of Mandelbrot [29].

Theorem 2 ([21]). *The Hausdorff dimension of the planar Brownian frontier is* $4/3$.

5. Loop-erased walks

A different set of results are stated somewhat informally in the next theorem. They concern loop-erased random walks and related random objects on lattices. Unlike the percolation case discussed next, these results about continuum scaling limits, in which the lattice scale shrinks to zero, are not restricted to a particular lattice.

Theorem 3 ([24]). *Let D be* (*say*) *a Jordan domain in the plane; then the scaling limits of loop-erased random walk, the uniformly random spanning tree and the related lattice-filling curve in D are, respectively,* (*radial*) SLE_2*, a continuum "*SLE_2*-based tree" and the plane-filling* (*chordal*) SLE_8.

Scaling limits of lattice models are among the most interesting and often the most difficult results. To do them well requires the successful combination of concepts and techniques from three different areas: conformal geometry (as in the classical Löwner evolutions where the driving function is nonrandom), stochastic analysis (since for SLE the driving function is a Brownian motion), and the probability theory of lattice models (e.g., random walks or percolation or Ising models or ...). The work of Werner combines all three ingredients admirably well.

6. Percolation

Before closing, let me discuss one more example which demonstrates how these three areas can interact – scaling limits of two-dimensional critical percolation. The physics community knew (nonrigorously) the exponent values and even some geometric information in the form of specific formulas for scaling limits of crossing probabilities between boundary segments of domains. These formulas were derived by Cardy [9] following Aizenman's conjecture that they should be conformally invariant – see [15]. But there was little understanding of the scaling limit geometry of objects like cluster "interfaces" – see Figure 1.

In [33], Schramm argued that the limit of one particular interface, the "exploration path," should be SLE_6. Smirnov, for the triangular lattice, then proved [34] that (A) the crossing probabilities do converge to the conformally invariant Cardy formulas, sketched an argument as to how that could lead to (B) convergence of the whole exploration path to SLE_6 and argued further that one should be able to extend these

results to (C) a "full scaling limit" for the family of "interface loops" of all clusters. In [35], Smirnov and Werner then proved certain percolation exponents, using exploration path convergence (B), while in [22], Lawler, Schramm and Werner combined the full scaling limit (C) with percolation arguments to prove another exponent value that is stated below.

Convergence in (B) and (C) can be proved by using a considerable amount of lattice percolation machinery [6], [7], [8] – including results of Kesten, Sidoravicius and Zhang [14] about six-fold crossings of annuli and of Aizenman, Duplantier and Aharony [3] about narrow "fjords." Then the percolation exponent results of Werner and coauthors apply and provide another excellent example of how the combination of the three ingredients mentioned above work together – e.g., the next theorem proves a prediction of den Nijs and Nienhuis [10], [30].

Theorem 4 ([22]). *In critical site percolation on the triangular lattice,*

$$\textbf{Prob}[\text{cluster of origin has diameter} \geq R] = R^{-5/48+o(1)} \quad \text{as } R \to \infty\,. \tag{3}$$

7. Conclusion

I close with some comments about continuum models of Probability Theory and their relation to other areas of Mathematics which are exemplified by the work of Wendelin Werner. Traditionally, a major focus of Probability Theory, and especially so in France, has been on continuum objects such as Brownian Motion and Stochastic Calculus, with SLE and related processes as the latest continuum objects in the pantheon. Those of us raised in a different setting, such as Statistical Mechanics, sometimes regard lattice models as more "real" or "physical." But this is a narrow view. It is only the continuum models which possess extra properties, like conformal invariance in the two-dimensional setting, that relate Probability Theory to other well-developed areas of Mathematics. Such relations and interactions have become of increasing importance in recent years and will continue to do so. Even if one is primarily interested in the original lattice models, it is quite clear that their properties, such as critical exponents and critical universality, cannot be understood without a deep analysis of the continuum models that arise in the scaling limit. Thanks to the work of Wendelin Werner, his collaborators, and others, one might say that now we are all "continuistas."

References

[1] Aizenman, M., Burchard, A., Hölder regularity and dimension bounds for random curves. *Duke Math. J.* **99** (1999), 419–453.

[2] Aizenman, M., Burchard, A., Newman, C. M., Wilson, D., Scaling Limits for Minimal and Random Spanning Trees in Two Dimensions. *Random Structures Algorithms* **15** (1999), 319–367.

[3] Aizenman, M., Duplantier, B., Aharony, A., Connectivity exponents and the external perimeter in $2D$ independent percolation. *Phys. Rev. Lett.* **83** (1999), 1359–1362.

[4] Belavin, A. A., Polyakov, A. M., Zamolodchikov, A. B., Infinite conformal symmetry of critical fluctutations in two dimensions. *J. Statist. Phys.* **34** (1984), 763–774.

[5] Belavin, A. A., Polyakov, A. M., Zamolodchikov, A. B., Infinite conformal symmetry in two-dimensional quantum field theory. *Nuclear Phys. B* **241** (1984), 333–380.

[6] Camia, F., Newman, C. M., Continuum Nonsimple Loops and $2D$ Critical Percolation. *J. Statist. Phys.* **116** (2004), 157–173.

[7] Camia, F., Newman, C. M.. Two-dimensional critical percolation: the full scaling limit. *Commun. Math. Phys.* **268** (2006), 1–38.

[8] Camia, F., Newman, C. M., Critical percolation exploration path and SLE_6: a proof of convergence. *Probab. Theory Related Fields*, submitted; arXiv:math.PR/0604487.

[9] Cardy, J. L., Critical percolation in finite geometries. *J. Phys. A* **25** (1992), L201–L206.

[10] den Nijs, M., A relation between the temperature exponents of the eight-vertex and the q-state Potts model. *J. Phys. A* **12** (1979), 1857–1868.

[11] Duplantier, B., Random walks and quantum gravity in two dimensions. *Phys. Rev. Lett.* **81** (1998), 5489–5492.

[12] Duplantier, B., Kwon, K.-H., Conformal invariance and intersection of random walks. *Phys. Rev. Lett.* **61** (1988), 2514–2517.

[13] Kenyon, R., Conformal invariance of domino tiling. *Ann. Probab.* **28** (2000), 759–795.

[14] Kesten, H., Sidoravicius, V., Zhang, Y., Almost all words are seen in critical site percolation on the triangular lattice. *Electron. J. Probab.* **3** (1998), paper no. 10.

[15] Langlands, R., Pouliot, P., Saint-Aubin, Y., Conformal invariance for two-dimensional percolation. *Bull. Amer. Math. Soc.* **30** (1994), 1–61.

[16] Lawler, G., *Conformally Invariant Processes in the Plane*. Math. Surveys Monogr. 114, Amer. Math. Soc., Providence, RI, 2005.

[17] Lawler, G., Schramm, O., Werner, W., Values of Brownian intersection exponents I: Half-plane exponents. *Acta Math.* **187** (2001), 237–273.

[18] Lawler, G., Schramm, O., Werner, W., Values of Brownian intersection exponents II: Plane exponents. *Acta Math.* **187** (2001), 275–308.

[19] Lawler, G., Schramm, O., Werner, W., The dimension of the planar Brownian frontier is $4/3$. *Math. Res. Lett.* **8** (2001), 401–411.

[20] Lawler, G., Schramm, O., Werner, W., Values of Brownian intersection exponents III: Two-sided exponents. *Ann. Inst. Henri Poincaré* **38** (2002), 109–123.

[21] Lawler, G., Schramm, O., Werner, W., Analyticity of intersection exponents for planar Brownian motion. *Acta Math.* **189** (2002), 179–201.

[22] Lawler, G., Schramm, O., Werner, W., One-arm exponent for critical $2D$ percolation. *Electron. J. Probab.* **7** (2002), paper no. 2, 1–13.

[23] Lawler, G., Schramm, O., Werner, W., Conformal restriction: the chordal case. *J. Amer. Math. Soc.* **16** (2003), 917–955.

[24] Lawler, G., Schramm, O., Werner, W., Conformal invariance of planar loop-erased random walks and uniform spanning trees. *Ann. Probab.* **32** (2004), 939–995.

[25] Lawler, G., Werner, W., Intersection exponents for planar Brownian motion. *Ann. Probab.* **27** (1999), 1601–1642.

[26] Lawler, G., Werner, W., Universality for conformally invariant intersection exponents. *J. Eur. Math. Soc.* **2** (2000), 291–328.

[27] Lawler, G., Werner, W., The Brownian loop-soup. *Probab. Theory Related Fields* **128** (2004), 565–588.

[28] Löwner, K. (Loewner, C.), Untersuchungen über schlichte konforme Abbildungen des Einheitskreises, I. *Math. Ann.* **89** (1923), 103–121.

[29] B. B. Mandelbrot, *The Fractal Geometry of Nature*. Freeman, San Francisco, Calif., 1982.

[30] Nienhuis, B., Critical behavior of two-dimensional spin models and charge asymmetry in the Coulomb gas. *J. Statist. Phys.* **34** (1984), 731–761.

[31] Polyakov, A. M., Conformal symmetry of critical fluctuations. *JETP Letters* **12** (1970), 381–383.

[32] Rohde, S., Schramm, O., Basic properties of SLE. *Ann. Math.* **161** (2005), 883–924.

[33] Schramm, O., Scaling limits of loop-erased random walks and uniform spanning trees. *Israel J. Math.* **118** (2000), 221–288.

[34] Smirnov, S., Critical percolation in the plane: Conformal invariance, Cardy's formula, scaling limits. *C. R. Acad. Sci. Paris* **333** (2001), 239–244.

[35] Smirnov, S., Werner, W., Critical exponents for two-dimensional percolation. *Math. Rev. Lett.* **8** (2001), 729–744.

[36] Tóth, B., Werner, W., The true self-repelling motion. *Probab. Theory Related Fields* **111** (1998), 375–452.

[37] Werner, W., SLEs as boundaries of clusters of Brownian loops. *C. R. Acad. Sci. Paris* **337** (2003), 481–486.

[38] Werner, W., Random planar curves and Schramm-Loewner evolutions. In *Lectures on probability theory and statistics*, Lecture Notes in Math. 1840, Springer-Verlag, Berlin 2004, 107–195.

[39] Werner, W., The conformally invariant measure on self-avoiding loops. *J. Amer. Math. Soc.*, to appear; arXiv:math.PR/0511605.

Courant Institute of Mathematical Sciences, New York University, New York, NY 10012, U.S.A.

E-mail: newman@courant.nyu.edu

Jon Kleinberg

A.B. in Mathematics and Computer Science, Cornell University, 1993

Ph.D. in Computer Science, MIT, 1996

Positions until today

1996–1997	Visiting Scientist, IBM Almaden Research Center
1996–present	Faculty member, Cornell University Computer Science Department
2004–2005	Visiting Faculty, Carnegie Mellon University

The work of Jon Kleinberg

John Hopcroft

Introduction

Jon Kleinberg's research has helped lay the theoretical foundations for the information age. He has developed the theory that underlies search engines, collaborative filtering, organizing and extracting information from sources such as the World Wide Web, news streams, and the large data collections that are becoming available in astronomy, bioinformatics and many other areas. The following is a brief overview of five of his major contributions.

Hubs and authorities

In the 1960s library science developed the vector space model for representing documents [13]. The vector space model is constructed by sorting all words in the vocabulary of some corpus of documents and forming a vector space model where each dimension corresponds to one word of the vocabulary. A document is represented as a vector where the value of each coordinate is the number of times the word associated with that dimension appears in the document. Two documents are likely to be on a related topic if the angle between their vector representations is small. Early search engines relied on the vector space model to find web pages that were close to a query. Jon's work on hubs and authorities recognized that the link structure of the web provided additional information to aid in tasks such as search. His work on hubs and authorities addressed the problem of how, out of the millions of documents on the World Wide Web (WWW), you can select a small number in response to a query. Prior to 1997 search engines selected documents based on the vector space model or a variant of it. Jon's work on hubs and authorities [5] laid the foundation to rank pages based on links as opposed to word content. He introduced the notion of an authority as an important page on a topic and a hub as a page that has links to many authorities. Mathematically, an authority is a page pointed to by many hubs and a hub is a page that points to many authorities. For the concepts of hubs and authorities to be useful, one needs to develop the mathematics to identify hubs and authorities; that is, to break the cycle in the definition.

The World Wide Web can be represented as a directed graph where nodes correspond to web pages and directed edges represent links from one page to another. Let A be the adjacency matrix for the underlying web graph. Jon did a text based search

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

to find, say, the 200 most relevant web pages for a query based on word content. This set might not contain the most important web sites since, as he points out, the words "search engine" did not appear on the sites of the popular search engines in 1997, such as Alta Vista or Excite. Similarly there were over a million web sites containing the word "Harvard" but the site www.harvard.edu was not the site that contained the term "Harvard" most often. Thus, he expanded the set by adding web sites reached by either in or out links from the 200 sites. To avoid adding thousands of additional web sites when one of the web pages was extremely popular, he restricted each page in the set to add at most fifty additional pages to the original set. In the process of adding web pages, he ignored links to pages within the same domain name as these tended to be navigational links such as "top of page". In the resulting sub graph, which was now likely to contain most of the important relevant pages, he assigned weights to pages and then iteratively adjusted the weights. Actually, each page was assigned two weights, a hub weight and an authority weight. The hub weights were updated by replacing the weight of each hub with the sum of the weights of the authorities that it points to. Next the weights of the authorities were updated by replacing the weight of each authority with the sum of the hub weights pointing to it. The hub weights and the authority weights were then normalized so that the sum of the squares of each set of weights equaled one. This iterative technique converges so that the hub weights are the coordinates of the major eigenvector of AA^T and the authority weights are the coordinates of the major eigenvector of A^TA. Thus, the eigenvectors of AA^T and A^TA rank the pages as hubs and authorities. This work allowed a global analysis of the full WWW link structure to be replaced by a much more local method of analysis on a small focused sub graph.

This work is closely related to the work of Brin and Page [2] that lead to Google. Brin and Page did a random walk on the underlying graph of the WWW and computed the stationary probability of the walk. Since the directed graph has some nodes with no out degree, they had to resolve the problem of losing probability when a walk reached a node with no out going edges. Actually, they had to solve the more general problem of the probability ending up on sub graphs with no out going edges, leaving the other nodes with zero probability. The way this was resolved was that at each step the walk would jump with some small probability ε to a node selected uniformly at random and with probability $1-\varepsilon$ take a step of the random walk to an adjacent node.

Kleinberg's research on hubs and authorities has influenced the way that all major search engines rank pages today. It has also spawned an industry creating ways to help organizations get their web pages to the top of lists produced by search engines to various queries. Today there is a broad field of research in universities based on this work.

Small worlds

We are all familiar with the notion of "six degrees of separation", the notion that any two people in the world are connected by a short string of acquaintances. Stanley Milgram [12] in the sixties carried out experiments in which a letter would be given to an individual in a state such as Nebraska with instructions to get the letter to an individual in Massachusetts by mailing it to a friend known on a first name basis. The friend would be given the same instructions. The length of the path from Nebraska to Massachusetts would typically be between five and six steps.

Milgram's experiments on this inter-personal connectivity lead to a substantial research effort in the social sciences focused on the interconnections in social networks. From 1967 to 1999 this work was primarily concerned with the structure of relationships and the existence of short paths in social networks. Although the fact that individuals have the ability to actually find the short paths as was demonstrated by Milgram's original experiment, there was no work on understanding how individuals actually found the short paths or what conditions were necessary for them to do so.

In 1998 Watts and Strogatz [14] refined the concept of a small world, giving precise definitions and simple models. Their work captured the intuitive notion of a reference frame, such as the geographical location where people live or their occupation. In this reference frame, an individual is more likely to know the neighbor next door than a person in a different state. Most people know their neighbors but they also know some people who are far removed. The relationships between individuals and their neighbors were referred to as short links, and the few friends or relatives far away that the individuals knew were referred to as long-range links.

One simple model developed by Watts and Strogatz was a circular ring of nodes where each node was connected to its nearest neighbors clockwise and counterclockwise around the circle, as well as to a few randomly selected nodes that were far away. Watts and Strogatz proved that any pair of nodes is, with high probability, connected by a short path, thus justifying the terminology "small world".

Jon [6] raised the issue of how you find these short paths in a social network without creating a map of the entire social world. That is, how do you find a path using only local information? He assumed a rectangular grid with nodes connected to their four nearest neighbors, along with one random long range connection from each node. As the distance increased the probability of a long range random link connecting two nodes decreased. Jon's model captured the concept of a reference frame with different scales of resolution: neighbor, same block, same city, or same country. Jon showed that when the decrease in probability was quadratic with distance, then there exists an efficient (polynomial time) algorithm for finding a short path. If the probability decreases slower or faster, he proved the surprising result that no efficient algorithm, using only local information, could exist for finding a short path even though a short path may exist.

In Jon's model the probability of a long range edge between nodes x and y decreased as $\mathrm{dist}(x, y)^{-r}$ where $\mathrm{dist}(x, y)$ is the grid distance between nodes x and y.

For $r = 0$, the probability of a long range contact is independent of distance. In this case, the average length of such a contact is fairly long, but the long range contacts are independent of the geometry of the grid and there is no effective way to use them in finding short paths even though short paths exist. As r increases, the average length of the random long range contacts decreases but their structure starts to become useful in finding short paths. At $r = 2$ these two phenomena are balanced and one can find short paths efficiently using only local knowledge. For $r > 2$ the average length of the random long-range contact continues to decrease. Although short paths may still exist, there is no polynomial time algorithm using only local information for finding them. When r equals infinity, no long-range contacts exist and hence no short paths. What is surprising is that for $r < 2$ or for $r > 2$, no efficient algorithm using only local information exists for finding short paths.

Theorem 1. *Let G be a random graph consisting of an $n \times n$ grid plus an additional edge from each vertex u to some random vertex v where the probability of the edge (u, v) is inversely proportional to $\mathrm{dist}(u, v)^r$. Here $\mathrm{dist}(u, v)$ is the grid distance between vertices u and v. For $r = 2$, there is a decentralized algorithm so that the expected time to find a path from some start vertex s to a destination vertex t is $O(\log^2 n)$.*

Proof. At each step the algorithm selects the edge from its current location that gets it closest to its destination. The algorithm is said to be in phase j when the lattice distance from the current vertex to the destination t is in the interval $(2^j, 2^{j+1})$. Thus, there are at most $\log n$ phases. We will now prove that the expected time the algorithm remains in each phase is at most $\log n$ steps and, hence, the time to find a path is $O(\log^2 n)$.

For a fixed vertex u the probability that the long-distance edge from u goes to v is

$$\frac{d(u, v)^{-2}}{\sum_{w \neq u} d(u, w)^{-2}}.$$

We wish to get an upper bound on the denominator so as to get a lower bound on the probability of an edge of distance $d(u, v)$. Since the set of vertices at distance i from u forms a diamond centered at u with sides of length i, there are $4i$ vertices at distance i from vertex u, unless u is close to a boundary in which case there are fewer. Thus

$$\sum_{w \neq u} d(u, w)^{-2} \leq \sum_{i=1}^{2n-2} 4i \frac{1}{i^2} = 4 \sum_{i=1}^{2n-2} \frac{1}{i}.$$

For large n there exists a constant c_1 such that

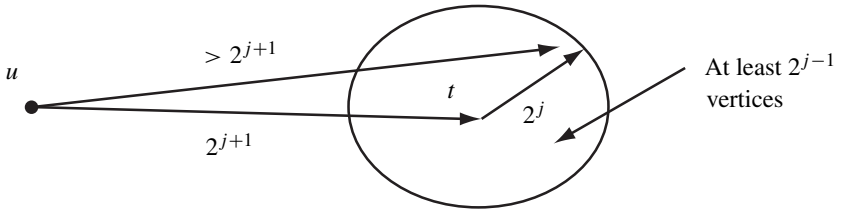
$$\sum_{w \neq u} d(u, w)^{-2} \leq c_1 \ln n.$$

It follows that there exists a constant c_2 such that each vertex that is within distance 2^j of u has probability of at least $c_2 \frac{2^{-2j}}{\ln n}$ of being the long distance contact of u.

The current step ends phase j of the algorithm if the vertex reached is within distance 2^j of the destination t. In the plane, the number of vertices at distance i from a given vertex grows linearly with i. Thus, the number of vertices within distance 2^j of the destination t is at least

$$\sum_{i=1}^{2^j} i = \frac{2^j(2^j+2)}{2} > 2^{2j-2}.$$

Since the current location is within distance 2^{j+1} of t and since there are at least 2^{2j-1} vertices within distance 2^j of t, there are at least 2^{2j-1} vertices within distance $2^{j+1} + 2^j < 2^{j+2}$ of the current location. Each of these vertices that are within distance 2^{j+2} of the current location has probability of at least $\frac{c_2}{\ln(n)2^{2j+4}}$ of being the long-distance contact.



If one of the 2^{2j-1} vertices that are within distance 2^j of t and within distance 2^{j+2} of the current location is the long-distance contact of u, it will be u's closest neighbor to t. Thus, phase j ends with probability at least

$$\frac{c_2 2^{2j-1}}{\ln(n)2^{2j+4}} = \frac{c_2}{8\ln(n)}.$$

We now bound by $\log n$ the total time spent in step j. For $j \le \log\log n$ the current vertex is distance at most $\log n$ from the destination t. Thus, even taking only local edges suffices. For $j > \log\log n$, let x_j be the number of steps spent in phase j. Then

$$E(x_j) = \sum_{i=1}^{\infty} i \,\mathrm{Prob}(x_j = i).$$

Since

$$1\,\mathrm{Prob}(x_i = 1) + 2\,\mathrm{Prob}(x_i = 2) + \cdots = \mathrm{Prob}(x_i \ge 1) + \mathrm{Prob}(x_i \ge 2) + \cdots$$

we get

$$E(x_j) = \sum_{i=1}^{\infty} \mathrm{Prob}(x_j \ge i) \le \sum_{i=1}^{\infty} \left(1 - \frac{c_2}{8\ln(n)}\right)^{i-1} = \frac{1}{1 - \left(1 - \frac{c_2}{8\ln(n)}\right)} = \frac{8\ln n}{c_2}.$$

Thus, the total number of steps is $O(\log^2 n)$. □

Even more surprising than the above result that states there exists an efficient local algorithm for finding short paths when the exponent r equals two, were Jon's additional results proving no such algorithms exist when the exponent r was either greater than two or less than two.

This research on finding paths in small worlds has found applications outside the social sciences in such areas as peer-to-peer file sharing systems. It turns out that many real sets of data have the needed quadratic decrease in probability distribution. For example, an on-line community where you measure distance between individuals by the distance between their zip codes, often has this distribution after distances are corrected for the highly nonuniform population density of the U.S. [11].

Bursts

In order to understand a stream of information, one may organize it by topic, time, or some other parameter. In many data streams a topic suddenly appears with high frequency and then dies out. The burst of activity provides a structure that can be used to identify information in the data stream. Jon's work [7] on bursts developed the mathematics to organize a data stream by bursts of activity. If one is watching a news stream and the word Katrina suddenly appears, even if one does not understand English, one recognizes that an event has taken place somewhere in the world. The question is how do you automatically detect the sudden increase in frequency of a word and distinguish the increase from a statistical fluctuation? Jon developed a model in which bursts can be efficiently detected in a statistically meaningful manner.

A simple model for generating a sequence of events is to randomly generate the events according to a distribution where the gap x between events satisfies the distribution $p(x) = \alpha e^{-\alpha x}$. Thus, the arrival rate of events is α and the expected value of the gap between events is $\frac{1}{\alpha}$. A more sophisticated model has a set of states and state transitions. Associated with each state is an event arrival rate.

In Jon's model there is an infinite number of states $q_0, q_1, \ldots$, each having an event arrival rate. State q_0 is the base state and has the base event rate $\frac{1}{g}$. Each state q_i has a rate $\alpha_i = \frac{1}{g}s^i$ where s is a scaling parameter. In state q_i there are two transitions, one to the state q_{i+1} with higher event rate and one to q_{i-1} with lower event rate. There is a cost associated with each transition to a higher event rate state. Given a sequence of events, one finds the state sequence that most closely matches the gaps with the smallest number of state transitions.

Jon applied the methodology to several data streams demonstrating that his methodology could robustly and efficiently identify bursts and thereby provide a technique to organize the underlying content of the data streams. The data streams consisted of his own email, the papers that appeared in the professional conferences, FOCS and STOC, and finally the U.S. State of the Union Addresses from 1790 to 2002. The burst analysis of Jon's email indicated bursts in traffic when conference or proposal

deadlines neared. The burst analysis of words in papers in the FOCS and STOC conferences demonstrated that the technique finds words that suddenly increased in frequency rather then finding words of high frequency over time. Most of the words indicate the emergence or sudden increase in the importance of a technical area, although some of the bursts correspond to word usage, such as the word "how" which appeared in a number of titles in the 1982 to 1988 period. The burst analysis of the U.S. State of the Union Addresses covered a 200 year time period from 1790 to 2002 and considered each word. Adjusting the scale parameter s produced short bursts of 5–10 years or longer bursts covering several decades. The bursts corresponded to national events up through 1970 at which time the frequency of bursts increased dramatically.

Table 1. Bursts in word usage in U.S. State of the Union Addresses.

energy	1812–1814	rebellion	1861–1871	Korea	1951–1954
bank	1833–1836	veterans	1925–1931	Vietnam	1951–1954
California	1848–1852	wartime	1941–1947	inflation	1971–1980
slavery	1857–1860	atomic	1947–1959	oil	1974–1981

This work on bursts demonstrated that one could use the temporal structure of data streams, such as email, click streams, or search engine queries, to organize the material as well as its content. Organizing data streams around the bursts which occur, provides us with another tool for organizing material in the information age.

Nearest neighbor

Many problems in information retrieval and clustering involve the nearest neighbor problem in a high dimensional space. A good survey of important work in this area can be found in [3]. An important algorithmic question is how to preprocess n points in d-dimensions so that given a query vector, one can find its closest neighbor. An important version of this problem is the ε-approximation nearest neighbor problem. Given a set P of vectors in d-dimensional space and a query vector x, the ε-approximation nearest neighbor problem is to find a vector y in P such that for any z in P

$$\operatorname{dist}(x, y) \leq (1 + \varepsilon) \operatorname{dist}(x, z).$$

Prior to Jon's work on nearest neighbor search in high dimensions [4], there was much research on this problem. Early work asked how one could preprocess P so as to be able to efficiently find the nearest neighbor to a query vector x. Most of the previous papers required query time exponential in the dimension d. Thus, if the dimension of the space was larger than $\log n$, there was no method faster than the brute force algorithm that uses time $O(dn)$. Jon developed an algorithm for the ε-approximation nearest neighbor problem that improved on the brute force algorithm

for all values of d. Jon's work lead to an $O((d \log^2 d)(d + \log n))$ time algorithm for the problem [4].

The basic idea is to project the set of points P onto random lines through the origin. If a point x is closer than a point y to the query q, then with probability greater than $\frac{1}{2}$, the projection of x will be closer than the projection of y to the projection of the query q. Thus, with a sufficient number of projections, the probability that x is closer to the query than y in a majority of the projections, will be true with high probability. If

$$(1 + \varepsilon)\,\mathrm{dist}(x, q) \leq \mathrm{dist}(y, q),$$

then the test will fail for a majority of projections only if a majority of the lines onto which P is projected come from an exceptional set. Using a VC-dimension argument, Jon showed that the probability of more than half the lines lying in an exceptional set is vanishingly small.

Collaborative filtering

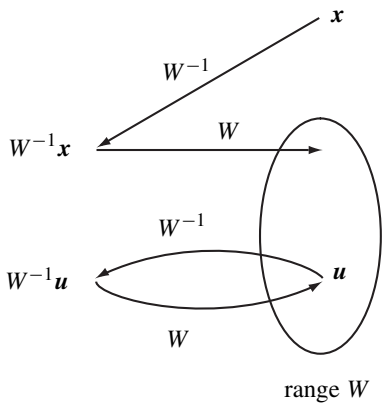
An important problem in the information age is to target a response to a person based on a small amount of information. For example, if a customer orders an item from a network store, the store may want to send him or her an advertisement based on that order. Similarly, a search engine may want to target an ad to a customer based on a query. In the case of a purchase, if for every potential item one knew the probability that the customer would buy the item, they might target an ad for the item of highest probability. However, in the case where there are possibly hundreds of thousands of items, how does one learn the probability of a customer purchasing each item based on the purchase of two or three items? If the only structure of the problem is the matrix of probabilities of customers and items, there is probably little one could do. However, if the items fall into a small number of categories and the mechanism with which a customer buys an item is that he or she first chooses a category and then having chosen a category chooses an item, one could use the structure to help in estimating the probabilities of purchasing the various items. Suppose the customer/item probability matrix is the product of a customer/category matrix times a category/item matrix. Then one can acquire information about the category/item matrix from purchases of all customers, not just the purchases of one customer.

Let A be the probability matrix of customers versus items. Then $A = PW$ where P is the probability matrix of customers versus categories and W is the probability matrix of items given a specific category. Note that the rank of A is at most the number of categories.

$$\begin{matrix} & \overset{\text{item}}{} & & \overset{\text{category}}{} & & \overset{\text{item}}{} \\ \text{customer} & \begin{pmatrix} A \end{pmatrix} & = \text{customer} & \begin{pmatrix} P \end{pmatrix} & = \text{category} & \begin{pmatrix} W \end{pmatrix} \end{matrix}$$

Suppose we know W the matrix of probabilities of items given the categories. Let $\boldsymbol{u}$ be a row of A, the vector of probabilities with which a customer selects items. Let $\tilde{\boldsymbol{u}}$ be an estimate of $\boldsymbol{u}$ obtained from s samples. That is, the ith component of the vector $\tilde{\boldsymbol{u}}$ is $\frac{1}{s}$ times the number of times the customer selected the ith item out of s selections. The question is, how close will $\tilde{\boldsymbol{u}}$ be to $\boldsymbol{u}$? Observe that $\boldsymbol{u}$ is in the range of W and that $\tilde{\boldsymbol{u}}$ most likely is not. Thus, projecting $\tilde{\boldsymbol{u}}$ onto the range of W might improve the approximation. The question is what projection should be used? The obvious projection is to project orthogonally but this is not the only possibility.

Recall that we know W. Let W' be a generalized pseudo inverse of W. For $\boldsymbol{u}$ in the range of W (a linear combination of the columns of W) $WW'\boldsymbol{u} = \boldsymbol{u}$. However, for x not in the range of W, $WW'\boldsymbol{x}$ is obviously not $\boldsymbol{x}$ but some vector in the range of W.



Applying WW' to $\tilde{\boldsymbol{u}} - \boldsymbol{u}$ we get

$$WW'(\tilde{\boldsymbol{u}} - \boldsymbol{u}) = WW'\tilde{\boldsymbol{u}} - \boldsymbol{u}.$$

We need to bound how far the projection $WW'\tilde{\boldsymbol{u}}$ can be from $\boldsymbol{u}$. What we would like is for each component of $WW'\tilde{\boldsymbol{u}}$ to be within ε of the corresponding component of $\boldsymbol{u}$ with high probability. Then, recommending the item corresponding to the largest component would be the optimal recommendation.

If the maximum element of WW' is B, then how large can any component of $WW'\tilde{\boldsymbol{u}} - \boldsymbol{u}$ be? Stated another way, how large can $v(\tilde{\boldsymbol{u}} - \boldsymbol{u})$ be for any vector $\boldsymbol{v}$ where every element of $\boldsymbol{v}$ is bounded by some constant B? Write

$$\tilde{\boldsymbol{u}} = \frac{1}{s}\sum_{i=1}^{s} \bar{\boldsymbol{u}}_i$$

where $\bar{\boldsymbol{u}}_i$ is the indicator vector for the ith selection. Then $\boldsymbol{v}^T\tilde{\boldsymbol{u}} = \frac{1}{s}\sum_{i=1}^{s} \boldsymbol{v}^T\bar{\boldsymbol{u}}_i$. The terms in the summation are independent random variables since the selections are

independent. The variance of the product of an element of v times an element of $\bar{\boldsymbol{u}}_i$ is at most $\left(\frac{B}{s}\right)^2$, and hence the variance of $\boldsymbol{v}^T\tilde{\boldsymbol{u}}$ is at most $\frac{B^2}{s}$. (Elements of $\bar{\boldsymbol{u}}_i$ have value 0 or $\frac{1}{s}$ and the maximum of v is B.) Hence, by Chebyshev's inequality, the probability that $\boldsymbol{v}^T\tilde{\boldsymbol{u}}$ will differ from its expected value by more than ε is bounded.

$$\text{Prob}(|\boldsymbol{v}^T\tilde{\boldsymbol{u}} - \boldsymbol{v}^T\boldsymbol{u}| < \frac{B^2}{\varepsilon^2 s}.$$

The above result tells us that $\boldsymbol{v}^T\tilde{\boldsymbol{u}}$ will be close to its expected value of $\boldsymbol{v}^T\boldsymbol{u}$ provided no element of $\boldsymbol{v}$ is excessively large. Thus, in projecting $\tilde{\boldsymbol{u}}$ onto the space of W we want to use a projection WW' where W' is selected so that it has no excessively large element.

This led Jon and his colleague Mark Sandler [8] to use linear programming to find a pseudo inverse in which the maximum element was bounded by $\frac{1}{\Gamma}$ where $\Gamma = \min_{\|x\|_1=1} \|W\boldsymbol{x}\|_1$. This lead to a collaborative filtering algorithm that recommends an item whose probability of being purchased by the customer is within an ε of the highest probability item with high probability. What is so important about this work is that it can be viewed as the start of a theory based on the 1-norm. Although much of the theory of approximation is based on the 2-norm and in fact approximating a matrix A by a low rank matrix A_k one can prove that the Frobenius norm of the error matrix is minimized by techniques based on the 2-norm, the error is not uniformly distributed. Furthermore, the error is strongly influenced by outliers. Use of the 1-norm is a promising approach to these problems.

Closing remarks

This brief summary covers five important research thrusts that are representative of Kleinberg's work. His web page contains many other exciting results of which I will mention three. First is his early work with Eva Tardos [9] on network routing and the disjoint paths problem. They developed a constant-factor approximation algorithm for the maximum disjoint paths problem in the two-dimensional grid graph. Given a designated set of terminal node pairs, one wants to connect as many pairs as possible by paths that are disjoint. Their algorithm extends to a larger class of graphs that generalizes the grid.

Second is his early work with Borodin, Ragahavan, Sudan and Williamson [1] on the worst-case analysis of packet-routing networks. This work presents a framework for analyzing the stability of packet-routing networks in a worst-case model without probabilistic assumptions. Here one assumes packets are injected into the network, limited only by simple deterministic rate bounds, and then shows that certain standard protocols guarantee queues remain bounded forever while other standard protocols do not.

Third is his work with Eva Tardos on classification with pairwise relationships [10]. This paper gives an algorithm for classification in the following setting: We are given a set of objects (e.g. web pages) to classify, each into one of k different types, and we have both local information about each object, as well as link information specifying that certain pairs of objects are likely to have similar types. For example, in classifying web pages by topic (or into some other categories), one may have an estimate for each page in isolation, and also know that pairs of pages joined by hyperlinks are more likely to be about similar topics.

Conclusions

Jon's work has laid a foundation for the science base necessary to support the information age. Not only is the work foundational mathematically but it has contributed to the economic growth of industries.

References

[1] Borodin, A., Kleinberg, J., Raghavan, P., Sudan, M., and Williamson, D., Adversarial queueing theory. In *Proceedings of the 28nd Annual Symposium on Theory of Computing*, 1996, 376–385.

[2] Brin, S., and Page, L., Anatomy of a Large-Scale Hypertextual Web Search Engine. In *Proceedings of the 7th International World Wide Web Conference*, 1998, 107–117.

[3] Indyk, P., Nearest Neighbors in High-dimensional Spaces. In *Handbook of Discrete and Computational Geometry* (J. E. Goodman and J. O'Rourke, eds.), 2nd edition, CRC Press, Boca Raton, FL, 2004, 877–892.

[4] Kleinberg, J., Two algorithms for nearest-neighbor search in high dimensions. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, ACM Press, New York 1997, 599–608.

[5] Kleinberg, J., Authoritative sources in a hyperlinked environment. In *Proceedings of the 9th ACM-SIAM Symposium on Discrete Algorithms*, ACM, New York 1998, 668–677.

[6] Kleinberg, J., The small-world phenomenon: An algorithmic perspective. In *Proceedings of the 32nd Annual Symposium on Theory of Computing*, ACM Press, New York 2000, 163–170.

[7] Kleinberg, J., Bursty and Hierarchical Structure in Streams. In *Proceedings of the 8th ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining*, ACM, New York 2002, 91–101.

[8] Kleinberg, J., and Sandler, M., Using Mixture Models for Collaborative Filtering. In *Proceedings of the 36th ACM Symposium on Theory of Computing*, ACM, New York 2004, 569–578.

[9] Kleinberg, J., and Tardos, E., Disjoint paths in densely embedded graphs. In *Proceedings of the 36th IEEE Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1995, 52–59.

[10] Kleinberg, J., and Tardos, E., Approximation Algorithms for Classification Problems with Pairwise Relationships: Metric Labeling and Markov Random Fields. In *Proceedings of 40th IEEE Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1999, 14–23.

[11] Liben-Nowell, D., Novak, J., Kumar, R., Raghavan, P., and Tomkins, A., Geographic routing in social networks. *Proc. Natl. Acad. Sci. USA* **102** (2005), 11623–11628.

[12] Milgram, S., The small world problem. *Psychology Today* **1** (1967), 60–67.

[13] Salton, G., *Automatic Text Processing.* Addison-Wesley, Reading, Mass., 1989.

[14] Watts, D., and Strogatz, S., Collective dynamics of small-world networks. *Nature* **393** (1998), 440–442.

Department of Computer Science, Cornell University, Ithaca, New York 14953, U.S.A.

On Kiyosi Itô's work and its impact

Hans Föllmer

About a week before the start of the International Congress, an anonymous participant in a weblog discussion of potential candidates for the Fields medals voiced his concern that there might be a bias against applied mathematics and went on to write: "*I am hoping that the Gauss prize will correct this obvious problem and they will pick someone really wonderful like Kiyosi Itô of Itô Calculus fame*". Indeed this has happened: The

Gauss Prize 2006 for Applications of Mathematics

has been awarded to Kiyosi Itô *"for laying the foundations of the theory of stochastic differential equations and stochastic analysis"*. However, in his message to the Congress Kiyosi Itô says that he considers himself a pure mathematician, and while he was delighted to receive this honor, he was also surprised to be awarded a prize for applications of mathematics. So why is the Gauss prize so appropriate in his case, and why was this anonymous discussant who obviously cares about applied mathematics so enthusiastic?

The statutes of the Gauss prize say that it is *"to be awarded for*

- *outstanding mathematical contributions that have found significant applications outside of mathematics, or*
- *achievements that made the application of mathematical methods to areas outside of mathematics possible in an innovative way"*.

My aim is to show why, on both accounts, Kiyosi Itô is such a natural choice.

Kiyosi Itô was born in 1915. The following photo was taken in 1942 when he was working in the Statistical Bureau of the Japanese Government:

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

At this time he had just achieved a major breakthrough in the theory of Markov processes. The results first appeared in 1942 in a mimeographed paper *"Differential equations determining a Markov process"* written in Japanese (Zenkoku Sizyo Sugaku Danwakai-si). English versions and further extensions of these initial results were published between 1944 and 1951 in Japan; see [24]. These papers laid the foundations of the field which later became known as stochastic analysis. A systematic account appeared in the *Memoirs of the American Mathematical Society* in 1951 under the title "*On stochastic differential equations"* [23], thanks to J. L. Doob who immediately recognized the importance of Itô's work.

What was the breakthrough all about? A Markov process is usually described in terms of the transition probabilities $P_t(x, A)$ which specify, for each state x and any time $t \geq 0$, the probability of finding the process at time t in some subset A of the state space, given that x is the initial state at time 0. These transition probabilities should satisfy the Chapman–Kolmogorov equations

$$P_{t+s}(x, A) = \int P_t(x, dy) P_s(y, A).$$

For the purpose of this exposition we limit the discussion to the special case of a diffusion process with state space $\mathbb{R}^d$. A fundamental extension theorem of Kolmogorov guarantees, for each initial state x, the existence of a probability measure P_x on the space of continuous paths

$$\Omega = C([0, \infty), \mathbb{R}^d)$$

such that the conditional probabilities governing future positions are given by the transition probabilities, i.e.,

$$P_x[X_{t+s} \in A | \mathcal{F}_t] = P_s(X_t, A).$$

Here we use the notation $X_t(\omega) = \omega(t)$ for $\omega \in \Omega$, and $\mathcal{F}_t$ denotes the σ-field generated by the path behavior up to time t. In analytical terms, the infinitesimal structure of the Markov process is described by the infinitesimal generator

$$\mathcal{L} := \lim_{t \downarrow 0} \frac{P_t - I}{t}. \tag{1}$$

In the diffusion case, this operator takes the form

$$\mathcal{L} = \frac{1}{2} \sum_{i,j=1}^{d} a_{ij}(x) \frac{\partial^2}{\partial x_i \partial x_j} + \sum_{i=1}^{d} b_i(x) \frac{\partial}{\partial x_i} \tag{2}$$

with a state-dependent diffusion matrix $a = (a_{ij})$ and a state-dependent drift vector $b = (b_i)$, and for any smooth function f the function u defined by $u(x, t) := P_t f(x)$ satisfies Kolmogorov's backward equation

$$\partial_t u = \mathcal{L} u \quad \text{on } \mathbb{R}^d \times (0, \infty). \tag{3}$$

Itô's aim was to reach a deeper understanding of the dynamics by describing the infinitesimal structure of the process in probabilistic terms. His basic idea was to

i) identify the "tangents" of the process, and to

ii) (re-) construct the process pathwise from its tangents.

At the level of stochastic processes, the role of "straight lines" is taken by processes whose increments are independent and identically distributed over time intervals of the same length. Such processes are named in honor of Paul Lévy. Kiyosi Itô had already investigated in depth the pathwise behavior of Lévy processes by proving what is now known as the Lévy–Itô decomposition [21]. In the continuous case and in dimension $d = 1$, the prototype of such a Lévy process is a Brownian motion with constant drift, whose increments have a Gaussian distribution with mean and variance proportional to the length of the time interval. This process had been introduced in 1900 by Louis Bachelier as a model for the price fluctuation on the Paris stock market, five years before Albert Einstein used the same model in connection with the heat equation. A standard Brownian motion, which starts in 0 and whose increments have zero mean and variance equal to the length of the time interval, is also named in honor of Norbert Wiener who in 1923 gave the first rigorous construction, and the corresponding measure on the space of continuous paths is usually called Wiener measure. An explicit construction of a Wiener process with time interval $[0, 1]$ can be obtained as follows: Take a sequence of independent Gaussian random variables $Y_1, Y_2, \ldots$ with mean 0 and variance 1, defined on some probability space $(\Omega, \mathcal{F}, P)$, and some orthonormal basis $(\varphi_n)_{n=1,2,\ldots}$ in $L^2[0, 1]$. Then the random series

$$W_t(\omega) = \sum_{n=1}^{\infty} Y_n(\omega) \int_0^t \varphi_n(s)\, ds$$

is uniformly convergent and thus defines a continuous curve, P-almost surely. Wiener had studied the special case of a trigonometric basis, and Lévy had simplified the computations by using the Haar functions. But the definitive proof that the construction works in full generality was given by Itô and Nisio [32] in 1968.

In the case of a diffusion it is therefore natural to say that a "tangent" of the Markov process in a state x should be an affine function of the Wiener process with coefficients depending on that state. Thus Itô was led to describe the infinitesimal behavior of the diffusion by a "stochastic differential equation" of the form

$$dX_t = \sigma(X_t)\, dW_t + b(X_t)\, dt. \tag{4}$$

In d dimensions, the Wiener process is of the form $W = (W^1, \ldots, W^d)$ with d independent standard Brownian motions, and $\sigma(x)$ is a matrix such that $\sigma(x)\sigma^T(x) = a(x)$. The second part of the program now consisted in solving the stochastic differential equation, i.e., constructing the trajectories of the Markov process in the form

$$X_t(\omega) = x + \int_0^t \sigma(X_s(\omega))\, dW_s(\omega) + \int_0^t b(X_s(\omega))\, ds. \tag{5}$$

At this point a major difficulty arose. Wiener et al. had shown that the typical path of a Wiener process is continuous but nowhere differentiable. In particular, a Brownian path is not of bounded variation and thus cannot be used as an integrator in the Lebesgue–Stieltjes sense. In order to make sense out of equation (5) it was thus necessary to introduce what is now known as the theory of "stochastic integration".

In their introduction to the *Selected Papers* [24] of Kiyosi Itô, D. Stroock and S. R. S. Varadhan write: "*Everyone who is likely to pick up this book has at least heard that there is a subject called the theory of stochastic integration and that K. Itô is the Lebesgue of this branch of integration theory* (*Paley and Wiener were its Riemann*)*"*. Wiener and Paley had in fact made a first step, using integration by parts to define the integral

$$\int_0^t \xi_s \, dW_s := \xi_t W_t - \int_0^t W_s \, d\xi_s$$

for deterministic integrands of bounded variation, and then using isometry to pass to deterministic integrands in $L^2[0,t]$. But this "Wiener integral" is no help for the problem at hand, since the integrand $\xi_t = \sigma(X_t)$ is neither deterministic nor of bounded variation. In a decisive step, Itô succeeded in giving a construction of much wider scope. Roughly speaking, he showed that the stochastic integral

$$\int_0^t \xi_s \, dW_s \approx \sum_i \xi_{t_i} (W_{t_{i+1}} - W_{t_i}) \tag{6}$$

can be defined as a limit of non-anticipating Riemann sums for a wide class of stochastic integrands $\xi = (\xi_t)$. These sums are non-anticipating in two ways. First, the integrand is evaluated at the beginning of each time interval. Secondly, the values ξ_t only depend on the past observations of the Brownian path up to time t and not on its future behavior. To carry out the construction, Kiyosi Itô used the isometry

$$E\left[\left(\int_0^t \xi_s \, dW_s\right)^2\right] = E\left[\int_0^t \xi_s^2 \, ds\right].$$

This is clearly satisfied for simple non-anticipating integrands which are piecewise constant along a fixed partition of the time axis. The appropriate class of general integrands and the corresponding stochastic integrals are obtained by taking L^2-limits on both sides. In particular the Itô integral has zero expectation, since this property obviously holds for the non-anticipating Riemann sums in (6).

Once Kiyosi Itô had introduced the stochastic integral in this way, it was clear how to define a solution of the stochastic differential equation in rigorous terms. In order to prove the existence of the solution, Itô used a stochastic version of the method of successive approximation, having first clarified the dynamic properties of stochastic integrals viewed as stochastic processes with time parameter t.

In order to complete his program, Itô had to verify that his solution of the stochastic differential equation indeed yields a pathwise construction of the given Markov

process. To do so, Itô invented a new calculus for smooth functions observed along the highly non-smooth paths of a diffusion. In particular he proved what is now known as Itô's formula. In fact there are nowadays many practioners who may not know or may not care about Lebesgue and Riemann, but who do know and do care about Itô's formula.

In 1987 Kiyosi Itô received the Wolf Prize in Mathematics. The laudatio states that "*he has given us a full understanding of the infinitesimal development of Markov sample paths. This may be viewed as Newton's law in the stochastic realm, providing a direct translation between the governing partial differential equation and the underlying probabilistic mechanism. Its main ingredient is the differential and integral calculus of functions of Brownian motion. The resulting theory is a cornerstone of modern probability, both pure and applied*". The reference to Newton stresses the fundamental character of Itô's contribution to the theory of Markov processes. Let us also mention Leibniz in order to emphasize the fundamental importance of Itô's work from another point of view. In fact Itô's approach can be seen as a natural extension of Leibniz's algorithmic formulation of the differential calculus. In a manuscript written in 1675 Leibniz argues that the whole differential calculus can be developed out of the basic product rule

$$d(XY) = XdY + YdX, \tag{7}$$

and he writes: "*Quod theorema sane memorabile omnibus curvis commune est*". In particular, this implies the rule $dX^2 = 2XdX$ and, more generally,

$$df(X) = f'(X)dX \tag{8}$$

for a smooth function f observed along the curve X. Since the 19th century we know, of course, that these rules are not "*common to all* (*continuous*) *curves*", since a continuous curve does not have to be differentiable. But it was Kiyosi Itô who discovered how these rules can be modified in such a way that they generate a highly efficient calculus for the non-differentiable trajectories of a diffusion process. In Itô's calculus, the classical rule $dX^2 = 2XdX$ is replaced by

$$dX^2 = 2XdX + d\langle X\rangle,$$

where

$$\langle X\rangle_t = \lim_n \sum_{\substack{t_i \in D_n \\ t_i < t}} (X_{t_{i+1}} - X_{t_i})^2 \tag{9}$$

denotes the quadratic variation (along dyadic partitions) of the path up to time t. Lévy had shown that a typical path of the Wiener process has quadratic variation $\langle W\rangle_t = t$. Itô proved that the solution of the stochastic differential equation (4) for $d = 1$ admits a quadratic variation of the form

$$\langle X\rangle_t = \int_0^t \sigma^2(X_s)\, ds. \tag{10}$$

He then went on to show that the behavior of a function $f \in C^2$ observed along the paths of the solution is described by the rule

$$df(X) = f'(X)dX + \frac{1}{2} f''(X)\, d\langle X\rangle, \tag{11}$$

which is now known as *Itô's formula*. Note that a continuous curve of bounded variation has quadratic variation 0, and so Itô's formula may indeed be viewed as an extension of the classical differentiation rule (8).

More generally, the classical product rule (7) becomes a special case of Itô's product rule

$$d(XY) = XdY + YdX + d\langle X, Y\rangle,$$

where $\langle X, Y\rangle$ denotes the quadratic covariation of X and Y, defined in analogy to (9) or, equivalently, by polarization:

$$\langle X, Y\rangle = \frac{1}{2}(\langle X + Y\rangle - \langle X\rangle - \langle Y\rangle).$$

For a smooth function f on $\mathbb{R}^d \times [0, \infty)$ and a continuous curve $X = (X^1, \ldots, X^d)$ such that the quadratic covariations $\langle X^i, X^j\rangle$ exist, the d-dimensional version of Itô's formula takes the form

$$df(X,t) = \nabla_x f(X,t)\, dX + f_t(X,t)\, dt + \frac{1}{2} \sum_{i,j=1}^{d} f_{x_i x_j}(X,t)\, d\langle X^i, X^j\rangle. \tag{12}$$

Let us now come back to the original task of identifying the solution of the stochastic differential equation (4) as a pathwise construction of the original Markov process. In a first step, Itô showed that the solution is indeed a Markov process. Moreover he proved that the solution has quadratic covariations of the form

$$\langle X^i, X^j\rangle_t = \int_0^t \sum_k \sigma_{i,k}(X_s)\sigma_{j,k}(X_s)\, ds.$$

Thus Itô's formula for a smooth function observed along the paths of the solution reduces to

$$df(X,t) = \nabla_x f(X,t)\sigma(X)\, dW + (\mathcal{L} + \frac{\partial}{\partial t}) f(X,t)\, dt, \tag{13}$$

where $\mathcal{L}$ is given by (2). In order to show that $\mathcal{L}$ is indeed the infinitesimal generator of the Markovian solution process, it is now enough to take a smooth function on $\mathbb{R}^d$ and to use Itô's formula in order to write

$$E_x[f(X_t) - f(X_0)] = E_x\left[\int_0^t \nabla_x f(X_s)\sigma(X_s)\, dW_s + \int_0^t \mathcal{L} f(X_s)\, ds\right].$$

Recalling that the Itô integral appearing on the right-hand side has zero expectation, dividing by t and passing to the limit, we see that the infinitesimal generator associated to the transition probabilities of the Markovian solution process as in (1) coincides with the partial differential operator $\mathcal{L}$ defined by (2). With a similar application of Itô's formula, Kiyosi Itô also showed that the solution of the stochastic differential equation satisfies Kolmogorov's backward equation (3).

This concludes our sketch of Itô's construction of Markov processes as solutions of a corresponding stochastic differential equation. Let us emphasize, however, that we have outlined the argument only in the special case of a time-homogeneous diffusion process. In fact, Kiyosi Itô himself succeeded immediately in solving the problem in full generality, including time-inhomogeneous Markov processes with jumps and making full use of his previous analysis of general Lévy processes. For a comprehensive view of the general picture we refer to D. Stroock's book *Markov Processes from K. Itô's Perspective* [46] and, of course, to Kiyosi Itô's original publications [24].

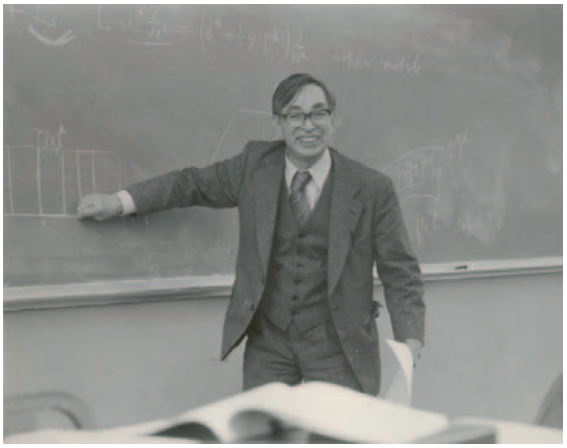
At this point let us make a brief digression to mention a parallel approach to the construction of diffusion processes which was discovered by Wolfgang Doeblin. Born in Berlin in 1915, son of the prominent Jewish writer Alfred Döblin who took his family into exile in 1933, he studied mathematics in Paris and published results on Markov chains which became famous in the fifties. It was much less known, however, that he had also worked on the probabilistic foundation of Kolmogorov's equation. In February 1940, while serving in the French army and shortly before he took his life rather than surrender himself to the German troops, Wolfgang Doeblin sent a manuscript to the Academy of Sciences in Paris as a *pli cacheté*. This sealed envelope was finally opened in May 2000. The manuscript contains a representation of the paths of the diffusion process where the stochastic integral on the right hand side of equation (5) is replaced by a time change of Brownian motion. While Doeblin's approach does not involve the theory of stochastic integration which was developed by Kiyosi Itô and which is crucial for the applications described below, it does provide an alternative solution to the pathwise construction problem, and it anticipates important developments in martingale theory related to the idea of a random time change; see Bru and Yor [4] for a detailed account of the human and scientific aspects of this startling discovery.

Over the last 50 years the impact of Itô's breakthrough has been immense, both within mathematics and over a wide range of applications in other areas. Within mathematics, this process took some time to gain momentum, at least in the West. On receiving Itô's manuscript *On stochastic differential equations*, J. L. Doob immediately recognized its importance and made sure that it was published in the *Memoirs of the AMS* in 1951. Moreover, in his book on *Stochastic processes* [9] which appeared in 1953, Doob devoted a whole chapter to Itô's construction of stochastic integrals and showed that it carries over without any major change from Brownian motion to general martingales. But when Kiyosi Itô came to Princeton in 1954, at that time a stronghold of probability theory with William Feller as the central figure, his new approach to diffusion theory did not attract much attention. Feller was mainly interested

in the general structure of one-dimensional diffusions with local generator

$$\mathcal{L} = \frac{d}{dm}\frac{d}{ds},$$

motivated by his intuition that a "one-dimensional diffusion traveler makes a trip in accordance with the road map indicated by the scale function s and with the speed indicated by the measure m"; see [30]. Together with Henry McKean, at that time a graduate student of Feller, Kiyosi Itô started to work on a probabilistic construction of these general diffusions in terms of Lévy's local time. This program was carried out in complete generality in their joint book *Diffusion Processes and Their Sample Paths* [31], a major landmark in the development of probability theory in the sixties. At that time I was a graduate student at the University of Erlangen, and when a group of us organized an informal seminar on the book of Itô and McKean we found it very hard to read. But then we were delighted to discover that Itô's own *Lectures on Stochastic Processes* [25] given at the Tata Institute were much more accessible; see also [26] and [27]. This impression was fully confirmed when Professor Itô came to Erlangen in the summer of 1968: We thoroughly enjoyed the stimulating style of his lectures as illustrated by the following photo (even though it was taken ten years later at Cornell University), and also his gentle and encouraging way of talking to the graduate students.



Ironically, however, neither stochastic integrals nor stochastic differential equations were mentioned anywhere in the book, in the Tata lecture notes, or in his talks in Erlangen.

The situation began to change in the sixties, first in the East and then in the West. G. Maruyama [40] and I. V. Girsanov [19] used stochastic integrals in order to describe the transformation of Wiener measure induced by an additional drift. First systematic expositions of stochastic integration and of stochastic differential

equations appeared in E. B. Dynkin's monograph [10] on Markov processes and, following earlier work of I. I. Gihman [16], [17] where some results of Itô had been found independently, in Gihman and Skorohod [18]. Kunita and Watanabe [34] clarified the geometry of spaces of martingales in terms of stochastic integrals. In the West, H. P. McKean published his book *Stochastic Integrals* [41] (dedicated to K. Itô) in 1969, and P. A. Meyer, C. Dellacherie, C. Doléans-Dade, J. Jacod and M. Yor started their systematic development of stochastic integration theory in the general framework of semimartingales; see, e.g. [8]. As a result, stochastic analysis emerged as one of the dominating themes of probability theory in the seventies. At the same time it began to interact increasingly with other mathematical fields. For example, J. Eells, K. D. Elworthy, P. Malliavin and others explored the idea of stochastic parallel transport presented by Kiyosi Itô at the ICM in Stockholm [28] and began to shape the new field of stochastic differential geometry; see, e.g., [12] and [13]. Connections to statistics, in particular to estimation and filtering problems for stochastic processes, were developed by R. S. Liptser and A. N. Shiryaev [35].

Infinite-dimensional extensions of stochastic analysis began to unfold in the eighties. Measure-valued diffusions and "superprocesses" arising as scaling limits of large systems of branching particles became an important area of research where the techniques of Itô calculus were crucial; see, e.g., [6], and [14]. Stochastic differential equations were studied in various infinite-dimensional settings, see, e.g., [1] and [5]. With his lectures *Foundations of Stochastic Differential Equations in Infinite Dimensional Spaces* [29], given at ETH Zurich and at Louisiana State University in 1983, Itô himself made significant contributions to this development. In fact, in his foreword to [24] Kiyosi Itô says that "*it became my habit to observe even finite-dimensional facts from the infinite-dimensional viewpoint*". Paul Malliavin developed the stochastic analysis of an infinite-dimensional Ornstein–Uhlenbeck process and showed that this approach provides powerful new tools in order to obtain regularity results for the distributions of functionals of the solutions of stochastic differential equations [37]. His ideas led to what is now known as the Malliavin calculus, a highly sophisticated methodology with a growing range of applications which emerged in the eighties and nineties as one of the most important advances of stochastic analysis; see, e.g., [38] and [42].

While the impact of Itô's ideas within mathematics took some time to become really felt, their importance was recognized early on in several areas outside of mathematics. I will briefly mention some of them in anecdotical form before I describe one case study in more detail, namely the application of Itô's calculus in finance. Already in the sixties engineers discovered that Itô's calculus provides the right concepts and tools for analyzing the stability of dynamical systems perturbed by noise and to deal with problems of filtering and control. When I was an instructor at MIT in 1969/70, stochastic analysis did not appear in any course offered in the Department of Mathematics. But I counted 4 courses in electrical engineering and 2 in aeronautics and astronautics in which stochastic differential equations played a role. The first systematic exposition in Germany was the book *Stochastische Differentialgleichungen*

[2] by Ludwig Arnold, with the motion of satellites as a prime example. It was based on seminars and lectures at the Technical University Stuttgart which he was urged to give by his colleagues in engineering. In the seventies the relevance of Itô's work was also recognized in physics and in particular in quantum field theory. When I came to ETH Zurich in 1977, Barry Simon gave a series of lectures for Swiss physicists on path integral techniques which included the construction of Itô's integral for Brownian motion, an introduction to stochastic calculus, and applications to Schrödinger operators with magnetic fields; see chapter V in [45]. When Kiyosi Itô was awarded a honorary degree by ETH Zurich in 1987, this was in fact due to a joint initiative of mathematicians and physicists. In another important development, the methods of Itô's calculus were crucial in analyzing scaling limits of models in population genetics in terms of measure-valued diffusions; see, e.g., [44] and the chapter on genetic models in [15], and [14].

I will now describe the application of Itô's calculus in finance which began around 1970 and which has transformed the field in a spectacular manner, in parallel with the explosive growth of markets for financial derivatives. Consider the price fluctuation of some liquid financial asset, modeled as a stochastic process $S = (S_t)_{0\le t\le T}$ on some probability space $(\Omega, \mathcal{F}, P)$ with filtration $(\mathcal{F}_t)_{0\le t\le T}$. Usually S is assumed to be the solution of some stochastic differential equation (4), and then the volatility of the price fluctuation as measured by the quadratic variation process $\langle X\rangle$ is governed by the state-dependent diffusion coefficient $\sigma(x)$ as described in equation (10). The best-known case is geometric Brownian motion, where the coefficients are of the form $\sigma(x) = \sigma x$ and $b(x) = bx$. This is known as the Black–Scholes model, and we will return to this special case below. In general, the choice of a specific model involves statistical and econometric considerations. But it also has theoretical aspects which are related to the idea of *market efficiency*.

In its strong form, market efficiency requires that at each time t the available information and the market's expectations are immediately "priced in". Assuming a constant interest rate r, this means that the discounted price process $X = (X_t)_{0\le t\le T}$ defined by $X_t = S_t \exp(-rt)$ satisfies the condition

$$E[X_{t+s}|\mathcal{F}_t] = X_t.$$

In other words, the discounted price process is assumed to be a *martingale* under the given probability measure P, and in this case P is called a *martingale measure* with respect to the given price process. In this strong form market efficiency has a drastic consequence: There is no way to generate a systematic gain by using a dynamic trading strategy. This follows from Itô's theory of the stochastic integral, applied to a general martingale instead of Brownian motion. Indeed, a trading strategy specifies the amount ξ_t of the underlying asset to be held at any time t. It is then natural to say that the resulting net gain at the final time T is given by Itô's stochastic integral

$$V_T = \int_0^T \xi_t \, dX_t \approx \sum_i \xi_{t_i}(X_{t_{i+1}} - X_{t_i}).$$

Note in fact that the non-anticipating construction of the Itô integral matches exactly the economic condition that each investment decision is based on the available information and is made before the future price increment is known. But if X is a martingale under the given probability measure P, as it is required by market efficiency in its strong form, then the stochastic integral inherits this property. Thus the expectation of the net gain under P is indeed given by

$$E[V_T] = 0.$$

There is a much more flexible notion of market efficiency, also known as the "absence of arbitrage opportunities". Here the existence of a trading strategy with positive expected net gain is no longer excluded. But it is assumed that there is no such profit opportunity without some downside risk, i.e.,

$$E[V_T] > 0 \Longrightarrow P[V_T < 0] \neq 0.$$

As shown by Harrison and Kreps [20], and then in much greater generality by Delbaen and Schachermayer [7], this relaxed notion of market efficiency is equivalent to the condition that the measure P, although it may not be a martingale measure itself, does admit an equivalent martingale measure $P^* \approx P$.

Equivalent martingale measures provide the key to the problem of pricing and hedging *financial derivatives*. Such derivatives, also known as *contingent claims*, are financial contracts based on the underlying price process. The resulting discounted outcome can be described as a nonnegative random variable H on the probability space $(\Omega, \mathcal{F}_T, P)$. The simplest example is a European call-option with maturity T, where $H = (X_T - c)^+$ only depends on the value of the stock price at the final time T. A more exotic example is the look-back option given by the maximal stock price observed up to time T.

For simple diffusion models such as the Black–Scholes model the equivalent martingale measure P^* is in fact unique, and in this case the financial market model is called *complete*. In such a complete situation any contingent claim H admits a unique arbitrage-free price, and this price is given by the expectation $E^*[H]$ under the martingale measure P^*. As shown by Jacod and Yor in the eighties, uniqueness of the equivalent martingale measure P^* is indeed equivalent to the fact that each contingent claim H admits a representation as a stochastic integral of the underlying price process:

$$H = E^*[H] + \int_0^T \xi_t \, dX_t. \tag{14}$$

This result may in fact be viewed as an extension of a fundamental theorem of Itô on the representation of functionals of Brownian motion as stochastic integrals. For a simple diffusion model it is actually a direct consequence of Itô's formula, as we will see below. In financial terms, the representation (14) means that the contingent claim H admits a perfect replication by means of a dynamic trading strategy, starting with

the initial capital $E^*[H]$. But this implies that the correct price is given by the initial capital, since otherwise there would be an obvious arbitrage opportunity.

In the financial context, the crucial insight that arbitrage-free prices of derivatives should be computed as expectations under an equivalent martingale measure goes back to Black and Scholes [3]. They considered the problem of pricing a European call-option of geometric Brownian motion and realized that the key to the solution is provided by Itô's formula. More generally, suppose that the price fluctuation is modeled by a stochastic differential equation (4) and that the contingent claim is of the form $H = h(X_T)$ with some continuous function h. Note first that we can rewrite Itô's formula (13) as

$$df(X,t) = \nabla_x f(X,t)\, dX + \left(\mathcal{L}^* + \frac{\partial}{\partial t}\right) f(X,t)\, dt$$

in terms of the operator $\mathcal{L}^* = \mathcal{L} - b\nabla_x$. Thus the contingent claim can be written as

$$H = f(x,0) + \int_0^T \nabla_x f(X_t,t)\, dX_t \tag{15}$$

if the function f on $\mathbb{R}^d \times [0,T]$ is chosen to be a solution of the partial differential equation

$$\left(\mathcal{L}^* + \frac{\partial}{\partial t}\right) f = 0 \tag{16}$$

with terminal condition $f(\cdot, T) = h$. The representation (15) shows that the contingent claim admits a perfect replication, or a *perfect hedge*, by means of the strategy $\xi_t = \nabla_x f(X_t, t)$. Therefore its arbitrage-free price is given by $E^*[H] = f(x,0)$. In the same way, the arbitrage-free price at any time t is given by the value $f(X_t, t)$. Thus Itô's formula provides an explicit method of computing the hedging strategy and the arbitrage-free price which involves the associated partial differential equation (16).

This approach can be extended to arbitrarily exotic derivatives. Indeed, applying the preceding argument stepwise to products of the form $H = \prod h_i(X_{t_i})$ and using an approximation of general derivatives by such finitely based functionals, one obtains the crucial representation (14) of a general contingent claim H as a stochastic integral of the underlying diffusion process. While this approach clarifies the picture from a conceptual point of view, the explicit computation of the price and the hedging strategy usually becomes a major challenge when moving beyond the simple case of a call option. At this stage additional methods of numerical analysis and of stochastic analysis may be needed. In particular, the Malliavin calculus and the analysis of "cubature on Wiener space" developed by T. Lyons have started to play an important role in this context; see, e.g., Malliavin and Thalmaier [39] and Lyons and Victoir [36].

New conceptual problems arise as soon as the financial market model becomes *incomplete*, i.e., if the martingale measure P^* is no longer unique. This happens if, for example, the driving Brownian motion in (4) is replaced by a general Lévy process as in Itô's original work, or if volatility becomes stochastic in the sense that

the diffusion coefficient σ is replaced by a stochastic process. The issue of pricing and hedging financial derivatives in such an incomplete setting has led to new optimization problems and has opened new connections to convex analysis and to microeconomic theory. It has also become the source of new directions in martingale theory. In particular it has led to new variants of some fundamental decomposition theorems such as the Kunita–Watanabe decomposition and the Doob–Meyer decomposition, and it has motivated the systematic development of the theory of backward stochastic differential equations; see, e.g., [33] and [11]. In all these ramifications, however, Itô's stochastic analysis continues to provide the crucial concepts and tools.

In the beginning we recalled the statutes of the Gauss prize. We can now see more clearly why each and every one of their requirements is so well met by Kiyosi Itô's contributions. In the first place, these contributions are outstanding and in fact of fundamental importance from a strictly mathematical point of view. Secondly, they have found significant applications outside of mathematics as illustrated by the preceding case study: There is no doubt that the field of quantitative finance has been thoroughly transformed by the basic insights provided by Itô's calculus, both on a conceptual and on a computational level. Finally, this transformation of the field has paved the way to the innovative application of a wide range of mathematical methods, not only from stochastic analysis but also, following in their wake, methods from PDE's, convex analysis, statistics, and numerical analysis.

In their introduction to [24] quoted above, Stroock and Varadhan say that Kiyosi Itô "*has molded the way in which we all think about stochastic processes"*. When this was written, *"we all"* referred to a rather small group of specialists. Over the last three decades this group has increased dramatically, both within and beyond the boundaries of mathematics. And I am sure that there is overwhelming agreement with the anonymous weblog discussant that the Gauss prize has been awarded to "*someone really wonderful"*.

References

[1] Albeverio, S., and Röckner, M., Stochastic differential equations in infinite dimensions: solutions via Dirichlet forms. *Probab. Theory Relat. Fields* **89** (1991), 347–386.

[2] Arnold, L., *Stochastische Differentialgleichungen - Theorie und Anwendung*. R. Oldenbourg Verlag, München, Wien 1973.

[3] Black, F., and Scholes, M., The Pricing of Options and Corporate Liabilities. *J. Political Econom.* **72** (1973), 637–659.

[4] Bru, B., and Yor, M., Comments on the life and mathematical legacy of Wolfgang Doeblin. *Finance Stoch.* **6** (2002), 3–47.

[5] Da Prato, G., and Röckner, M., Singular dissipative stochastic equations in Hilbert spaces. *Probab. Theory Related Fields* **124** (2002), 261–303.

[6] Dawson, D. A., Stochastic evolution equations and related measure processes. *J. Multivariate Anal.* **5** (1975), 1–52.

[7] Delbaen, F., and Schachermayer, W., A general version of the fundamental theorem of asset pricing. *Math. Ann.* **300** (1994), 463–520.

[8] Dellacherie, C., and Meyer, P. A., *Probabilités et potentiel, Ch. V-VIII: Théorie des martingales*. Hermann, Paris 1980.

[9] Doob, J. L., *Stochastic Processes*. J. Wiley, New York 1953.

[10] Dynkin, E. B., *Markov Processes I, II*. Grundlehren Math. Wiss. 121, 122, Springer-Verlag, Berlin 1965.

[11] El Karoui, N., Peng, S., Quenez, M. C., Backward Stochastic Differential Equations in Finance. *Math. Finance* **7** (1997), 1–72.

[12] Elworthy, K. D., *Stochastic Differential Equations on Manifolds*. London Math. Soc. Lecture Note Ser. 70, Cambridge University Press, Cambridge 1982.

[13] Emery , M., *Stochastic Calculus in Manifolds*. Universitext, Springer-Verlag, Berlin 1989.

[14] Etheridge, A. M., *An introduction to superprocesses*. Univ. Lecture Ser. 20, Amer. Math. Soc., Providence, RI, 2000.

[15] Ethier, S. N., and Kurtz, T. G., *Markov Processes: Characterization and Convergence*, Wiley Series in Probability and Statistics, John Wiley & Sons, Hoboken, NJ, 2005.

[16] Gihman, I. I., A method of constructing random processes. *Dokl. Akad. Nauk SSSR* **58** (1947), 961–964 (in Russian).

[17] Gihman, I. I., On the theory of differential equations of random processes. *Ukrain. Math. Zh.* **2** (4) (1950), 37–63; English transl. *Amer. Math. Soc. Transl.* (2) **1** (1955), 111–137.

[18] Gihman, I. I., and Skorohod, A. V., *Stochastic Differential Equations*. Ergeb. Math. Grenzgeb. 72, Springer-Verlag, Berlin 1972.

[19] Girsanov, I. V., On transforming a certain class of stochastic processes by absolutely continuous substitution of measures. *Theor. Probab. Appl.* **5** (1960), 285–301.

[20] Harrison, J. M., and Kreps, D. M., Martingales and arbitrage in multiperiod security markets. *J. Econom. Theory* **20** (1979), 381–408.

[21] Itô, K., On stochastic processes (infinitely divisible laws of probability). *Jap. J. Math.* **18** (1942), 261–301.

[22] Itô, K., Differential equations determining a Markov process. *J. Pan-Japan Math. Coll.* **1077** (1942); English transl. *Kiyosi Itô Selected Papers*, Springer-Verlag, 1986.

[23] Itô, K., *On stochastic differential equations*. Mem. Amer. Math. Soc. **4** (1951), 1–51.

[24] Itô, K., *Selected Papers*. Ed. by D. W. Stroock, and S. R. S. Varadhan, Springer-Verlag, New York 1986.

[25] Itô, K., *Lectures on Stochastic Processes*. Tata Institute of Fundamental Research, Bombay 1960.

[26] Itô, K., *Stochastic Processes*. Lectures given at Aarhus University, Springer-Verlag, Berlin 2004.

[27] Itô, K., *Essentials of Stochastic Processes*. Transl. Math. Monogr. 231, Amer. Math. Soc. Providence RI, 2006.

[28] Itô, K., The Brownian motion and tensor fields on Riemannian manifold. In *Proceedings of the International Congress of Mathematicians* (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 536–539.

[29] Itô, K., *Foundations of Stochastic Differential Equations in Infinite Dimensional Spaces*. CBMS-NSF Regional Conf. Ser. in Appl. Math. 47, SIAM, Philadelphia, PA, 1984.

[30] Itô, K., Memoirs of My Research on Stochastic Analysis. In *Stochastic Analysis and Applications, in Honor of Kiyosi Itô*, Proceedings of the Abel Symposium 2005 (Oslo, Norway), to appear.

[31] Itô, K., and McKean, Jr., H. P., *Diffusion Processes and Their Sample Paths*. Grundlehren Math. Wiss. 125, Springer-Verlag, Berlin 1965; Classics in Math., Springer-Verlag, Berlin 1996.

[32] Itô, K., and Nisio, M., On the convergence of sums of independent Banach space valued random variables. *Osaka J. Math.* **5** (1968), 35–48.

[33] Kramkov, D. O., Optional decomposition of supermartingales and hedging contingent claims in incomplete security markets. *Probab. Theory Relat. Fields* **105** (1996), 459–479.

[34] Kunita, H., and Watanabe, S., On square integrable martingales. *Nagoya Math. J.* **30** (1967), 209–245.

[35] Liptser, R. S., and Shiryaev, A. N., *Statistics of random processes. I General theory.* Probability Theory and Mathematical Statistics 15, Nauka, Moscow 1974; English transl.: Applications of Mathematics 5 (second revised and expanded edition), Springer-Verlag, New York 2001.

[36] Lyons, T., and Victoir, N., Cubature on Wiener space. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **460** (2041) (2004), 169–198.

[37] Malliavin, P., Stochastic calculus of variation and hypoelliptic operators. In *Proceedings of the International Symposium on Stochastic Differential Equations* (Kyoto 1976), Wiley, New York 1978, 195–263.

[38] Malliavin, P., *Stochastic Analysis*. Grundlehren Math. Wiss. 313, Springer-Verlag, Berlin 1997.

[39] Malliavin, P., and Thalmaier, A., *Stochastic Calculus of Variations in Mathematical Finance*. Springer Finance, Springer-Verlag, 2006.

[40] Maruyama, G., On the transition probability functions of the Markov process. *Nat. Sci. Rep. Ochanomizu Univ.* **5** (1954), 10–20.

[41] McKean, H. P., *Stochastic Integrals*. Probability and Mathematical Statistics 5, Academic Press, New York 1969.

[42] Nualart, D., *Malliavin Calculus and Related Topics*. Probab. Appl. (N. Y.), Springer-Verlag, New York 1995.

[43] Øksendal, B., *Stochastic differential equations*. 4th ed., Universitext, Springer-Verlag, Berlin 1995

[44] Shiga, T., Diffusion processes in population genetics. *J. Math. Kyoto Univ.* **21** (1) (1981), 133–151.

[45] Simon, B., *Functional Integration and Quantum Physics*. Pure Appl. Math. 86, Academic Press, New York 1979.

[46] Stroock, D. W., *Markov Processes from K. Itô's Perspective*, Ann. of Math. Stud. 155, Princeton University Press, Princeton, NJ, 2003.

Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin, Germany

E-mail: foellmer@math.hu-berlin.de

Universality for mathematical and physical systems

Percy Deift*

Abstract. All physical systems in equilibrium obey the laws of thermodynamics. In other words, whatever the precise nature of the interaction between the atoms and molecules at the microscopic level, at the macroscopic level, physical systems exhibit universal behavior in the sense that they are all governed by the same laws and formulae of thermodynamics. In this paper we describe some recent history of universality ideas in physics starting with Wigner's model for the scattering of neutrons off large nuclei and show how these ideas have led mathematicians to investigate universal behavior for a variety of mathematical systems. This is true not only for systems which have a physical origin, but also for systems which arise in a purely mathematical context such as the Riemann hypothesis, and a version of the card game solitaire called patience sorting.

Mathematics Subject Classification (2000). Primary 60C05; Secondary 47N30.

Keywords. Random matrices, universality, Riemann–Hilbert problems.

1. Introduction

All physical systems in equilibrium obey the laws of thermodynamics. The first law asserts the conservation of energy. The second law has a variety of formulations, one of which is the following: Suppose that in a work cycle a heat engine extracts Q_1 units of heat from a heat reservoir at temperature T_1, performs W units of work, and then exhausts the remaining $Q_2 = Q_1 - W$ units of heat to a heat sink at temperature $T_2 < T_1$. Let $\eta = \frac{W}{Q_1}$ denote the efficiency of the conversion of heat into work. Then the second law tells us there is a maximal efficiency $\eta_{\max} = (T_1 - T_2)/T_1$, depending only on T_1 and T_2, so that for all heat engines, and all work cycles,

$$\eta \leq \eta_{\max}. \tag{1}$$

Nature is so set up that we just cannot do any better.

On the other hand, it is a very old thought, going back at least to Democritus and the Greeks, that matter, all matter, is built out of tiny constituents – atoms – obeying their own laws of interaction. The juxtaposition of these two points of view, the

*The author would like to thank Sourav Chatterjee, Patrik Ferrari, Peter Sarnak and Toufic Suidan for useful comments and Irina Nenciu for her help and suggestions in preparing the manuscript. The work of the author was supported in part by DMS Grants No. 0296084 and No. 0500923, and also by a Friends of the Institute Visiting Membership at the Institute for Advanced Study in Princeton, Spring 2006.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

macroscopic world of tangible objects and the microscopic world of atoms, presents a fundamental, difficult and long-standing challenge to scientists; namely, how does one derive the macroscopic laws of thermodynamics from the microscopic laws of atoms? The special, salient feature of this challenge is that the *same* laws of thermodynamics should emerge no matter what the details of the atomic interaction. In other words, on the macroscopic scale, physical systems should exhibit universality[1]. Indeed, it is the very emergence of universal behavior for macroscopic systems that makes possible the existence of physical laws.

This kind of thinking, however, is not common in the world of mathematics. Mathematicians tend to think of their problems as sui generis, each with its own special, distinguishing features. Two problems are regarded as "the same" only if some isomorphism, explicit or otherwise, can be constructed between them. In recent years, however, universality in the above sense of macroscopic physics has started to emerge in a wide variety of mathematical problems, and the goal of this paper is to illustrate some of these developments. As we will see, there are problems from diverse areas, often with no discernible, mechanistic connections, all of which behave, on the appropriate scale, in precisely the same way. The list of such problems is varied, long and growing, and points to the emergence of what one might call "macroscopic mathematics."

A precedent for the kind of results that we are going to describe is given by the celebrated central limit theorem of probability theory, where one considers independent, identically distributed variables $\{x_n\}_{n\geq 1}$. The central limit theorem tells us that if we center and scale the variables, $x_n \to y_n \equiv \big(x_n - \mathbb{E}(x_n)\big)/\sqrt{\mathbb{V}(x_n)}$, then

$$\lim_{n\to\infty} \text{Prob}\left(\frac{\sum_{k=1}^{n} y_k}{\sqrt{n}} \leq t\right) = \int_{-\infty}^{t} e^{-\frac{u^2}{2}}\,\frac{du}{\sqrt{2\pi}}\,. \tag{2}$$

We see here explicitly that the Gaussian distribution on the right-hand side of (2) is *universal*, independent of the distribution for the x_n's. The proof of the central limit theorem for independent coin flips, $\text{Prob}(x_n = +1) = \text{Prob}(x_n = -1) = \frac{1}{2}$, goes back to de Moivre and Laplace in the 18th century. Of course (2) is only one of many similar universality-type results now known in probability theory.

The outline of the paper is as follows: In Section 2 we will introduce and discuss some models from random matrix theory (RMT). Various distributions associated with these models will play the same role in the problems that we discuss later on in the paper as the Gaussian does in (2). As noted above, thermodynamics reflects universality for all macroscopic systems, but there are also many universality subclasses which describe the behavior of physical systems in restricted situations. For example, many fluids, such as water and vinegar, obey the Navier–Stokes equation, but a variety of heavy oils obey the lubrication equations. In the same way we will see

[1] In physics, the term "universality" is usually used in the more limited context of scaling laws for critical phenomena. In this paper we use the term "universality" more broadly in the spirit of the preceding discussion. We trust this will cause no confusion.

that certain mathematical problems are described by so-called Unitary Ensembles of random matrices, and others by so-called Orthogonal or Symplectic Ensembles. In Section 3, we present a variety of problems from different areas of mathematics, and in Section 4 we show how these problems are described by random matrix models from Section 2. In the final Section 5 we discuss briefly some of the mathematical methods that are used to prove the results in Section 4. Here combinatorial identities, Riemann–Hilbert problems (RHP's) and the nonlinear steepest descent method of [DeiZho], as well as the classical steepest descent method, play a key role. We end the section with some speculations, suggesting how to place the results of Sections 3 and 4 in a broader mathematical framework.

2. Random matrix models

There are many ensembles of random matrices that are of interest, and we refer the reader to the classic text of Mehta [Meh] for more information (see also [Dei1]). In this paper we will consider almost exclusively (see, however, (54) et seq. below) only three kinds of ensembles:

(a) Orthogonal Ensembles (OE's) consisting of $N \times N$ real symmetric matrices M, $M = \bar{M} = M^T$.

(b) Unitary Ensembles (UE's) consisting of $N \times N$ Hermitian matrices M, $M = M^*$.

(c) Symplectic Ensembles (SE's) consisting of $2N \times 2N$ Hermitian, self-dual matrices $M = M^* = JM^TJ^T$, where J is the standard $2N \times 2N$ block diagonal symplectic matrix, $J = \mathrm{diag}(\tau, \tau, \ldots, \tau)$, $\tau = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

For reasons that will soon become clear, OE's, UE's and SE's are labeled by a parameter β, where $\beta = 1, 2$ or 4, respectively. In all three cases the ensembles are equipped with probability distributions of the form

$$P_{N,\beta}(M)\, d_\beta M = \frac{1}{Z_{N,\beta}} e^{-\mathrm{tr}\left(V_{N,\beta}(M)\right)}\, d_\beta M \tag{3}$$

where $V_{N,\beta}$ is a real-valued function on $\mathbb{R}$ such that $V_{N,\beta}(x) \to +\infty$ sufficiently rapidly as $|x| \to \infty$, $Z_{N,\beta}$ is a normalization coefficient, and $d_\beta M$ denotes Lebesgue measure on the algebraically independent entries of M. For example, in the orthogonal case, $d_{\beta=1}M = \prod_{1 \le j \le k \le N} dM_{jk}$, where $M = (M_{jk})$ (see, e.g. [Meh]). The notation "orthogonal", "unitary", and "symplectic" refers to the fact that the above ensembles with associated distributions (3) are invariant under conjugation $M \to SMS^{-1}$, where S is orthogonal, unitary, or unitary-symplectic (i.e., $S \in \mathrm{USp}(2N) = \{S : SS^* = I,\ SJS^T = J\}$) respectively. When $V_{N,\beta}(x) = x^2$, one has the so-called Gaussian Orthogonal Ensemble (GOE), the Gaussian Unitary Ensemble (GUE), and the Gaussian Symplectic Ensemble (GSE), for $\beta = 1, 2$ or 4, respectively.

The distributions (3) in turn give rise to distributions on the eigenvalues $\lambda_1 \leq \lambda_2 \leq \cdots$ of M,

$$\hat{P}_{N,\beta}(\lambda)\, d^N\lambda = \frac{1}{\hat{Z}_{N,\beta}} e^{-\eta_\beta \sum_{i=1}^N V_{N,\beta}(\lambda_i)} \prod_{1\leq i<j\leq N} |\lambda_i - \lambda_j|^\beta \, d\lambda_1 \cdots d\lambda_N \qquad (4)$$

where $\hat{Z}_{N,\beta}$ is again a normalization coefficient, and $\eta_\beta = 1$ if $\beta = 1$ or 2 and $\eta_4 = 2$ (this is because the eigenvalues for $\beta = 4$ double up). The labeling of OE's, UE's, and SE's by $\beta = 1, 2$ and 4 is now clear. In all three cases, we see that the random matrix ensembles give rise to random particle systems $\{\lambda_1, \lambda_2, \dots\}$ with *repulsion* built in: the probability that two eigenvalues are close together is small and vanishes like a power of the distance between them. This is an essential feature of random matrix ensembles, in contrast to random Poisson particle systems, say, where the particles may bunch together or exhibit large gaps.

Loosely speaking, we say that a system is *modeled by random matrix theory (RMT) if it behaves statistically like the eigenvalues of a "large" OE, UE,...matrix*. In analyzing such systems there is something known as the *standard procedure*: Suppose we wish to compare some statistical quantities $\{a_k\}$ in the neighborhood of some point A with the eigenvalues $\{\lambda_k\}$ of some matrix in the neighborhood of some energy E, say, in the bulk of the spectrum. Then we always *center* and *scale* the a_k's and the λ_k's,

$$a_k \to \tilde{a}_k = \gamma_a(a_k - A), \quad \lambda_k \to \tilde{\lambda}_k = \gamma_\lambda(\lambda_k - E) \qquad (5)$$

so that

$$\mathbb{E}\big(\#\{\tilde{a}_k\text{'s per unit interval}\}\big) = \mathbb{E}\big(\#\{\tilde{\lambda}_k\text{'s per unit interval}\}\big) = 1. \qquad (6)$$

For energies E at the edge of the spectrum, the above procedure must be modified slightly (see below).

This procedure can be viewed as follows: A scientist wishes to investigate some statistical phenomenon. What s'he has at hand is a microscope and a handbook of matrix ensembles. The data $\{a_k\}$ are embedded on a slide which can be inserted into the microscope. The only freedom that the scientist has is to center the slide, $a_k \to a_k - A$, and then adjust the focus $a_k - A \to \tilde{a}_k = \gamma_a(a_k - A)$ so that on average one data point $\tilde{a}_k$ appears per unit length on the slide. At that point the scientist takes out his'r handbook, and then tries to match the statistics of the $\tilde{a}_k$'s with those of the eigenvalues of some ensemble. If the fit is good, the scientist then says that the system is well-modeled by RMT.

It is a remarkable fact, going back to the work of Gaudin and Mehta, and later Dyson, in the 1960s, that the key statistics for OE's, UE's, and SE's can be computed in closed form. This is true not only for finite N, but also for various scaling limits as $N \to \infty$. For GOE, GUE, and GSE we refer the reader to [Meh]. Here the Hermite polynomials, which are orthogonal with respect to the weight $e^{-x^2}\, dx$ on $\mathbb{R}$, play

a critical role, and the scaling limits as $N \to \infty$ follow from the known, classical asymptotics of the Hermite polynomials. For UE's with general potentials $V_{N,\beta=2}$, the techniques described in [Meh] for GUE go through for finite N, the role of the Hermite polynomials now being played by the polynomials orthogonal with respect to the weight $e^{-V_{N,\beta=2}(x)}\,dx$ on $\mathbb{R}$ (see, e.g. [Dei1]). For general $V_{N,\beta=2}$, however, the asymptotic behavior of these polynomials as $N \to \infty$ does not follow from classical estimates. In order to overcome this obstacle, the authors in [DKMVZ1] and [DKMVZ2] (see also [Dei1] for a pedagogical presentation) used the Riemann–Hilbert steepest-descent method introduced by Deift and Zhou [DeiZho], and further developed with Venakides [DVZ], to compute the asymptotics as $N \to \infty$ of the orthogonal polynomials for a very general class of analytic weights. In view of the preceding comments, the scaling limits of the key statistics for UE's then follow for such weights (see also [BleIts] for the special case $V_{N,\beta=2}(x) = N(x^4 - tx^2)$). For another approach to UE universality, see [PasSch]. For OE's and SE's with classical weights, such as Laguerre, Jacobi, etc., for which the asymptotics of the associated orthogonal polynomials are known, the GOE and GSE methods in [Meh] apply (see the introductions to [DeiGio1] and [DeiGio2] for a historical discussion). For general $V_{N,\beta}$, $\beta = 1$ or 4, new techniques are needed, and these were introduced, for finite N, by Tracy and Widom in [TraWid2] and [Wid]. In [DeiGio1] and [DeiGio2], the authors use the results in [TraWid2] and [Wid], together with the asymptotic estimates in [DKMVZ2], to compute the large N limits of the key statistics for OE's and SE's with general polynomial weights $V_{N,\beta}(x) = \kappa_{2m}x^{2m} + \cdots$, $\kappa_{2m} > 0$.

It turns out that not only can the statistics for OE's, UE's and SE's be computed explicitly, but in the large N limit the behavior of these systems is universal in the sense described above, as conjectured earlier by Dyson, Mehta, Wigner, and many others. It works like this: Consider $N \times N$ matrices M in a UE with potential $V_{N,2}$. Let K_N denote the finite rank operator with kernel

$$K_N(x, y) = \sum_{j=0}^{N-1} \varphi_j(x)\varphi_j(y), \quad x, y \in \mathbb{R} \tag{7}$$

where

$$\varphi_j(x) = p_j(x)e^{-\frac{1}{2}V_{N,2}(x)}, \quad j \geq 0 \tag{8}$$

and

$$p_j(x) = \gamma_j x^j + \cdots, \quad j \geq 0,\ \gamma_j > 0 \tag{9}$$

are the orthonormal polynomials with respect to the weight $e^{-V_{N,2}(x)}\,dx$,

$$\int_{\mathbb{R}} p_j(x)\,p_k(x)e^{-V_{N,2}(x)}\,dx = \delta_{jk}, \quad j, k \geq 0.$$

Then the m-point correlation functions

$$R_m(\lambda_1, \ldots, \lambda_m) \equiv \frac{N!}{(N-m)!}\int\cdots\int \hat{P}_{N,2}(\lambda_1, \ldots, \lambda_N)\,d\lambda_{m+1}\cdots d\lambda_N$$

can be expressed in terms of K_N as follows:

$$R_m(\lambda_1, \ldots, \lambda_m) = \det\big(K_N(\lambda_i, \lambda_j)\big)_{1 \le i,j \le m}. \tag{10}$$

A simple computation for the 1-point and 2-point functions, $R_1(\lambda)$ and $R_2(\lambda_1, \lambda_2)$, shows that

$$\mathbb{E}\big(\#\{\lambda_i \in B\}\big) = \int_B R_1(\lambda)\, d\lambda \tag{11}$$

for any Borel set $B \subset \mathbb{R}$, and

$$\mathbb{E}\big(\#\{\text{ordered pairs } (i, j),\ i \neq j\ :\ (\lambda_i, \lambda_j) \in \Delta\}\big) = \iint_\Delta R_2(\lambda_1, \lambda_2)\, d\lambda_1 d\lambda_2 \tag{12}$$

for any Borel set $\Delta \subset \mathbb{R}^2$.

It follows in particular from (11) that, for an energy E, $R_1(E) = K_N(E, E)$ is the density of the expected number of eigenvalues in a neighborhood of E, and hence, by the standard procedure, one should take the scaling factor γ_λ in (5) to be $K_N(E, E)$. For energies E in the bulk of the spectrum, one finds for a broad class of potentials $V_{N,2}$ (see [DKMVZ1] and [DKMVZ2]) that, in the scaling limit dictated by $K_N(E, E)$, $K_N(\lambda, \lambda')$ takes on a universal form

$$\lim_{N\to\infty} \frac{1}{K_N(E, E)}\, K_N\left(E + \frac{x}{K_N(E, E)}, E + \frac{y}{K_N(E, E)}\right) = K_\infty(x - y) \tag{13}$$

where $x, y \in \mathbb{R}$ and K_∞ is the so-called *sine-kernel*,

$$K_\infty(u) = \frac{\sin(\pi u)}{\pi u}. \tag{14}$$

Inserting this information into (10) we see that the scaling limit for R_m is universal for each $m \ge 2$, and in particular for $m = 2$, we have for $x, y \in \mathbb{R}$

$$\begin{aligned} \lim_{N\to\infty} \frac{1}{\big(K_N(E, E)\big)^2}\, R_2\left(E + \frac{x}{K_N(E, E)}, E + \frac{y}{K_N(E, E)}\right) \\ = \det\begin{pmatrix} K_\infty(0) & K_\infty(x - y) \\ K_\infty(x - y) & K_\infty(0) \end{pmatrix} \\ = 1 - \left(\frac{\sin \pi(x - y)}{\pi(x - y)}\right)^2. \end{aligned} \tag{15}$$

For a Borel set $B \subset \mathbb{R}$, let $n_B = \#\{\lambda_j\ :\ \lambda_j \in B\}$ and let

$$\mathbb{V}_B = \mathbb{E}\big(n_B - \mathbb{E}(n_B)\big)^2 \tag{16}$$

denote the number variance in B. A simple computation again shows that

$$\mathbb{V}_B = \int_B R_1(x)\, dx + \iint_{B\times B} R_2(x, y)\, dxdy - \left(\int_B R_1(x)\, dx\right)^2.$$

For an energy E in the bulk of the spectrum as above, set

$$B_N(s) = \left(E - \frac{s}{2K_N(E,E)}, E + \frac{s}{2K_N(E,E)}\right), \quad s > 0.$$

For such B, $\mathbb{V}_B$ is the number variance for an interval about E of scaled size s. Recalling that $K_N(E,E) = R_1(E)$, and using (15), we find as $N \to \infty$

$$\lim_{N\to\infty} \mathbb{V}_{B_N(s)} = \frac{1}{\pi^2}\int_0^{2\pi s} \frac{1-\cos u}{u}\,du + \frac{2s}{\pi}\int_{\pi s}^{\infty}\left(\frac{\sin u}{u}\right)^2 du. \tag{17}$$

For large s, the right-hand side has the form (see [Meh])

$$\frac{1}{\pi^2}\big(\log(2\pi s) + \gamma + 1\big) + O\Big(\frac{1}{s}\Big) \tag{18}$$

where γ is Euler's constant.

For $\theta > 0$, the so-called *gap probability*

$$G_{N,2}(\theta) = \mathrm{Prob}\big(M \,:\, M \text{ has no eigenvalues in } (E-\theta, E+\theta)\big) \tag{19}$$

is given by (see [Meh], and also [Dei1])

$$G_{N,2}(\theta) = \det\big(1 - K_N\restriction_{L^2(E-\theta,E+\theta)}\big) \tag{20}$$

where $K_N\restriction_{L^2(E-\theta,E+\theta)}$ denotes the operator with kernel (7) acting on $L^2(E-\theta, E+\theta)$. In the bulk scaling limit, we find

$$\lim_{N\to\infty} G_{N,2}\left(\frac{x}{K_N(E,E)}\right) = \det\big(1 - K_\infty\restriction_{L^2(E-\theta,E+\theta)}\big), \quad x \in \mathbb{R}. \tag{21}$$

In terms of the scaled eigenvalues $\tilde{\lambda}_j = K_N(E,E)\cdot(\lambda_j - E)$, this means that for $x > 0$

$$\lim_{N\to\infty} \mathrm{Prob}\big(M \,:\, \tilde{\lambda}_j \notin (-x,x),\ 1 \le j \le N\big) = \det\big(1 - K_\infty\restriction_{L^2(-x,x)}\big). \tag{22}$$

Now consider a point E, say $E = 0$, where $K_N(E,E) = K_N(0,0) \to \infty$ as $N \to \infty$. This is true, in particular, if

$$V_{N,2}(x) = \kappa_m x^{2m} + \cdots, \quad \kappa_m > 0,\ m \ge 1, \tag{23}$$

and so for $V_{N,2}(x) = x^2$ (GUE). For such $V_{N,2}$'s, we have $K_N(0,0) \sim N^{1-\frac{1}{2m}}$ (see [DKMVZ1]). Let $t_N > 0$ be such that

$$t_N \to \infty, \quad \frac{t_N}{K_N(0,0)} \to 0. \tag{24}$$

Then

$$\hat{N} \equiv \mathbb{E}\left(\#\left\{|\lambda_j| \le \frac{t_N}{K_N(0,0)}\right\}\right) = \int_{-\frac{t_N}{K_N(0,0)}}^{\frac{t_N}{K_N(0,0)}} K_N(\lambda,\lambda)\,d\lambda \sim 2t_N \to \infty. \tag{25}$$

For $a < b$, define the Borel set $\Delta_N \subset \mathbb{R}^2$ by

$$\Delta_N = \left\{(x,y) : \frac{a}{K_N(0,0)} < x - y < \frac{b}{K_N(0,0)} \text{ and } |x|, |y| \le \frac{t_N}{K_N(0,0)}\right\}. \tag{26}$$

Then we have by (12) and (15), as $N \to \infty$,

$$\begin{aligned}
&\frac{1}{\hat{N}}\mathbb{E}\big(\#\{\text{ordered pairs } (i,j),\ i \ne j\ :\ (\lambda_i,\lambda_j) \in \Delta_N\}\big)\\
&\quad = \frac{1}{\hat{N}}\iint_{\Delta_N} R_2(\lambda_1,\lambda_2)\,d\lambda_1 d\lambda_2\\
&\quad = \frac{1}{\hat{N}}\iint_{\{(s,t):\, a<s-t<b,\ |s|,|t|<t_N\}} \frac{1}{\big(K_N(0,0)\big)^2} R_2\left(\frac{s}{K_N(0,0)}, \frac{t}{K_N(0,0)}\right) ds\,dt\\
&\quad \sim \frac{1}{\hat{N}}\iint_{\{(s,t):\, a<s-t<b,\ |s|,|t|<t_N\}} \left(1 - \Big(\frac{\sin\pi(s-t)}{\pi(s-t)}\Big)^2\right) ds\,dt\\
&\quad \sim \frac{2t_N}{\hat{N}}\int_a^b \left(1 - \Big(\frac{\sin\pi r}{\pi r}\Big)^2\right) dr\\
&\quad \sim \int_a^b \left(1 - \Big(\frac{\sin\pi r}{\pi r}\Big)^2\right) dr, \quad \text{by (25).}
\end{aligned}$$

Thus, if $\tilde{\lambda}_j \equiv K_N(0,0)\lambda_j$ are, again, the scaled eigenvalues, then for t_N as in (24)

$$\begin{aligned}
\lim_{N\to\infty}\frac{1}{\hat{N}}\mathbb{E}\big(\#\{\text{ordered pairs } (i,j), i \ne j\ :\ a < \tilde{\lambda}_i - \tilde{\lambda}_j < b,\ |\tilde{\lambda}_i|, |\tilde{\lambda}_j| \le t_N\}\big)\\
= \int_a^b \left(1 - \Big(\frac{\sin\pi r}{\pi r}\Big)^2\right) dr.
\end{aligned} \tag{27}$$

Another quantity of interest is the spacing distribution of the eigenvalues $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_N$ of a random $N \times N$ matrix as $N \to \infty$. More precisely, for $s > 0$, we want to compute

$$\mathbb{E}\left(\frac{\#\{1 \le j \le N-1\ :\ \lambda_{j+1} - \lambda_j \le s\}}{N}\right)$$

as N becomes large. If we again restrict our attention to eigenvalues in a neighborhood of a bulk energy $E = 0$, say, then the eigenvalue spacing distribution exhibits universal behavior for UE's as $N \to \infty$. We have in particular the following result of Gaudin

(see [Meh], and also [Dei1]): With t_N, $\hat{N}$ and $\tilde{x}_j = K_N(0,0)x_j$ as above,

$$\begin{aligned}\lim_{N\to\infty} \mathbb{E}\left(\frac{\#\{1 \le j \le N-1 \,:\, \tilde{\lambda}_{j+1} - \tilde{\lambda}_j \le s,\ |\tilde{\lambda}_j| \le t_N\}}{\hat{N}}\right) \\ = \lim_{N\to\infty} \text{Prob(at least one eigenvalue } \tilde{\lambda}_j \text{ in } (0,s] \,|\, \text{eigenvalue at 0}) \\ = \int_0^s p(u)\,du\end{aligned} \tag{28}$$

where

$$p(u) = \frac{d^2}{du^2}\left(\det\left(1 - K_\infty\restriction_{L^2(0,u)}\right)\right). \tag{29}$$

At the upper spectral edge $E = \lambda_{\max}$, one again finds universal behavior for UE's with potentials $V_{N,2}$, in particular, of the form (23) above. For such $V_{N,2}$'s there exist constants $z_N^{(2)}$, $s_N^{(2)}$ such that for $t \in \mathbb{R}$ (see [DeiGio2] and the notes therein)

$$\lim_{N\to\infty} \text{Prob}\left(M \,:\, \frac{\lambda_{\max} - z_N^{(2)}}{s_N^{(2)}} \le t\right) = \det\left(1 - \mathcal{A}\restriction_{L^2(t,\infty)}\right). \tag{30}$$

Here $\mathcal{A}$ is the so-called *Airy operator* with kernel

$$\mathcal{A}(x,y) = \frac{\text{Ai}(x)\text{Ai}'(y) - \text{Ai}'(x)\text{Ai}(y)}{x-y}, \tag{31}$$

where $\text{Ai}(x)$ is the classical Airy function. For GUE, where $V_{N,2}(x) = x^2$, one has $z_N^{(2)} = \sqrt{2N}$ and $s_N^{(2)} = 2^{-\frac{1}{2}} N^{-\frac{1}{6}}$ (see Forrester [For1] and the seminal work of Tracy and Widom [TraWid1]).

It turns out that $\det\left(1 - K_\infty\restriction_{L^2(-x,x)}\right)$ in (21) and $\det\left(1 - \mathcal{A}\restriction_{L^2(t,\infty)}\right)$ can be expressed in terms of solutions of the Painlevé V and Painlevé II equations respectively. The first is a celebrated result of Jimbo, Miwa, Môri, and Sato [JMMS], and the second is an equally celebrated result of Tracy and Widom [TraWid1]. In particular for edge scaling we find

$$\lim_{N\to\infty} \text{Prob}\left(M \,:\, \frac{\lambda_{\max} - z_N^{(2)}}{s_N^{(2)}} \le t\right) = F_{\beta=2}(t) \tag{32}$$

where

$$F_{\beta=2}(t) = \det\left(1 - \mathcal{A}\restriction_{L^2(t,\infty)}\right) = e^{-\int_t^\infty (s-t)u^2(s)\,ds} \tag{33}$$

and $u(s)$ is the (unique, global) Hastings–McLeod solution of the Painlevé II equation

$$u''(s) = 2u^3(s) + su(s) \tag{34}$$

such that

$$u(s) \sim \text{Ai}(s) \quad \text{as } s \to +\infty. \tag{35}$$

$F_2(t) = F_{\beta=2}(t)$ is called the *Tracy–Widom distribution* for $\beta = 2$.

Finally we note that for OE's and SE's there are analogs for all the above results (10)–(35), and again one finds universality in the scaling limits as $N \to \infty$ for potentials $V_{N,\beta}$, $\beta = 1, 4$, of the form (23) above (see [DeiGio1] and [DeiGio2] and the historical notes therein). We note, in particular, the following results: for $V_{N,\beta}$ as above, $\beta = 1$ or 4, there exist constants $z_N^{(\beta)}$, $s_N^{(\beta)}$ such that

$$\lim_{N\to\infty} \text{Prob}\left(M \,:\, \frac{\lambda_{\max}(M) - z_N^{(\beta)}}{s_N^{(\beta)}} \le t \right) = F_\beta(t) \tag{36}$$

where

$$F_1(t) = \big(F_2(t)\big)^{\frac{1}{2}} e^{-\frac{1}{2}\int_t^\infty u(s)\,ds} \tag{37}$$

and

$$F_4(t) = \big(F_2(t)\big)^{\frac{1}{2}} \cdot \frac{e^{\frac{1}{2}\int_t^\infty u(s)\,ds} + e^{-\frac{1}{2}\int_t^\infty u(s)\,ds}}{2} \tag{38}$$

with $F_2(t)$ and $u(s)$ as above. $F_1(t)$ and $F_4(t)$ are called the *Tracy–Widom distributions* for $\beta = 1$ and 4 respectively.

3. The problems

In this section we consider seven problems. The first is from physics and is included for historical reasons that will become clear in Section 4 below; the remaining six problems are from mathematics/mathematical physics.

Problem 1. Consider the scattering of neutrons off a heavy nucleus, say uranium U^{238}. The scattering cross-section is plotted as a function of the energy E of the incoming neutrons, and one obtains a jagged graph (see [Por] and [Meh]) with many hundreds of sharp peaks $E_1 < E_2 < \cdots$ and valleys $E_1' < E_2' < \cdots$. If $E \sim E_j$ for some j, the neutron is strongly repelled from the nucleus, and if $E \sim E_j'$ for some j, then the neutron sails through the nucleus, essentially unimpeded. The E_j's are called *scattering resonances*. The challenge faced by physicists in the late 40s and early 50s was to develop an effective model to describe these resonances. One could of course write down a Schrödinger-type equation for the scattering system, but because of the high dimensionality of the problem there is clearly no hope of solving the equation for the E_j's either analytically or numerically. However, as more experiments were done on heavy nuclei, each with hundreds of E_j's, a consensus began to emerge that the "correct" theory of resonances was statistical, and here Wigner led the way. Any effective theory would have to incorporate two essential features present in the data, viz.

(i) modulo certain natural symmetry considerations, all nuclei in the same symmetry class exhibited universal behavior;

(ii) in all cases, the E_j's exhibited *repulsion*, or, more precisely, the probability that two E_j's would be close together was small.

Question 1. What theory did Wigner propose for the E_j's?

Problem 2. Here we consider the work of H. Montgomery [Mon] in the early 1970s on the zeros of the Riemann zeta function $\zeta(s)$. Assuming the Riemann hypothesis, Montgomery rescaled the imaginary parts $\gamma_1 \le \gamma_2 \le \cdots$ of the (nontrivial) zeros $\{\frac{1}{2} + i\gamma_j\}$ of $\zeta(s)$,

$$\gamma_j \to \tilde{\gamma}_j = \frac{\gamma_j \log \gamma_j}{2\pi} \tag{39}$$

to have mean spacing 1 as $T \to \infty$, i.e.

$$\lim_{T\to\infty} \frac{\#\{j \ge 1 \,:\, \tilde{\gamma}_j \le T\}}{T} = 1.$$

For any $a < b$, he then computed the two-point correlation function for the $\tilde{\gamma}_j$'s

$$\#\{\text{ordered pairs } (j_1, j_2),\, j_1 \ne j_2 \,:\, 1 \le j_1, j_2 \le N,\ \tilde{\gamma}_{j_1} - \tilde{\gamma}_{j_2} \in (a, b)\}$$

and showed, modulo certain technical restrictions, that

$$\begin{aligned} R(a,b) \equiv \lim_{N\to\infty} \frac{1}{N} \#\{&\text{ordered pairs } (j_1, j_2),\ j_1 \ne j_2 \,: \\ &1 \le j_1, j_2 \le N,\ \tilde{\gamma}_{j_1} - \tilde{\gamma}_{j_2} \in (a, b)\} \end{aligned} \tag{40}$$

exists and is given by a certain explicit formula.

Question 2. What formula did Montgomery obtain for $R(a, b)$?

Problem 3. Consider the solitaire card game known as *patience sorting* (see [AldDia] and [Mal]). The game is played with N cards, numbered $1, 2, \ldots, N$ for convenience. The deck is shuffled and the first card is placed face up on the table in front of the dealer. If the next card is smaller than the card on the table, it is placed face up on top of the card; if it is bigger, the card is placed face up to the right of the first card, making a new pile. If the third card in the pile is smaller than one of the cards on the table, it is placed on top of that card; if it is smaller than both cards, it is placed as far to the left as possible. If it is bigger than both cards, it is placed face up to the right of the pile(s), making a new pile. One continues in this fashion until all the cards are dealt out. Let q_N denote the number of piles obtained. Clearly q_N depends on the particular shuffle $\pi \in S_N$, the symmetric group on N numbers, and we write $q_N = q_N(\pi)$.

For example, if $N = 6$ and $\pi = 3\,4\,1\,5\,6\,2$, where 3 is the top card, 4 is the next card and so on, then patience sorting proceeds as follows:

				1			1			1				1	2				
3		3	4	3	4		3	4	5	3	4	5	6	3	4	5	6		

and $q_6(\pi) = 4$.

Question 3. Equip S_N with the uniform distribution. If each card is of unit size, how big a table does one typically need to play patience sorting with N cards? Or, more precisely, how does

$$p_{n,N} = \text{Prob}\big(\pi \ : \ q_N(\pi) \leq n\big) \tag{41}$$

behave as $N \to \infty$, $n \leq N$?

Problem 4. The city of Cuernavaca in Mexico (population about 500,000) has an extensive bus system, but there is no municipal transit authority to control the city transport. In particular there is no timetable, which gives rise to Poisson-like phenomena, with bunching and long waits between buses. Typically, the buses are owned by drivers as individual entrepreneurs, and all too often a bus arrives at a stop just as another bus is loading up. The driver then has to move on to the next stop to find his fares. In order to remedy the situation the drivers in Cuernavaca came up with a novel solution: they introduced "recorders" at specific locations along the bus routes in the city. The recorders kept track of when buses passed their locations, and then sold this information to the next driver, who could then speed up or slow down in order to optimize the distance to the preceding bus. The upshot of this ingenious scheme is that the drivers do not lose out on fares and the citizens of Cuernavaca now have a reliable and regular bus service. In the late 1990s two Czech physicists with interest in transportation problems, M. Krbálek and P. Šeba, heard about the buses in Cuernavaca and went down to Mexico to investigate. For about a month they studied the statistics of bus arrivals on Line 4 close to the city center. In particular, they studied the bus spacing distribution, and also the bus number variance measuring the fluctuations of the total number of buses arriving at a fixed location during a time interval T. Their findings are reported in [KrbSeb].

Question 4. What did Krbálek and Šeba learn about the statistics of the bus system in Cuernavaca?

Problem 5. In his investigation of wetting and melting phenomena in [Fis], Fisher introduced various "vicious" walker models. Here we will consider the so-called *random turns vicious walker model*. In this model, the walks take place on the integer lattice $\mathbb{Z}$ and initially the walkers are located at $0, 1, 2, \ldots$. The rules for a walk are as follows:

(a) at each tick of the clock, precisely one walker makes a step to the left;

(b) no two walkers can occupy the same site (hence "vicious walkers").

For example, consider the following walk from time $t = 0$ to time $t = 4$: At $t = 0$, clearly only the walker at 0 can move. At time $t = 1$, either the walker at -1 or at $+1$ can move, and so on. Let d_N be the distance traveled by the walker starting from 0. In the above example, $d_4 = 2$. For any time N, there are clearly only a finite number of possible walks of duration $t = N$. Suppose that all such walks are equally likely.

Question 5. How does d_N behave statistically as $N \to \infty$?

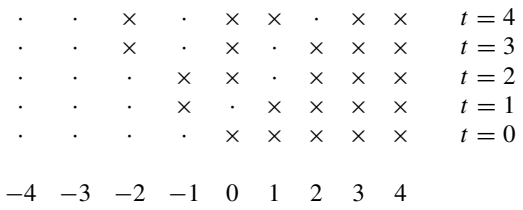


Figure 1. Random turns walk.

Problem 6. Consider tilings $\{T\}$ of the tilted square $\boldsymbol{T}_n = \{(x, y) : |x|+|y| \leq n+1\}$ in $\mathbb{R}^2$ by horizontal and vertical dominos of length 2 and width 1. For example, for $n = 3$ we have the tiling T of Figure 2. For each tiling the dominos must lie strictly

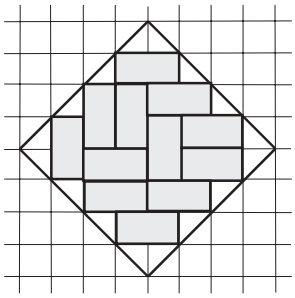


Figure 2. Aztec diamond for $n = 3$.

within $\boldsymbol{T}_n$. The tilings T are called *Aztec diamonds* because the boundary of T in $\{(x, y) : y > 0\}$, say, has the shape of a Mexican pyramid. It is a nontrivial theorem (see [EKLP]) that for any n, the number of domino tilings of $\boldsymbol{T}_n$ is $2^{\frac{n(n+1)}{2}}$. Assume that all tilings are equally likely.

Question 6. What does a typical tiling look like as $n \to \infty$?

Finally we have

Problem 7. How long does it take to board an airplane? We consider the random boarding strategy in [BBSSS] under the following simplifying assumptions:

(a) there is only 1 seat per row;

(b) the passengers are very thin compared to the distance between seats;

(c) the passengers move very quickly between seats. The main delay in boarding is the time – one unit – that it takes for the passengers to organize their luggage and seat themselves once they arrive at their assigned seats.

For the full problem with more than one seat per row, passengers who are not "very thin", etc., see [BBSSS], and also the discussion of the boarding problem in Section 4 below.

The passengers enter the airplane through a door in front and the seats are numbered $1, 2, \ldots, N$, with seat 1 closest to the door. How does boarding proceed? Consider, for example, the case $N = 6$. There are 6 passengers, each with a seating card $1, 2, \ldots, 6$. At the call to board, the passengers line up randomly at the gate. Suppose for definitiveness that the order in the line is given by

$$\pi : \ 3\,4\,1\,5\,6\,2 \tag{42}$$

with 3 nearest the gate. Now 3 can proceed to his'r seat, but 4 is blocked and must wait behind 3 while s'he puts his'r bag up into the overhead bin. However, at the same time, 1 can proceed to his'r seat, but 5, 6, and 2 are blocked. At the end of one unit of time, 3 and 1 sit down, and 4 and 2 can proceed to their seats, but 5 and 6 are blocked behind 4. After one more unit of time 4 and 2 sit down, and 5 can proceed to his'r seat, but 6 is blocked. At the end of one more unit of time 5 sits down, and finally 6 can move to his'r seat. Thus for π as above, it takes 4 units of time to board. Let $b_N = b_N(\pi)$ denote the boarding time for any $\pi \in S_N$, and assume that the π's are uniformly distributed.

Question 7. How does $b_N(\pi)$ behave statistically as $N \to \infty$?

4. Solutions and explanations

As indicated in the Introduction, the remarkable fact of the matter is that all seven problems in Section 3 are modeled by RMT.

Problem 1 (Neutron scattering). At some point in the mid-1950s, in a striking development, Wigner suggested that the statistics of the neutron scattering resonances was governed by GOE[2] (and hence, by universality [DeiGio1], by all OE's). And indeed, if one scales real scattering data for a variety of nuclei according to the standard procedure and then evaluates, in particular, the nearest neighbor distribution, one finds remarkable agreement with the OE analog of the spacing distribution (28), (29).

It is interesting, and informative, to trace the development of ideas that led Wigner to his suggestion (see [Wig1], [Wig2], [Wig3]; all three papers are reproduced in [Por]). In these papers, Wigner is guided by the fact that any model for the resonances would have to satisfy the constraints of universality and repulsion, (i) and (ii) respectively, in the description of Problem 1. In [Wig2] he recalls a paper that he had written with von Neumann in 1929 in which they showed, in particular, that in the $\frac{n(n+1)}{2}$-dimensional space of real $n \times n$ symmetric matrices, the matrices with double

[2]Here we must restrict the data to scattering for situations where the nuclear forces are time-reversal invariant. If not, the statistics of the scattering resonances should be governed by GUE.

eigenvalues form a set of codimension 2. For example, if a 2×2 real symmetric matrix has double eigenvalues, then it must be a multiple of the identity and hence it lies in a set of dimension 1 in $\mathbb{R}^3$. It follows that if one equips the space of real, symmetric matrices with a probability measure with a smooth density, the probability of a matrix M having equal eigenvalues would be zero and the eigenvalues $\lambda_1, \ldots, \lambda_n$ of M would comprise a random set with repulsion built in. So Wigner had a model, or more precisely, a class of models, which satisfied constraint (ii). But why choose GOE? This is where the universality constraint (i) comes into play. We quote from [Wig3][3]: "Let me say only one more word. It is very likely that the curve in Figure 1 is a universal function. In other words, it doesn't depend on the details of the model with which you are working. There is one particular model in which the probability of the energy levels can be written down exactly. I mentioned this distribution already in Gatlinburg. It is called the Wishart distribution. Consider a set…." So in this way Wigner introduced GOE into theoretical physics: It provided a model with repulsion (and time-reversal) built in. Furthermore, the energy level distribution could be computed explicitly. By universality, it should do the trick!

As remarkable as these developments were, even the most prophetic observer could not have predicted that, a few years down the line, these developments would make themselves felt within pure mathematics.

Problem 2 (Riemann zeta function). Soon after completing his work on the scaling limit (40) of the two-point correlation function for the zeros of zeta, Montgomery was visiting the Institute for Advanced Study in Princeton and it was suggested that he show his result to Dyson. What happened is a celebrated, and oft repeated, story in the lore of the Institute: before Montgomery could describe his hard won result to Dyson, Dyson took out a pen, wrote down a formula, and asked Montgomery "And did you get this?"

$$R(a,b) = \int_a^b 1 - \left(\frac{\sin(\pi r)}{\pi r}\right)^2 dr \tag{43}$$

Montgomery was stunned: this was exactly the formula he had obtained. Dyson explained: "If the zeros of the zeta function behaved like the eigenvalues of a random GUE matrix, then (43) would be exactly the formula for the two-point correlation function!" (See (27) above.)

More precisely, what Montgomery actually proved was that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{1\le i\ne j\le N} f(\tilde{\gamma}_i - \tilde{\gamma}_j) = \int_{\mathbb{R}} f(r) \left(1 - \left(\frac{\sin \pi r}{\pi r}\right)^2\right) dr \tag{44}$$

for any rapidly decaying function f whose Fourier transform $\hat{f}(\xi)$ is supported in the interval $|\xi| < 2$. Of course, if one could prove (44) for all smooth, rapidly decaying functions, one would recover the full result (43). Nevertheless, in an impressive series

[3]In the quotation that follows, "Figure 1" portrays a level spacing distribution, the "Wishart distribution" is the statisticians' name for GOE, and "Gatlinburg" is [Wig1].

of numerical computations starting in the 1980s, Odlyzko verified (43) to extraordinary accuracy (see [Odl1], [Odl2], and the references therein). In his computations, Odlyzko also considered GUE behavior for other statistics for the $\tilde{\gamma}_j$'s, such as the nearest neighbor spacing, verifying in particular the relationship

$$\lim_{N\to\infty} \frac{1}{N}\#\{1 \le j \le N-1 \,:\, \tilde{\gamma}_{j+1} - \tilde{\gamma}_j \le s\} = \int_0^s p(u)\,du, \quad s > 0, \tag{45}$$

(cf. (28), (29)) to high accuracy.

The relationship between the zeros of the zeta function and random matrix theory first discovered by Montgomery has been taken up with great virtuosity by many researchers in analytic number theory, with Rudnick and Sarnak [RudSar], and then Katz and Sarnak [KatSar], leading the way. GUE behavior for the zeros of quite general automorphic L-functions over $\mathbb{Q}$, as well as for a wide class of zeta and L-functions over finite fields, has now been established (modulo technicalities as in (44) above in the number field case). Another major development has been the discovery of a relationship between random polynomials whose roots are given by the eigenvalues of a matrix from some random ensemble, and the moments of the L-functions on the critical line $\operatorname{Re} z = \frac{1}{2}$ (see [KeaSna1], [KeaSna2]). The discovery of Montgomery/Odlyzko counts as one of the major developments in analytic number theory in many, many years.

Problem 3 (Patience sorting). In 1999 Baik, Deift and Johansson [BDJ1] proved the following result for $q_N(\pi)$, the number of piles obtained in patience sorting starting from a shuffle π of N cards. Let $\chi_N = \frac{q_N - 2\sqrt{N}}{N^{1/6}}$. Then

$$\lim_{N\to\infty} \operatorname{Prob}\big(\chi_N \le t\big) = F_2(t) \tag{46}$$

where F_2 is the Tracy–Widom distribution (32), (33) for $\beta = 2$. Thus the number of piles, suitably centered and scaled, behaves statistically like the largest eigenvalue of a GUE matrix. In addition, the authors proved convergence of moments. For any $m = 1, 2, \ldots,$

$$\lim_{N\to\infty} \mathbb{E}(\chi_N^m) = \mathbb{E}(\chi^m) \tag{47}$$

where χ is any random variable with distribution F_2. In particular, for $m = 1, 2$ one obtains

$$\lim_{N\to\infty} \frac{\mathbb{E}(q_N) - 2\sqrt{N}}{N^{1/6}} = \int_{\mathbb{R}} t\,dF_2(t) \tag{48}$$

and

$$\lim_{N\to\infty} \frac{\mathbb{V}(q_N)}{N^{1/3}} = \int_{\mathbb{R}} t^2\,dF_2(t) - \left(\int_{\mathbb{R}} t\,dF_2(t)\right)^2. \tag{49}$$

Numerical evaluation shows that the constants on the right-hand side of (48) and (49) are given by -1.7711 and 0.8132, respectively. Thus, as $N \to \infty$,

$$\mathbb{E}(q_N) \sim 2\sqrt{N} - 1.7711 \cdot N^{1/6}$$

so that for a deck of $N = 52$ cards, one needs a table of size about 12 units on average to play the game.

Patience sorting is closely related to the problem of *longest increasing subsequences* for permutations $\pi \in S_N$. Recall that we say that $\pi(i_1), \ldots, \pi(i_k)$ is an increasing subsequence in π of length k if $i_1 < i_2 < \cdots < i_k$ and $\pi(i_1) < \pi(i_2) < \cdots < \pi(i_k)$. Let $l_N(\pi)$ be the length of the longest increasing subsequence in π. For example, if $N = 6$ and $\pi = 3\,4\,1\,5\,6\,2$ we see that $3\,4\,5\,6$ is a longest increasing subsequence for π and hence $l_6(\pi) = 4$. Comparing with the introduction to Question 3, we see that $l_6(\pi) = q_6(\pi)$. This is no accident: for any $\pi \in S_N$, we always have $l_N(\pi) = q_N(\pi)$ (see, e.g. [AldDia]), and hence we learn from (46) that the length l_N of the longest increasing subsequence behaves statistically like the largest eigenvalue of a GUE matrix as $N \to \infty$. The relation $l_N(\pi) = q_N(\pi)$ and (48) imply in particular that

$$\lim_{N\to\infty} \frac{\mathbb{E}(l_N)}{N^{1/2}} = 2. \tag{50}$$

The claim that the limit in (50) exists, and equals 2, is known as "Ulam's problem" and has a long history (see [BDJ1]). In another direction, uniform distribution on S_N pushes forward under the Robinson–Schensted correspondence (see, e.g. [Sag]) to so-called *Plancherel measure* on Young diagrams of size N. Young diagrams are parameterized by partitions $\mu \vdash N$, $\{\mu = (\mu_1, \mu_2, \ldots, \mu_l) : \mu_1 \geq \mu_2 \geq \cdots \geq \mu_l \geq 1, \sum_{i=1}^{l} \mu_i = N\}$, where μ_i is the number of boxes in the ith row, and it turns out that under the correspondence we have

$$\text{Prob}\big(\pi : l_N(\pi) \leq n\big) = \text{Prob}\big(\mu \vdash N : \mu_1 \leq n\big). \tag{51}$$

Consequently, the number of boxes in the first row of Plancherel-random Young diagrams behaves statistically, as $N \to \infty$, like the largest eigenvalue of a GUE matrix. In [BDJ1] the authors conjectured that the number of boxes in the first k rows of a Young diagram should behave statistically as $N \to \infty$ like the top k eigenvalues $\lambda_N \geq \lambda_{N-1} \geq \cdots \geq \lambda_{N-k+1}$ of a GUE matrix. This conjecture was proved for the 2^{nd} row in [BDJ2]. For general k, the conjecture was proved, with convergence in joint distribution, in three separate papers in rapid succession ([Oko], [BOO], [Joh1]), using very different methods. The proof in [Oko] relies on an interplay between maps on surfaces and ramified coverings of the sphere; the proof in [BOO] is based on the analysis of specific characters on $S(\infty)$, the infinite symmetric group defined as the inductive limit of the finite symmetric groups S_N under the embeddings $S_N \hookrightarrow S_{N+1}$; and the proof in [Joh1] utilizes certain discrete orthogonal polynomial ensembles arising in combinatorial probability.

One can consider the statistics of $l_N(\pi)$ for π restricted to certain distinguished subsets of S_N (see [BaiRai1]). Amongst the many results in [BaiRai1] relating combinatorics and random matrix theory, we mention the following. Let $S_N^{(\text{inv})} = \{\pi \in S_N : \pi^2 = \text{id}\}$ be the set of involutions in S_N. Then, under the Robinson–Schensted correspondence, uniform distribution on $S_N^{(\text{inv})}$ pushes forward to a new measure on

Young diagrams, different from the Plancherel measure. Denote this measure by $\mathrm{Prob}^{(\mathrm{inv})}$, and in place of (51) we have

$$\mathrm{Prob}\big(\pi \in S_N^{(\mathrm{inv})} \,:\, l_N(\pi) \le n\big) = \mathrm{Prob}^{(\mathrm{inv})}\big(\mu \vdash N \,:\, \mu_1 \le n\big).$$

In [BaiRai1] the authors show that

$$\begin{aligned}
&\lim_{N\to\infty} \mathrm{Prob}\left(\pi \in S_N^{(\mathrm{inv})} \,:\, \frac{l_N - 2\sqrt{N}}{N^{1/6}} \le x\right) \\
&\quad = \lim_{N\to\infty} \mathrm{Prob}^{(\mathrm{inv})}\left(\mu \vdash N \,:\, \frac{\mu_1 - 2\sqrt{N}}{N^{1/6}} \le x\right) \\
&\quad = F_{\beta=1}(x)
\end{aligned} \tag{52}$$

and for the second row of μ

$$\lim_{N\to\infty} \mathrm{Prob}^{(\mathrm{inv})}\left(\mu \vdash N \,:\, \frac{\mu_2 - 2\sqrt{N}}{N^{1/6}} \le x\right) = F_{\beta=4}(x). \tag{53}$$

Here $F_{\beta=1}$ and $F_{\beta=4}$ are the Tracy–Widom distributions for the largest eigenvalue of the GOE and GSE ensemble, respectively (see (36), (37), (38)). Thus all three of the basic ensembles $\beta = 1, 2$ and 4 show up in the analysis of the (general) increasing subsequence problem.

A problem which is closely related to the longest increasing subsequence problem is the random word problem. In [TraWid4] the authors consider words $\{\omega\}$ of length N in an alphabet of k letters, i.e. maps $\omega\colon \{1, 2, \ldots, N\} \to \{1, 2, \ldots, k\}$. One says that $\omega(i_1), \ldots, \omega(i_j)$ is a weakly increasing subsequence in ω of length j if $i_1 < i_2 < \cdots < i_j$ and $\omega(i_1) \le \omega(i_2) \le \cdots \le \omega(i_j)$. Let $l_N^{\mathrm{wk}}(\omega)$ denote the length of the longest weakly increasing subsequence in ω. Assuming that all words are equally likely, Tracy and Widom in [TraWid4] proved that

$$\begin{aligned}
&\lim_{N\to\infty} \mathrm{Prob}\left(\omega \,:\, \frac{l_N^{\mathrm{wk}}(\omega) - \frac{N}{k}}{\sqrt{\frac{2N}{k}}} \le s\right) \\
&\quad = \gamma_k \int_{\mathcal{L}_s} e^{-\sum_{i=1}^k x_i^2} \prod_{1\le i<j\le k} (x_i - x_j)^2 \, dx_1 \cdots dx_{k-1}
\end{aligned} \tag{54}$$

where

$$\mathcal{L}_s = \big\{(x_1, \ldots, x_k) \,:\, \max_{1\le i\le k} x_i \le s,\ x_1 + \cdots + x_k = 0\big\} \tag{55}$$

and

$$\gamma_k = \frac{\sqrt{k}\, 2^{\frac{k^2-1}{k}}}{\left(\prod_{i=1}^k i!\right)(2\pi)^{\frac{k-1}{2}}}. \tag{56}$$

It is easy to see that the right-hand side of (54) is just the distribution function for the largest eigenvalue of a $k \times k$ GUE matrix conditioned to have trace zero.

Consider the representation of the number π, say, in any basis b,

$$\pi = 0.a_1a_2a_3 \ldots \times b^q, \quad q \in \mathbb{Z}. \tag{57}$$

It has long been believed that in some natural asymptotic sense the digits a_1, a_2, a_3,... are independent and identically distributed, with uniform distribution on $\{0, 1, \ldots, b-1\}$. In an attempt to formalize this notion, E. Borel (1909) introduced the idea of normality (see [Wag]): A real number x is *normal* if for any base b, any $m \geq 1$, and any m-string s,

$$\lim_{n\to\infty} \frac{\#\{\text{occurrences of } s \text{ in the first } n \text{ base-}b \text{ digits of } x\}}{n} = b^{-m}. \tag{58}$$

While it is known that non-normal numbers form a set of Lebesgue measure zero, and all numerical evidence confirms (58) to high order, no explicit examples of normal numbers are known.

Relation (54) suggests a new way to test for asymptotic randomness, as follows. Consider the first LN base-b digits $a_1a_2 \ldots a_{LN}$ of a given number x, where L and N are "large". Partition these digits into L words $\omega_j = a_{(j-1)N+1} \ldots a_{jN}$, $1 \leq j \leq L$, each of length N. For each ω_j compute $l_N^{\text{wk}}(\omega_j)$. Then if the digits $\{a_j\}$ of x are asymptotically random, we could expect that as $L, N \to \infty$, the empirical distribution

$$\frac{1}{L}\#\left\{1 \leq j \leq L \,:\, \frac{l_N^{\text{wk}}(\omega_j) - \frac{N}{b}}{\sqrt{\frac{2N}{b}}} \leq s\right\}$$

is close to the conditional GUE distribution on the right-hand side of (54). Preliminary calculations in [DeiWit] for $x = \pi$ and $b = 2$ show that for L, N "large" the empirical distribution is indeed close to the right-hand side of (54) with high accuracy. The work is in progress.

Problem 4 (Bus problem in Cuernavaca). Krbálek and Šeba found that both the bus spacing distribution and the number variance are well modeled by GUE, (28), (29) and (17) respectively (see Figures 2 and 3 in [KrbSeb]). In order to provide a plausible explanation of the observations in [KrbSeb], the authors in [BBDS] introduced a microscopic model for the bus line that leads simply and directly to GUE.

The main features of the bus system in Cuernavaca are

(a) the stop-start nature of the motion of the buses;

(b) the "repulsion" of the buses due to the presence of recorders.

To capture these features, the authors in [BBDS] introduced a model for the buses consisting of n(= # of buses) independent, rate 1 Poisson processes moving from the bus depot at time $t = 0$ to the final terminus at time T, and conditioned not to intersect

for $0 \le t \le T$. The authors then showed that at any observation point x along the route of length $N > n$, the probability distribution for the (rescaled) arrival times of the buses, $y_j = \frac{2t_j}{T} - 1 \in [-1, 1]$, $1 \le j \le n$, is given by

$$\text{const.} \prod_{j=1}^{n} w_J(y_j) \prod_{1 \le i < j \le n} (y_i - y_j)^2 \, dy_1 \cdots dy_n \tag{59}$$

where

$$w_J(y) = (1+y)^{x-1}(1-y)^{N-x-n+1}, \quad -1 < y < 1. \tag{60}$$

Formula (59) is precisely the eigenvalue distribution for the so-called Jacobi Unitary Ensemble (cf. (4) with $e^{-V_{N,2}(y)} = w_J(y) =$ weight for Jacobi polynomials on $[-1, 1]$). In the appropriate scaling limit, GUE then emerges by universality. The authors also compute the distributions of the positions $x_1, \ldots, x_n$ of the buses at any time $t \in (0, T)$. Again the statistics of the x_j's are described by a Unitary Ensemble, but now w_J is (59) is replaced by the weight for the Krawtchouk polynomials: by universality, GUE again emerges in the appropriate scaling limit.

In an intriguing recent paper, Abul-Magd [Abu] noted that drivers have a tendency "to park their cars near to each other and at the same time keep a distance sufficient for manoeuvring." He then analyzed data measuring the gaps between parked cars on four streets in central London and showed quite remarkably that the gap size distribution was well represented by the spacing distribution (28), (29) of GUE. It is an interesting challenge to develop a microscopic model for the parking problem in [Abu], analogous to the model for the bus problem in [BBDS].

Problem 5 (Random turns vicious walker model). In [BaiRai2] the authors proved that, as $N \to \infty$, d_N, the distance traveled by the walker starting from 0, behaves statistically like the largest eigenvalue of a GOE matrix. More precisely, they showed that

$$\lim_{N \to \infty} \text{Prob}\left(\frac{d_N - 2\sqrt{N}}{N^{1/6}} \le t \right) = F_1(t) \tag{61}$$

where F_1 is given by (37). In a variant of this model, [For3], the walkers again start at 0, 1, 2,..., and move to the left for a time N; thereafter they must move to the right, returning to their initial positions 0, 1, 2,...at time $2N$. Let d'_N denote the maximum excursion of the walker starting from 0. Then Forrester shows that d'_N behaves statistically like the largest eigenvalue of a GUE matrix,

$$\lim_{N \to \infty} \text{Prob}\left(\frac{d'_N - 2\sqrt{N}}{N^{1/6}} \le t \right) = F_2(t) \tag{62}$$

where F_2 is given by (33).

The proofs of (61) and (62) rely on the observation of Forrester in [For3] that, in the first case, the set of walks is in one-to-one correspondence with the set $Y^{(1)}$ of standard Young tableaux of size N (see [Sag]), whereas in the second case, the variant model,

the set of walks is in one-to-one correspondence with the set $Y^{(2)}$ of pairs (P, Q) of standard Young tableaux of size N with the same shape, $\mathrm{sh}(P) = \mathrm{sh}(Q)$. In both cases, d_N and d'_N equal the number of boxes in the first row of the corresponding standard Young tableaux. Uniform measure on $Y^{(2)}$ (resp $Y^{(1)}$) gives rise to Plancherel measure (resp. $\mathrm{Prob}^{(\mathrm{inv})}$) on Young diagrams of size N, and the proof of (62) then follows from (46), (51), and the proof of (61) follows from (52).

In [Bai], Baik proved the analogue of (61), (62) for the so-called lock step vicious walker introduced in [Fis]. The proof in [Bai] relies in part on an observation of Guttmann et al. in [GOV], which preceded [For3], that the set of path configurations for the lock step model is in one-to-one correspondence with the set of semi-standard Young tableaux (see [Sag]).

Problem 6 (Aztec diamond). After scaling by $n+1$, Jockush et al., [JPS], considered the tiling problem with dominos of size $\frac{2}{n+1} \times \frac{1}{n+1}$ in the tilted square $\boldsymbol{T}_0 = \{(u, v) : |u| + |v| \leq 1\}$. As $n \to \infty$, they found that the inscribed circle $C_0 = \{(u, v) : u^2 + v^2 = \frac{1}{2}\}$, which they called the *arctic circle*, plays a remarkable role. In the four regions of $\boldsymbol{T}_0$ outside C_0, which they call the *polar regions* and label N, E, S, W clockwise from the top, the typical tiling is *frozen*, with all the dominoes in N and S horizontal, and all the dominos in E and W vertical. In the region inside C_0, which they call the *temperate zone*, the tiling is random. (See, for example, http://www.math.wisc.edu/~propp/tiling, where a tiling with $n = 50$ is displayed.)

But more is true. In [Joh1], [Joh2], Johansson considered fluctuations of the boundary of the temperate zone about the circle C_0. More precisely, for $-1 < \alpha < 1$, $\alpha \neq 0$, let

$$(x_\alpha^+, y_\alpha^+) = \left(\tfrac{\alpha+\sqrt{1-\alpha^2}}{2}, \tfrac{\alpha-\sqrt{1-\alpha^2}}{2}\right), \quad (x_\alpha^-, y_\alpha^-) = \left(\tfrac{\alpha-\sqrt{1-\alpha^2}}{2}, \tfrac{\alpha+\sqrt{1-\alpha^2}}{2}\right)$$

denote the two points of intersection of the line $u + v = \alpha$ with $C_0 = \{u^2 + v^2 = \frac{1}{2}\}$. Then for fixed α, Johansson showed that the fluctuations of the boundary of the temperate zone along the line $u + v = \alpha$ about the points (x_α^+, y_α^+) and (x_α^-, y_α^-) were described by the Tracy–Widom distribution F_2 (see [Joh2], equation (2.72), for a precise statement). Johansson proceeds by expressing the fluctuations in terms of the Krawtchouk ensemble (cf. Problem 4), which he then evaluates asymptotically as $n \to \infty$. Such an analysis is possible because the associated Krawtchouk polynomials have an integral representation which can be evaluated asymptotically using the classical method of steepest descent. In [CLP], the authors considered tilings of hexagons of size n by unit rhombi and proved an arctic circle theorem for the tilings as $n \to \infty$ as in the case of the Aztec diamond. In [Joh1], [Joh2], Johansson again expressed the fluctuations of the arctic circle for the hexagons in terms of a random particle ensemble, but now using the Hahn polynomials rather than the Krawtchouk polynomials. The Hahn polynomials, however, do not have a convenient integral representation and their asymptotics cannot be evaluated by classical means. This obstacle was overcome by Baik et al., [BKMM], who extended the Riemann–Hilbert/steepest descent method

in [DKMVZ1] and [DKMVZ2] to a general class of discrete orthogonal polynomials. In this way they were able to compute the asymptotics of the Hahn polynomials and verify F_2-behavior for the fluctuations of the temperate zone, as in the case of the Aztec diamond.

Problem 7 (Airline boarding). In [BBSSS] the authors show that $b_N(\pi)$, the boarding time for N passengers subject to the protocol (a)(b)(c) in Problem 7, behaves statistically like the largest eigenvalue of a GUE matrix,

$$\lim_{N\to\infty} \text{Prob}\left(\frac{b_N - 2\sqrt{N}}{N^{1/6}} \le t\right) = F_2(t). \tag{63}$$

The proof of (63) in [BBSSS] relies on the description of the Robinson–Schensted correspondence in terms of Viennot diagrams (see [Sag]). We illustrate the situation with the permutation $\pi :\ 3\,4\,1\,5\,6\,2$ in S_6 (cf. Problem 3 and (42)). We say that a point (x', y') *lies in the shadow* of a point (x, y) in the plane if $x' > x$ and $y' > y$. Plot π as a graph $(1, 3), (2, 4), \ldots, (6, 2)$ in the first quadrant of $\mathbb{R}^2$. Consider all the points in the graph which are not in the shadow of any other point: in our case $(1, 3)$ and $(3, 1)$. The *first shadow line* L_1 is the boundary of the combined shadows of these two points (see Figure 3). To form the *second shadow line* L_2, one removes the points $(1, 3)$, $(3, 1)$ on L_1, and repeats the procedure, etc. Eventually one obtains $k_N(\pi) = k$ shadow lines $L_1, \ldots, L_k$ for some integer k. In our example $k = 4$, which we note is precisely $l_6(\pi)$, the length of the longest increasing subsequence for π. This is no accident: for any $\pi \in S_N$, we always have $k_N(\pi) = l_N(\pi)$ (see [Sag]).

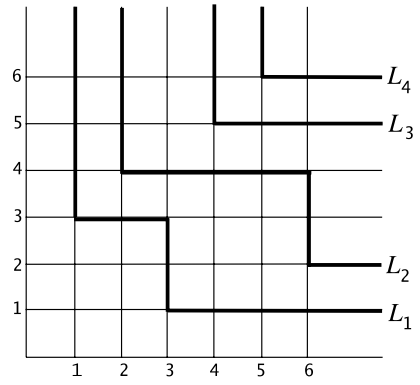


Figure 3. Shadow lines for $\pi :\ 3\,4\,1\,5\,6\,2$ in S_6.

The beautiful fact is that each shadow line describes a step in the boarding process. Indeed, noting the y-values of the L_j's, we observe that

$$\begin{aligned} L_1 &\longleftrightarrow \text{3 and 1 are seated} \\ L_2 &\longleftrightarrow \text{4 and 2 are seated} \\ L_3 &\longleftrightarrow \text{5 is seated} \\ L_4 &\longleftrightarrow \text{6 is seated} \end{aligned}$$

Thus $b_N(\pi) = k_N(\pi) = l_N(\pi) = q_N(\pi)$, and (63) follows from (46). In the language of physics, if we rotate the Viennot diagram for π counterclockwise by 45^o, we see that the shadow region of a point on the graph is simply the forward light cone based at that point (speed of light = 1). In other words, for appropriate coordinates $a,\ b$ we are dealing with the Lorentzian metric $ds^2 = dadb$. In order to incorporate more realistic features into their boarding model, such as the number of seats per row, average amount of aisle length occupied by a passenger, etc., the authors in [BBSSS] observe that it is enough simply to replace $ds^2 = dadb$ by a more general Lorentzian metric $ds^2 = 4D^2 p(a,b)(dadb + k\alpha(a,b)da^2)$ for appropriate parameters/functions D, p, k and α (see [BBSSS], equation (1)). Thus the basic phenomenon of blocking in the airline boarding problem is modeled in the general case by the forward light cone of some Lorentzian metric.

Problems 1 and 2 above, as opposed to 3–7, are purely deterministic and yet it seems that they are well described by a random model, RMT. At first blush, this might seem counterintuitive, but there is a long history of the description of deterministic systems by random models. After all, the throw of a (fair) 6-sided die through the air is completely described by Newton's laws: Nevertheless, there is no doubt that the *right* way to describe the outcome is probabilistic, with a one in six chance for each side. With this example in mind, we may say that Wigner was looking for the right stochastic model to describe the neutron scattering "die".

Problems 1–7 above are just a few of the many examples now known of mathematical/physical systems which exhibit random matrix type universal behavior. Other systems, from many different areas, can be found for example in [Meh] and the reviews [TraWid3], [For2], and [FerPra]. A particularly fruitful development has been the discovery of connections between random matrix theory and stochastic growth models in the KPZ class ([PraSpo], [FerPra]), and between random matrix theory and equilibrium crystals with short range interactions ([CerKen], [FerSpo], [OkoRes], [FerPraSpo]). In addition, for applications to principal component analysis in statistics in situations where the number of variables is comparable to the sample size, see [John] and [BBP] and the references therein. For a relatively recent review of the extensive application of RMT to quantum transport, see [Bee].

Returning to Wigner's introduction of random matrix theory into theoretical physics, we note that GOE is of course a mathematical model far removed from the laboratory of neutrons colliding with nuclei. Nevertheless, Wigner posited that

these two worlds were related: With hindsight, we recognize Wigner's insight as heralding the emergence of a scientific commonality far across the borders of physics and mathematics.

5. Comments and speculations

As is clear from the text, many different kinds of mathematics are needed to analyze Problems 3–7. These include

- combinatorial identities,
- Riemann–Hilbert methods,
- Painlevé theory,
- theory of Riemann surfaces,
- representation theory,
- classical and Riemann–Hilbert steepest descent methods

and, most importantly,

- random matrix theory.

The relevant combinatorial identities are often obtained by analyzing random particle systems conditioned not to intersect, as in Problem 4. The Riemann–Hilbert steepest descent method has its origins in the theory of integrable systems, as in [DeiZho]. There is no space in this article to describe the implementation of any of the above techniques in any detail. Instead, we refer the reader to [Dei2], which is addressed to a general mathematical audience, for a description of the proof of (46) in particular, using Gessel's formula in combinatorics [Ges], together with the Riemann–Hilbert steepest descent method. For Problem 2 the proofs are based on combinatorial facts and random matrix theory, together with techniques from the theory of L-functions, over $\mathbb{Q}$ and also (in [KatSar]) over finite fields.

Universality as described in this article poses a challenge to probability theory per se. The central limit theorem (2) above has three components: a statistical component (take independent, identically distributed random variables, centered and scaled), an algebraic component (add the variables), and an analytic component (take the limit in distribution as $n \to \infty$). The outcome of this procedure is then universal – the Gaussian distribution. The challenge to probabilists is to describe an analogous purely probabilistic procedure whose outcome is F_1, or F_2, etc. The main difficulty is to identify the algebraic component, call it operation X. Given X, if one takes i.i.d.'s, suitably centered and scaled, performs operation X on them, and then takes the limit in distribution, the outcome should be F_1, or F_2, etc. Interesting progress has been made recently (see [BodMar] and [BaiSui]) on identifying X for F_2. For a different approach to the results in [BodMar] and [BaiSui], see [Sui], where the author uses a very interesting generalized version of the Lindeberg principle due to Chatterjee [Cha1], [Cha2].

Our final comment/speculation is on the space D, say, of probability distributions. A priori, D is just a set without any "topography". But we know at least one interesting point on D, the Gaussian distribution F_G. By the central limit theorem, F_G lies in a "valley", and nearby distributions are drawn towards it. What we seem to be learning is that there are other interesting distributions, like F_1 or F_2, etc., which also lie in "valleys" and draw nearby distributions in towards them. This suggests that we equip D with some natural topological and Riemannian structure, and study the properties of D as a manifold per se.

References

[Abu] Abul-Magd, A. Y., Modelling gap-size distribution of parked cars using random-matrix theory. *Phys. A* **368** (2) (2006), 536–540.

[AldDia] Aldous, D., Diaconis, P., Longest increasing subsequences: from patience sorting to the Baik-Deift-Johansson theorem. *Bull. Amer. Math. Soc.* (*N.S.*) **36** (4) (1999), 413–432.

[BBSSS] Bachmat, E., Berend, D., Sapir, L., Skiena, S., Stolyarov, N., Analysis of airplane boarding via space-time geometry and random matrix theory. *J. Phys. A* **39** (29) (2006), L453–L459.

[Bai] Baik, J., Random vicious walks and random matrices. *Comm. Pure Appl. Math.* **53** (11) (2000), 1385–1410.

[BBP] Baik, J., Ben Arous, G., Péché, S., Phase transition of the largest eigenvalue for non-null complex sample covariance matrices. *Ann. Probab.* **33** (5) (2005), 1643–1697.

[BBDS] Baik, J., Borodin, A., Deift, P., Suidan, T., A model for the bus system in Cuernavaca (Mexico). *J. Phys. A* **39** (28) (2006), 8965–8975.

[Bee] Beenakker, C. W. J., Random-matrix theory of quantum transport. *Rev. Mod. Phys.* **69** (1997), 731–808.

[BDJ1] Baik, J., Deift, P., Johansson, K., On the distribution of the length of the longest increasing subsequence of random permutations. *J. Amer. Math. Soc.* **12** (4) (1999), 1119–1178.

[BDJ2] Baik, J., Deift, P., Johansson, K., On the distribution of the length of the second row of a Young diagram under Plancherel measure. *Geom. Funct. Anal.* **10** (4) (2000), 702–731.

[BKMM] Baik, J., Kriecherbauer, T., McLaughlin, K. D. T.-R., Miller, P. D., *Discrete Orthogonal Polynomials: Asymptotics and Applications*. Ann. Math. Studies 164, Princeton University Press, Princeton, N.J., 2007.

[BaiRai1] Baik, J., Rains, E. M., The asymptotics of monotone subsequences of involutions. *Duke Math. J.* **109** (2) (2001), 205–281.

[BaiRai2] Baik, J., Rains, E. M., Symmetrized random permutations. In *Random matrix models and their applications,* Math. Sci. Res. Inst. Publ. 40, Cambridge University Press, Cambridge 2001, 1–19.

[BaiSui] Baik, J., Suidan, T. M., A GUE central limit theorem and universality of directed first and last passage site percolation. *Internat. Math. Res. Notices* **6** (2005), 325–337.

[BleIts] Bleher, P. M., Its, A. R., Semiclassical asymptotics of orthogonal polynomials, Riemann-Hilbert problems, and universality in the matrix model. *Ann. of Math.* (2) **150** (1999), 185–266.

[BodMar] Bodineau, T., Martin, J. B., A universality property for last-passage percolation paths close to the axis. *Electron. Comm. Probab.* **10** (2005), 105–112.

[BOO] Borodin, A., Okounkov, A., Olshanski, G., Asymptotics of Plancherel measures for symmetric groups. *J. Amer. Math. Soc.* **13** (3) (2000), 481–515.

[CerKen] Cerf, R., Kenyon, R., The low-temperature expansion of the Wulff crystal in the 3D Ising model. *Comm. Math. Phys.* **222** (1) (2001), 147–179.

[Cha1] Chatterjee, S., A simple invariance theorem. arXiv:math.PR/0508213.

[Cha2] Chatterjee, S., A generalization of the Lindeberg principle. *Ann. Probab.* **34** (2006), 2061–2076.

[CLP] Cohn, H., Larsen, M., Propp, J., The shape of a typical boxed plane partition. *New York J. Math.* **4** (1998), 137–165 (electronic).

[Dei1] Deift, P., *Orthogonal polynomials and random matrices: A Riemann-Hilbert approach*. Courant Lect. Notes Math. 3, Amer. Math. Soc., Providence, R.I., 2000.

[Dei2] Deift, P., Integrable systems and combinatorial theory. *Notices Amer. Math. Soc.* **47** (6) (2000), 631–640.

[DeiGio1] Deift, P., Gioev, D., Universality in random matrix theory for orthogonal and symplectic ensembles. *Internat. Math. Res. Papers*, to appear.

[DeiGio2] Deift, P., Gioev, D., Universality at the edge of the spectrum for unitary, orthogonal and symplectic ensembles of random matrices. *Comm. Pure. Appl. Math.* **60** (2007), 867–910.

[DKMVZ1] Deift, P. A., Kriecherbauer, T., McLaughlin, K. T.-R., Venakides, S., Zhou, X., Uniform asymptotics for polynomials orthogonal with respect to varying exponential weights and applications to universality questions in random matrix theory. *Comm. Pure Appl. Math.* **52** (1999), 1335–1425.

[DKMVZ2] Deift, P. A., Kriecherbauer, T., McLaughlin, K. T.-R., Venakides, S., Zhou, X., Strong asymptotics of orthogonal polynomials with respect to exponential weights. *Comm. Pure Appl. Math.* **52** (1999), 1491–1552.

[DVZ] Deift, P., Venakides, S., Zhou, X., New results in small dispersion KdV by an extension of the steepest descent method for Riemann-Hilbert problems. *Internat. Math. Res. Notices* **6** (1997), 286–299.

[DeiWit] Deift, P., Witko, R., On the normality of π. In preparation.

[DeiZho] Deift, P., Zhou, X., A steepest descent method for oscillatory Riemann-Hilbert problems. Asymptotics for the MKdV equation. *Ann. of Math.* **137** (1993), 295–368.

[EKLP] Elkies, N., Kuperberg, G., Larsen, M., Propp, J., Alternating-sign matrices and domino tilings. I. *J. Algebraic Combin.* **1** (2) (1992), 111–132.

[FerPra] Ferrari, P., Prähofer, M., One-dimensional stochastic growth and Gaussian ensembles of random matrices. *Markov Processes Relat. Fields* **12** (2) (2006), 203–234.

[FerPraSpo] Ferrari, P., Prähofer, M., Spohn, H., Fluctuations of an atomic ledge bordering a crystaline facet. *Phys. Rev. E, Rapid Communications* **69** (2004), 035102(R).

[FerSpo] Ferrari, P., Spohn, H., Step fluctuations for a faceted crystal. *J. Statist. Phys.* **113** (1–2) (2003), 1–46.

[Fis] Fisher, M. E., Walks, walls, wetting and melting. *J. Statist. Phys.* **34** (1984), 667–729.

[For1] Forrester, P. J., The spectrum edge of random matrix ensembles. *Nuclear Phys. B* **402** (3) (1993), 709–728.

[For2] Forrester, P. J., Growth models, random matrices and Painlevé transcendents. *Nonlinearity* **16** (6) (2003), R27–R49.

[For3] Forrester, P. J., Random walks and random permutations. *J. Phys. A* **34** (31) (2001), L417–L423.

[Ges] Gessel, I. M., Symmetric functions and P-recursiveness. *J. Combin. Theory Ser. A* **53** (2) (1990), 257–285.

[GOV] Guttmann, A. J., Owczarek, A. L.,Viennot, X. G., Vicious walkers and Young tableaux. I. Without walls. *J. Phys. A* **31** (40) (1998), 8123–8135.

[JMMS] Jimbo, M., Miwa, T., Môri, Y., Sato, M., Density matrix of an impenetrable Bose gas and the fifth Painlevé transcendent. *Phys. D* **1** (1) (1980), 80–158.

[JPS] Jockusch, W., Propp, J., Shor, P., Random domino tilings and the arctic circle theorem. arXiv:math.CO/9801068.

[Joh1] Johansson, K., Discrete orthogonal polynomial ensembles and the Plancherel measure. *Ann. of Math.* (2) **153** (1) (2001), 259–296.

[Joh2] Johansson, K., Non-intersecting paths, random tilings and random matrices. *Probab. Theory Related Fields* **123** (2) (2002), 225–280.

[John] Johnstone, I. M., On the distribution of the largest eigenvalue in principal components analysis. *Ann. Statist.* **29** (2) (2001), 295–327.

[KatSar] Katz, N. M., Sarnak, P., *Random matrices, Frobenius eigenvalues, and monodromy.* Amer. Math. Soc. Colloq. Publ. 45, Amer. Math. Soc., Providence, R.I., 1999.

[KeaSna1] Keating, J. P., Snaith, N. C., Random matrix theory and $\zeta(1/2+it)$. *Comm. Math. Phys.* **214** (1) (2000), 57–89.

[KeaSna2] Keating, J. P., Snaith, N.,C. Random matrix theory and L-functions at $s = 1/2$. *Comm. Math. Phys.* **214** (1) (2000), 91–110.

[KrbSeb] Krbálek, M., Šeba, P., Statistical properties of the city transport in Cuernavaca (Mexico) and random matrix theory. *J. Phys. A: Math. Gen.* **33** (2000), 229–234.

[Mal] Mallows, C. E., Patience sorting. *Bull. Inst. Math. Appl.* **9** (1973), 216–224.

[Meh] Mehta, M., *Random Matrices*. Third edition, Pure and Appl. Math. 142, Elsevier/Academic Press, Amsterdam 2004.

[Mon] Montgomery, H., The pair correlation of zeros of the zeta function. In *Analytic number theory* (St. Louis Univ., St. Louis, Mo., 1972), Proc. Sympos. Pure Math. XXIV, Amer. Math. Soc., Providence, R.I., 1973, 181–193.

[Odl1] Odlyzko, A. M., The 10^{20}-th zero of the Riemann zeta function and 70 million of its neighbors. ATT Bell Laboratories preprint, 1989; available at http://www.research.att.com/~amo/doc/zeta.html.

[Odl2] Odlyzko, A. M., The 10^{22}-nd zero of the Riemann zeta function. In *Dynamical, spectral, and arithmetic zeta functions* (San Antonio, TX, 1999), Contemp. Math. 290, Amer. Math. Soc., Providence, R.I., 2001, 139–144.

[Oko] Okounkov, A., Random matrices and random permutations. *Internat. Math. Res. Notices* **20** (2000), 1043–1095.

[OkoRes] Okounkov, A., Reshetikhin, N., Correlation function of Schur process with application to local geometry of a random 3-dimensional Young diagram. *J. Amer. Math. Soc.* **16** (3) (2003), 3, 581–603.

[PasSch] Pastur, L., Shcherbina, M., Universality of the local eigenvalue statistics for a class of unitary invariant random matrix ensembles. *J. Statist. Phys.* **86** (1–2) (1997), 109–147.

[Por] Porter, C. E. (Ed), *Statistical theories of spectra: fluctuations*. Academic Press, New York 1965.

[PraSpo] Prähofer, M., Spohn, H., Scale invariance of the PNG droplet and the Airy process. Dedicated to David Ruelle and Yasha Sinai on the occasion of their 65th birthdays. *J. Statist. Phys.* **108** (5–6) (2002), 1071–1106.

[RudSar] Rudnick, Z., Sarnak, P., Zeros of principal L-functions and random matrix theory. A celebration of John F. Nash, Jr. *Duke Math. J.* **81** (2) (1996), 269–322.

[Sag] Sagan, B. E., *The symmetric group. Representations, combinatorial algorithms, and symmetric functions*. Second edition, Grad. Texts in Math. 203, Springer-Verlag, New York 2001.

[Sui] Suidan, T., A remark on a theorem of Chatterjee and last passage percolation. *J. Phys. A* **39** (28) (2006), 8977–8981.

[TraWid1] Tracy, C. A., Widom, H., Level-spacing distributions and the Airy kernel. *Comm. Math. Phys.* **159** (1) (1994), 151–174.

[TraWid2] Tracy, C. A., Widom, H., Correlation functions, cluster functions, and spacing distributions for random matrices. *J. Statist. Phys.* **92** (5–6) (1998), 809–835.

[TraWid3] Tracy, C. A., Widom, H., Universality of the distribution functions of random matrix theory. In *Integrable systems: from classical to quantum* (Montréal, QC, 1999), CRM Proc. Lecture Notes 26, Amer. Math. Soc., Providence, RI, 2000, 251–264.

[TraWid4] Tracy, C. A., Widom, H., On the distributions of the lengths of the longest monotone subsequences in random words. *Probab. Theory Related Fields* **119** (3) (2001), 350–380.

[Wag] Wagon, S., Is Pi normal? *Math. Intelligencer* **7** (1985), 65–67.

[Wid] Widom, H., On the relation between orthogonal, symplectic and unitary matrix ensembles. *J. Statist. Phys.* **94** (1999), 347–363.

[Wig1] Wigner, E., Results and theory of resonance absorbtion. In *Conference on neutron physics by time-of-flight* (Gatlinburg, Tennessee), Oak Ridge Natl. Lab. Rept. ORNL-2309, 1957, 59–70.

[Wig2] Wigner, E., Statistical properties of real symmetric matrices with many dimmensions. *Can. Math. Congr. Proc.*, University of Toronto Press, Toronto 1957, 174–184.

[Wig3] Wigner, E., Distribution of neutron resonance level spacing. In *International conference on the neutron interactions with the nucleus* (Columbia University, New York, 1957), Columbia Univ. Rept. CU-175 (TID-7547), 1957, 49–50.

Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street,
New York, NY 10012, U.S.A.

E-mail: deift@cims.nyu.edu

Kähler manifolds and transcendental techniques in algebraic geometry

Jean-Pierre Demailly

Abstract. Our goal is to survey some of the main advances which took place recently in the study of the geometry of projective or compact Kähler manifolds: very efficient new transcendental techniques, a better understanding of the geometric structure of cones of positive cohomology classes and of the deformation theory of Kähler manifolds, new results around the invariance of plurigenera and in the minimal model program.

Mathematics Subject Classification (2000). Primary 14C30; Secondary 32C17, 32C30, 32L20.

Keywords. Projective variety, Kähler manifold, Hodge theory, positive current, Monge–Ampère equation, Lelong number, Chern connection, curvature, Bochner–Kodaira technique, Kodaira embedding theorem, Kähler cone, ample divisor, nef divisor, pseudo-effective cone, Neron–Severi group, L^2 estimates, vanishing theorem, Ohsawa–Takegoshi extension theorem, pluricanonical ring, invariance of plurigenera.

1. Introduction

Modern algebraic geometry is one the most intricate crossroads between various branches of mathematics: commutative algebra, complex analysis, global analysis on manifolds, partial differential equations, differential topology, symplectic geometry, number theory…. This interplay has already been strongly emphasized by historical precursors, including Hodge, Kodaira, Hirzebruch and Grauert. Of course, there have been also fruitful efforts to establish purely algebraic foundations of the major results of algebraic geometry, and many prominent mathematicians such as Grothendieck, Deligne and Mumford stand out among the founders of this trend. The present contribution stands closer to the above mentioned wider approach; its goal is to explain some recent applications of local and global complex analytic methods to the study of projective algebraic varieties.

A unifying theme is the concept of positivity: ample line bundles are characterized by the positivity of their curvature in the complex geometric setting (Kodaira [35]). Projective manifolds thus appear as a subclass of the class of compact Kähler manifolds, and their cohomological properties can be derived from the study of harmonic forms on Kähler manifolds (Hodge theory). In this vein, another central concept is the concept of positive current, which was introduced by P. Lelong during the 50s.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

By carefully studying the singularities and the intersection theory of such currents, we derive precise structure theorems for the Kähler cone and for the cone of effective divisors of arbitrary projective varieties ([5], [18]).

L^2 estimates for solutions of $\overline{\partial}$ equations are another crucial technique for proving vanishing theorems for the cohomology of holomorphic vector bundles or sheaves. A combination of the Bochner–Kodaira differential geometric estimate with PDE techniques of Kohn, Hörmander and Andreotti–Vesentini led in the 60s to powerful existence theorems for $\overline{\partial}$-equations in hermitian vector bundles of positive curvature. A more recent and equally decisive outcome is the L^2 extension theorem by Ohsawa and Takegoshi [48] in 1987. Among applications, we have various forms of approximation theorems (closed positive $(1,1)$-currents can be approximated by algebraic divisors, and their singularities can be approximated by algebraic singularities). In the analytic setting, this turns out to be the key for the study of adjunction theory (generation properties of adjoint linear systems $K_X + L$, pluricanonical embeddings…). As an illustration, we present a recent proof, adapted from work by Y. T. Siu [58], [59], S. Takayama [62] and M. Păun [52], of the deformation invariance of plurigenera $h^0(X_t, mK_{X_t})$, for an arbitrary projective family (X_t) of algebraic varieties.

2. Basic concepts and results of complex geometry

This section mostly contains only well-known definitions and results. However, we want to fix the notation and describe in detail our starting point.

2.1. Forms, currents, Kähler metrics. Let X be a compact complex manifold and $n = \dim_{\mathbb{C}} X$. In any local holomorphic coordinate system $z = (z_1, \ldots, z_n)$, a differential form u of type (p, q) can be written as a sum $u(z) = \sum_{|J|=p,|K|=q} u_{JK}(z)\, dz_J \wedge d\overline{z}_K$ extended to all increasing multi-indices J, K of length p, q, with the usual notation $dz_J = dz_{j_1} \wedge \cdots \wedge dz_{j_p}$. We are especially interested in *positive currents* of type (p, p)

$$T = i^{p^2} \sum_{|J|=|K|=p} T_{JK}(z) dz_J \wedge d\overline{z}_K.$$

Recall that a current is a differential form with distribution coefficients, and that a current is said to be positive if the distribution $\sum \lambda_j \overline{\lambda}_k T_{JK}$ is a positive real measure for all complex numbers λ_J (which implies $T_{KJ} = \overline{T}_{JK}$, hence $\overline{T} = T$). The coefficients T_{JK} are then complex measures – and the diagonal ones T_{JJ} are positive (real) measures.

A current is said to be closed if $dT = 0$ in the sense of distributions. Important examples of closed positive (p, p)-currents are currents of integration over codimension p analytic cycles $[A] = \sum c_j [A_j]$ where the current $[A_j]$ is defined by duality

as

$$\langle [A_j], u\rangle = \int_{A_j} u_{|A_j}$$

for every $(n-p, n-p)$ test form u on X. Another important example of $(1, 1)$-current is the Hessian form $T = i\partial\bar{\partial}\varphi$ of a plurisubharmonic function on an open set $\Omega \subset X$ (plurisubharmonic functions are upper semi-continuous functions satisfying the mean value inequality on complex analytic disc; they are characterized by positivity of $i\sum \partial^2\varphi/\partial z_j \partial \bar{z}_k \; dz_j \wedge d\bar{z}_k$). A *Kähler metric* on X is a positive definite hermitian $(1, 1)$-form

$$\omega(z) = i \sum_{1\le j,k\le n} \omega_{jk}(z) dz_j \wedge d\bar{z}_k \quad \text{such that } d\omega = 0,$$

with smooth coefficients. The manifold X is said to be *Kähler* if it possesses at least one Kähler metric ω. It is clear that every complex analytic and locally closed submanifold $X \subset \mathbb{P}^N_{\mathbb{C}}$ is Kähler (the restriction of the Fubini–Study metric $\omega_{FS} = \frac{i}{2\pi}\log(|z_0|^2 + |z_1|^2 + \cdots + |z_N|^2)$ to X is a Kähler metric). Especially projective algebraic varieties are Kähler.

2.2. Cohomology of compact Kähler manifolds. To every d-closed complex valued k-form or current α (resp. to every $\bar{\partial}$-closed complex valued (p, q)-form or current α) is associated its De Rham (resp. Dolbeault) cohomology class

$$\{\alpha\} \in H^{p+q}(X, \mathbb{C}) \quad (\text{resp. } H^{p,q}(X, \mathbb{C})).$$

This definition hides a nontrivial result, namely the fact that all cohomology groups involved (De Rham, Dolbeault, ...) can be defined either in terms of smooth forms or in terms of currents. In fact, if we consider the associated complexes of sheaves, forms and currents both provide acyclic resolutions of the same sheaf (locally constant functions, resp. holomorphic sections). One of the main results of Hodge theory, historically obtained by W. V. D. Hodge through the theory of harmonic forms, is the following fundamental

Theorem 2.1. *Let (X, ω) be a compact Kähler manifold. Then there is a canonical isomorphism*

$$H^k(X, \mathbb{C}) = \bigoplus_{p+q=k} H^{p,q}(X, \mathbb{C}),$$

where each group $H^{p,q}(X, \mathbb{C})$ can be viewed as the space of (p, q)-forms α which are harmonic with respect to ω, i.e. $\Delta_\omega \alpha = 0$.

Now observe that every analytic cycle $A = \sum \lambda_j A_j$ of codimension p with integral coefficients defines a cohomology class

$$\{[A]\} \in H^{p,p}(X, \mathbb{C}) \cap H^{2p}(X, \mathbb{Z})/\{\text{torsion}\} \subset H^{p,p}(X, \mathbb{C}) \cap H^{2p}(X, \mathbb{Q})$$

where $H^{2p}(X,\mathbb{Z})/\{\text{torsion}\} \subset H^{2p}(X,\mathbb{Q}) \subset H^{2p}(X,\mathbb{C})$ denotes the image of integral classes in complex cohomology. When X is a projective algebraic manifold, this observation leads to the following statement, known as the *Hodge conjecture* (which was to become one of the famous seven Millenium problems of the Clay Mathematics Institute).

Conjecture 2.2. Let X be a projective algebraic manifold. Then the space of "Hodge classes" $H^{p,p}(X,\mathbb{C}) \cap H^{2p}(X,\mathbb{Q})$ of type $(p,\,p)$ is generated by classes of algebraic cycles of codimension p with $\mathbb{Q}$-coefficients.

At present not much is known to support the positive direction of the Hodge conjecture, not even the case of *abelian varieties* (i.e. projective algebraic complex tori $X = \mathbb{C}/\Lambda$) – which is the reason why several experts believe that the conjecture could eventually lead to a counterexample. There are however a number of cases where the cohomology algebra can be explicitly computed in terms of the geometry, and which do satisfy the conjecture: flag manifolds (Schubert cycles generate the cohomology ring), moduli spaces of stable or parabolic bundles over a general curve (I. Biswas and M. S. Narasimhan [2]).

In the Kähler case the conjecture is trivially wrong as shown by a general complex torus possessing a line bundle with indefinite curvature. Moreover, by a recent result of C. Voisin [66], even a considerably weakened form of the conjecture – adding Chern classes of arbitrary coherent analytic sheaves to the pool of potential generators – is false for non projective complex tori:

Theorem 2.3 (C. Voisin [66]). *There exists a* 4*-dimensional complex torus X which possesses a non trivial Hodge class of degree* 4*, such that every coherent analytic sheaf $\mathcal{F}$ on X satisfies $c_2(\mathcal{F}) = 0$.*

The idea is to show the existence of a 4-dimensional complex torus $X = \mathbb{C}^4/\Lambda$ which does not contain any analytic subset of positive dimension, and such that the Hodge classes of degree 4 are perpendicular to ω^{n-2} for a suitable choice of the Kähler metric ω. The lattice Λ is explicitly found via a number theoretic construction of Weil based on the number field $\mathbb{Q}[i]$, also considered by S. Zucker [70]. The theorem of existence of Hermitian Yang–Mills connections for stable bundles combined with Lübke's inequality then implies $c_2(\mathcal{F}) = 0$ for every coherent sheaf $\mathcal{F}$ on the torus.

2.3. Fundamental L^2 existence theorems. Let X be a complex manifold and $(E,\,h)$ a hermitian holomorphic vector bundle of rank r over X. If $E_{|U} \simeq U \times \mathbb{C}^r$ is a local holomorphic trivialization, the hermitian product can be written as $\langle u,\,v\rangle = {}^t u H(z)\bar{v}$ where $H(z)$ is the hermitian matric of h and $u,\,v \in E_z$. It is well known that there exists a unique "Chern connection" $D = D^{1,0} + D^{0,1}$ such that $D^{0,1} = \overline{\partial}$ and such that D is compatible with the hermitian metric; in the given trivialization we have $D^{1,0}u = \overline{\partial}u + \Gamma^{1,0} \wedge u$ where $\Gamma^{1,0} = \overline{H}^{-1}\partial\overline{H}$, and its curvature operator $\Theta_{E,h} = D^2$ is the smooth section of $\Lambda^{1,1}T^*_X \otimes \mathrm{Hom}(E,\,E)$ given by $\Theta_{E,h} = \overline{\partial}(\overline{H}^{-1}\partial\overline{H})$. If E is

of rank $r = 1$, then it is customary to write $H(z) = e^{-\varphi(z)}$, and the curvature tensor then takes the simple expression $\Theta_{E,h} = \partial\overline{\partial}\varphi$. In that case the *first Chern class* of E is the cohomology class $c_1(E) = \left\{\frac{i}{2\pi}\Theta_{E,h}\right\} \in H^{1,1}(X, \mathbb{C})$, which is also an integral class in $H^2(X, \mathbb{Z})$).

In case (X, ω) is a Kähler manifold, the bundles $\Lambda^{p,q}T^*_X \otimes E$ are equipped with the hermitian metric induced by $\Lambda^{p,q}\omega \otimes h$, and we have a Hilbert space of global L^2 sections over X by integrating with respect to the Kähler volume form $dV_\omega = \omega^n/n!$. If A, B are differential operators acting on L^2 space of sections (in general, they are just closed and densely defined operators), we denote by A^* the formal adjoint of A, and by $[A, B] = AB - (-1)^{\deg A \deg B}BA$ the usual commutator bracket of operators. The fundamental operator Λ_ω of Kähler geometry is the adjoint of the wedge multiplication operator $u \mapsto \omega \wedge u$.

In this context we have the following fundamental existence theorems for $\overline{\partial}$-equations, which is the culmination of several decades of work by Bochner [3], Kodaira [35], Kohn [37], Andreotti–Vesentini [1], Hörmander [25], Skoda [60], Ohsawa–Takegoshi [48] (and many others). The proofs always proceed through differential geometric inequalities relating the Laplace–Beltrami operators with the curvature (Bochner–Kodaira identities and inequalities). The most basic result is the L^2 existence theorem for solutions of $\overline{\partial}$-equations.

Theorem 2.4 ([1], see also [10]). *Let (X, ω) be a Kähler manifold which is "complete" in the sense that it possesses a geodesically complete Kähler metric $\widetilde{\omega}$. Let E be a hermitian holomorphic vector bundle of rank r over X, and assume that the curvature operator $A^{p,q}_{E,h,\omega} = [i\Theta_{E,h}, \Lambda_\omega]$ is positive definite everywhere on $\Lambda^{p,q}T^\star_X \otimes E$, $q \geq 1$. Then for any form $g \in L^2(X, \Lambda^{p,q}T^\star_X \otimes E)$ satisfying $\overline{\partial}g = 0$ and $\int_X \langle (A^{p,q}_{E,h,\omega})^{-1}g, g\rangle\, dV_\omega < +\infty$, there exists $f \in L^2(X, \Lambda^{p,q-1}T^\star_X \otimes E)$ such that $\overline{\partial}f = g$ and*

$$\int_X |f|^2\, dV_\omega \leq \int_X \langle (A^{p,q}_{E,h,\omega})^{-1}g, g\rangle\, dV_\omega.$$

It is thus of crucial importance to study conditions under which the operator $A^{p,q}_{E,h,\omega}$ is positive definite. An easier case is when E is a line bundle. Then we denote by $\gamma_1(z) \leq \cdots \leq \gamma_n(z)$ the eigenvalues of the real $(1, 1)$-form $i\Theta_{E,h}(z)$ with respect to the metric $\omega(z)$ at each point. A straightforward calculation shows that

$$\langle A^{p,q}_{E,h,\omega}u, u\rangle = \sum_{|J|=p,|K|=q} \Big(\sum_{k\in K}\gamma_k - \sum_{j\in \complement J}\gamma_j\Big)|u_{JK}|^2.$$

In particular, for (n, q)-forms the negative sum $-\sum_{j\in\complement J}\gamma_j$ disappears and we have

$$\langle A^{n,q}_{E,h,\omega}u, u\rangle \geq (\gamma_1 + \cdots + \gamma_q)|u|^2, \quad \langle (A^{n,q}_{E,h,\omega})^{-1}u, u\rangle \leq (\gamma_1 + \cdots + \gamma_q)^{-1}|u|^2$$

provided the line bundle (E, h) has positive definite curvature. Therefore $\overline{\partial}$-equations can be solved for all L^2 (n, q)-forms with $q \geq 1$, and this is the major reason

why vanishing results for H^q cohomology groups are usually obtained for sections of the "*adjoint line bundle*" $\widetilde{E} = K_X \otimes E$, where $K_X = \Lambda^n T^*_X = \Omega^n_X$ is the "*canonical bundle*" of X, rather than for E itself. Especially, if X is compact (or weakly pseudoconvex) and $i\Theta_{E,h} > 0$, then $H^q(X, K_X \otimes E) = 0$ for $q \geq 1$ (Kodaira), and more generally $H^{p,q}(X, E) = 0$ for $p + q \geq n + 1$ (Kodaira–Nakano, take $\omega = i\Theta_{E,h}$, in which case $\gamma_j \equiv 1$ for all j and $\sum_{k\in K} \gamma_k - \sum_{j\in \complement J} \gamma_j = p + q - n$).

As shown in [10], Theorem 2.4 still holds true in that case when h is a *singular hermitian metric*, i.e. a metric whose weights φ are arbitrary locally integrable functions, provided that the curvature is (E, h) is positive in the sense of currents (i.e., the weights φ are strictly plurisubharmonic). This implies the well-known Nadel vanishing theorem ([42], [12], [15]), a generalization of the Kawamata–Viehweg vanishing theorem [28], [65].

Theorem 2.5 (Nadel). *Let (X, ω) be a compact (or weakly pseudoconvex) Kähler manifold, and (L, h) a singular hermitian line bundle such that $\Theta_{L,h} \geq \varepsilon\omega$ for some $\varepsilon > 0$. Then $H^q(X, K_X \otimes L \otimes \mathcal{I}(h)) = 0$ for $q \geq 1$, where $\mathcal{I}(h)$ is the multiplier ideal sheaf of h, namely the sheaf of germs of holomorphic functions f on X such that $|f|^2 e^{-\varphi}$ is locally integrable with respect to the local weights $h = e^{-\varphi}$.*

It is well known that Theorems 2.4 and 2.5, more specifically its "singular hermitian" version, imply almost all other fundamental vanishing or existence theorems of algebraic geometry, as well as their analytic counterparts in the framework of Stein manifolds (general solution of the Levi problem by Grauert), see e.g. Demailly [16] for a recent account. In particular, one gets as a consequence the *Kodaira embedding theorem* [35].

Theorem 2.6. *Let X be a compact complex n-dimensional manifold. Then the following properties are equivalent.*

(i) *X can be embedded in some projective space $\mathbb{P}^N_{\mathbb{C}}$ as a closed analytic submanifold (and such a submanifold is automatically algebraic by Chow's theorem).*

(ii) *X carries a hermitian holomorphic line bundle (L, h) with positive definite smooth curvature form $i\Theta_{L,h} > 0$.*

(iii) *X possesses a Hodge metric, i.e., a Kähler metric ω such that $\{\omega\} \in H^2(X, \mathbb{Z})$.*

If property (ii) *holds true, then for $m \geq m_0 \gg 1$ the multiple $L^{\otimes m}$ is very ample, namely we have an embedding given by the linear system $V = H^0(X, L^{\otimes m})$ of sections,*

$$\Phi_{L^{\otimes m}} : X \longrightarrow P(V^*), \quad z \mapsto H_z = \{\sigma \in V\,;\ \sigma(z) = 0\} \subset V,$$

and $L^{\otimes m} \simeq \Phi^*_{L^{\otimes m}} \mathcal{O}(1)$ is the pull-back of the canonical bundle on $P(V^*)$.

Another fundamental existence theorem is the L^2-extension result by Ohsawa–Takegoshi [48]. Many different versions and generalizations have been given in recent years [43], [44], [45], [46], [47]. Here is another one, due to Manivel [40], which is slightly less general but simpler to state.

Theorem 2.7 (Ohsawa–Takegoshi [48], Manivel [40]). *Let X be a compact or weakly pseudoconvex n-dimensional complex manifold equipped with a Kähler metric ω, let L (resp. E) be a hermitian holomorphic line bundle (resp. a hermitian holomorphic vector bundle of rank r over X), and s a global holomorphic section of E. Assume that s is generically transverse to the zero section, and let*

$$Y = \big\{x \in X\,;\ s(x) = 0,\, \Lambda^r ds(x) \neq 0\big\}, \quad p = \dim Y = n - r.$$

Moreover, assume that the $(1,1)$-form $i\Theta(L) + r\, i\, \partial\overline{\partial} \log |s|^2$ is semipositive and that there is a continuous function $\alpha \geq 1$ such that the following two inequalities hold everywhere on X:

(i) $i\Theta(L) + r\, i\, \partial\overline{\partial} \log |s|^2 \geq \alpha^{-1} \dfrac{\{i\Theta(E)s, s\}}{|s|^2}$,

(ii) $|s| \leq e^{-\alpha}$.

Then for every holomorphic section f over Y of the adjoint line bundle $\widetilde{L} = K_X \otimes L$ (restricted to Y), such that $\int_Y |f|^2 |\Lambda^r(ds)|^{-2} dV_\omega < +\infty$, there exists a holomorphic extension F of f over X, with values in $\widetilde{L}$, such that

$$\int_X \frac{|F|^2}{|s|^{2r}(-\log|s|)^2}\, dV_{X,\omega} \leq C_r \int_Y \frac{|f|^2}{|\Lambda^r(ds)|^2} dV_{Y,\omega}\,,$$

where C_r is a numerical constant depending only on r.

The proof actually shows that the extension theorem holds true as well for $\overline{\partial}$-closed $(0,q)$-forms with values in $\widetilde{L}$, of which the stated theorem is the special case $q = 0$.

There are several other important L^2 existence theorems. One of them is Skoda's criterion for the surjectivity of holomorphic bundle morphisms – more concretely, a Bezout type division theorem for holomorphic function. It can be derived either from Theorem 2.4 on $\overline{\partial}$-equations through sharp curvature calculations (this is Skoda's original approach in [60]), or as a consequence of the above extension theorem 2.7 (see Ohsawa [46]).

2.4. Positive cones. We now introduce some further basic objects of projective or Kähler geometry, namely *cones of positive cohomology classes*.

Definition 2.8. Let X be a compact Kähler manifold and $H^{1,1}(X, \mathbb{R})$ the space of real $(1,1)$ cohomology classes.

(i) The *Kähler cone* is the set $\mathcal{K} \subset H^{1,1}(X, \mathbb{R})$ of cohomology classes $\{\omega\}$ of Kähler forms. This is clearly an open convex cone.

(ii) The *pseudo-effective* cone is the set $\mathcal{E} \subset H^{1,1}(X, \mathbb{R})$ of cohomology classes $\{T\}$ of closed positive currents of type $(1,1)$. This is a closed convex cone (as follows from the weak compactness property of bounded sets of positive measures or currents).

It follows from this definition that $\overline{\mathcal{K}} \subset \mathcal{E}$. In general the inclusion is strict. To see this, it is enough to observe that a Kähler class $\{\alpha\}$ satisfies $\int_Y \alpha^p > 0$ for every p-dimensional analytic set. On the other hand, if X is the surface obtained by blowing-up $\mathbb{P}^2$ in one point, then the exceptional divisor $E \simeq \mathbb{P}^1$ has a cohomology class $\{\alpha\}$ such that $\int_E \alpha = E^2 = -1$, hence $\{\alpha\} \notin \overline{\mathcal{K}}$, although $\{\alpha\} = \{[E]\} \in \mathcal{E}$.

In case X is projective it is interesting to consider also the algebraic analogues of our "transcendental cones" $\mathcal{K}$ and $\mathcal{E}$, which consist of suitable integral divisor classes. Since the cohomology classes of such divisors live in $H^2(X, \mathbb{Z})$, we are led to introduce the Neron–Severi lattice and the associated Neron–Severi space:

$$\begin{aligned} \mathrm{NS}(X) &:= H^{1,1}(X, \mathbb{R}) \cap \big(H^2(X, \mathbb{Z})/\{\text{torsion}\}\big), \\ \mathrm{NS}_{\mathbb{R}}(X) &:= \mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{R}. \end{aligned}$$

All classes of real divisors $D = \sum c_j D_j$, $c_j \in \mathbb{R}$, lie by definition in $\mathrm{NS}_{\mathbb{R}}(X)$. Notice that the integral lattice $H^2(X, \mathbb{Z})/\{\text{torsion}\}$ need not hit at all the subspace $H^{1,1}(X, \mathbb{R}) \subset H^2(X, \mathbb{R})$ in the Hodge decomposition, hence in general the *Picard number*, defined as

$$\rho(X) = \mathrm{rank}_{\mathbb{Z}} \mathrm{NS}(X) = \dim_{\mathbb{R}} \mathrm{NS}_{\mathbb{R}}(X),$$

satisfies $\rho(X) \le h^{1,1} = \dim_{\mathbb{R}} H^{1,1}(X, \mathbb{R})$, but the equality can be strict (actually, it is well known that a generic complex torus $X = \mathbb{C}^n/\Lambda$ satisfies $\rho(X) = 0$ and $h^{1,1} = n^2$). In order to deal with the case of algebraic varieties we introduce

$$\mathcal{K}_{\mathrm{NS}} = \mathcal{K} \cap \mathrm{NS}_{\mathbb{R}}(X), \quad \mathcal{E}_{\mathrm{NS}} = \mathcal{E} \cap \mathrm{NS}_{\mathbb{R}}(X).$$

A very important fact is that the "Neron–Severi part" of any of the open or closed transcendental cones $\mathcal{K}$, $\mathcal{E}$, $\overline{\mathcal{K}}$, $\mathcal{E}^\circ$ is algebraic, i.e. can be characterized in simple algebraic terms.

Theorem 2.9. *Let X be a projective manifold. Then*

(i) *$\mathcal{E}_{\mathrm{NS}}$ is the closure of the cone generated by classes of effective divisors, i.e. divisors $D = \sum c_j D_j$, $c_j \in \mathbb{R}_+$.*

(ii) *$\mathcal{K}_{\mathrm{NS}}$ is the open cone generated by classes of ample (or very ample) divisors A (recall that a divisor A is said to be very ample if the linear system $H^0(X, \mathcal{O}(A))$ provides an embedding of X in projective space).*

(iii) *The interior $\mathcal{E}^\circ_{\mathrm{NS}}$ is the cone generated by classes of big divisors, namely divisors D such that $h^0(X, \mathcal{O}(kD)) \ge c\, k^{\dim X}$ for k large.*

(iv) *The closed cone $\overline{\mathcal{K}}_{\mathrm{NS}}$ consists of the closure of the cone generated by nef divisors D (or nef line bundles L), namely effective integral divisors D such that $D \cdot C \ge 0$ for every curve C.*

By extension, we will say that $\overline{\mathcal{K}}$ is the cone of *nef* $(1,1)$-cohomology classes (even though they are not necessarily integral).

Sketch of proof (see also [13] for more details). If we denote by $\mathcal{K}_{\mathrm{alg}}$ the open cone generated by ample divisors, resp. by $\mathcal{E}_{\mathrm{alg}}$ the closure of the cone generated by effective divisors, we have $K_{\mathrm{alg}} \subset K_{\mathrm{NS}}$, $\mathcal{E}_{\mathrm{alg}} \subset \mathcal{E}_{\mathrm{NS}}$, and clearly the interesting part lies in the converse inclusions. The inclusion $K_{\mathrm{NS}} \subset \mathcal{K}_{\mathrm{alg}}$ is equivalent to the Kodaira embedding theorem: if a rational class $\{\alpha\}$ is in $\mathcal{K}$, then some multiple of $\{\alpha\}$ is the first Chern class of a hermitian line bundle L whose curvature form is Kähler. Therefore L is ample and $\{\alpha\} \in \mathcal{K}_{\mathrm{alg}}$; property (ii) follows.

Similarly, if we take a rational class $\{\alpha\} \in \mathcal{E}^{\circ}_{\mathrm{NS}}$, then we still have $\{\alpha - \varepsilon\omega\} \in \mathcal{E}^{\circ}_{\mathrm{NS}}$ by subtracting a small multiple $\varepsilon\omega$ of a Kähler class, hence $\alpha - \varepsilon\omega \equiv T \geq 0$ for some positive current T. Therefore some multiple $\{m_0\alpha\}$ is the first Chern class of a hermitian line bundle (L, h) with curvature current T:

$$\Theta_{L,h} := -\frac{i}{2\pi} i\partial\bar{\partial} \log h = m_0(T + \varepsilon\omega) \geq m_0\varepsilon\omega.$$

Theorem 2.4 on L^2 estimates for $\bar{\partial}$-equations then shows that large multiples $L^{\otimes k}$ admit a large number of sections, hence $L^{\otimes k}$ can be represented by a big divisor. This implies (iii) and also that $\mathcal{E}^{\circ}_{\mathrm{NS}} \subset \mathcal{E}_{\mathrm{alg}}$. Therefore $\mathcal{E}_{\mathrm{NS}} \subset \mathcal{E}_{\mathrm{alg}}$ by passing to the closure; (i) follows. The statement (iv) about nef divisors follows e.g. from Klaiman [34] and Hartshorne [24], since every nef divisor is a limit of a sequence of ample rational divisors. □

As a natural extrapolation of the algebraic situation, we say that $\overline{\mathcal{K}}$ is the cone of *nef* $(1,1)$-cohomology classes (even though these classes are not necessarily integral). Property 2.9 (i) also explains the terminology used for the pseudo-effective cone.

2.5. Approximation of currents and Zariski decomposition. Let X be compact Kähler manifold and let $\alpha \in \mathcal{E}^{\circ}$ be in the *interior* of the pseudo-effective cone. In analogy with the algebraic context, such a class α is called "big", and it can then be represented by a *Kähler current* T, i.e. a closed positive $(1,1)$-current T such that $T \geq \delta\omega$ for some smooth hermitian metric ω and a constant $\delta \ll 1$. Notice that the latter definition of a Kähler current makes sense even if X is an arbitrary (non necessarily Kähler) compact complex manifold.

Theorem 2.10 (Demailly [14], Boucksom [4], 3.1.24). *If T is a Kähler current on a compact complex manifold X, then one can write $T = \lim T_m$ for a sequence of Kähler currents T_m in the same cohomology class as T, which have logarithmic poles and coefficients in $\frac{1}{m}\mathbb{Z}$. This means that there are modifications $\mu_m : \widetilde{X}_m \to X$ such that*

$$\mu_m^{\star} T_m = [E_m] + \beta_m$$

where E_m is an effective $\mathbb{Q}$-divisor on $\widetilde{X}_m$ with coefficients in $\frac{1}{m}\mathbb{Z}$ (E_m is the "fixed part" and β_m a closed semi-positive form, the "movable part").

Proof. We just recall the main idea and refer to [14] for details. Locally we can write $T = i\partial\bar\partial\varphi$ for some strictly plurisubharmonic potential φ on X. The approximating potentials φ_m of φ are defined as

$$\varphi_m(z) = \frac{1}{2m}\log\sum_\ell |g_{\ell,m}(z)|^2$$

where $(g_{\ell,m})$ is a Hilbert basis of the space $\mathcal{H}(\Omega, m\varphi)$ of holomorphic functions which are L^2 with respect to the weight $e^{-2m\varphi}$. The Ohsawa–Takegoshi L^2 extension theorem 2.7 (applied to extension from a single isolated point) implies that there are enough such holomorphic functions, and thus $\varphi_m \ge \varphi - C/m$. On the other hand $\varphi = \lim_{m\to+\infty}\varphi_m$ by a Bergman kernel trick and by the mean value inequality.

The Hilbert basis $(g_{\ell,m})$ is also a family of local generators of the globally defined multiplier ideal sheaf $\mathcal{I}(mT) = \mathcal{I}(m\varphi)$. The modification $\mu_m\colon \widetilde{X}_m \to X$ is obtained by blowing-up this ideal sheaf, so that

$$\mu_m^\star\mathcal{I}(mT) = \mathcal{O}(-mE_m)$$

for some effective $\mathbb{Q}$-divisor E_m with normal crossings on $\widetilde{X}_m$. Now we set $T_m = i\partial\bar\partial\varphi_m$ and $\beta_m = \mu_m^* T_m - [E_m]$. Then $\beta_m = i\partial\bar\partial\psi_m$ where

$$\psi_m = \frac{1}{2m}\log\sum_\ell |g_{\ell,m}\circ\mu_m/h|^2 \quad \text{locally on } \widetilde{X}_m$$

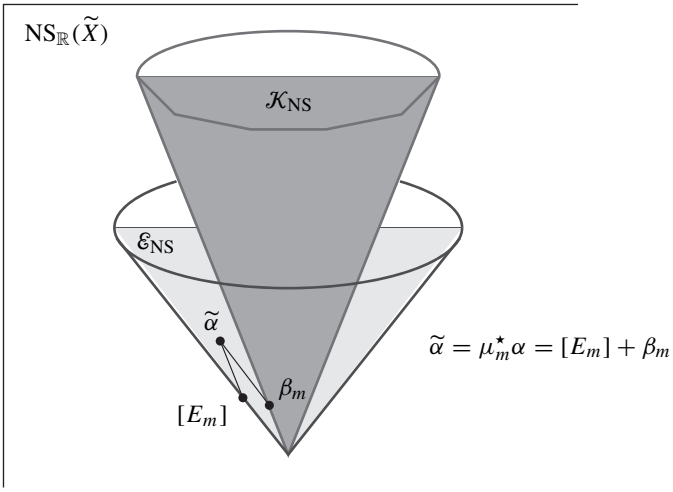
and h is a generator of $\mathcal{O}(-mE_m)$, and we see that β_m is a smooth semi-positive form on $\widetilde{X}_m$. The construction can be made global by using a gluing technique, e.g. via partitions of unity. □

Remark 2.11. The more familiar algebraic analogue would be to take $\alpha = c_1(L)$ with a big line bundle L and to blow-up the base locus of $|mL|$, $m \gg 1$, to get a $\mathbb{Q}$-divisor decomposition

$$\mu_m^\star L \sim E_m + D_m, \quad E_m \text{ effective, } D_m \text{ free.}$$

Such a blow-up is usually referred to as a "log resolution" of the linear system $|mL|$, and we say that $E_m + D_m$ is an approximate Zariski decomposition of L. We will also use this terminology for Kähler currents with logarithmic poles.

In the above construction β_m is not just semi-positive, it is even positive definite on tangent vectors which are not mapped to 0 by the differential $d\mu_m$, in particular β_m is positive definite outside the exceptional divisor. However, if E is the exceptional divisor of the blow-up along a smooth centre $Y \subset X$, then $\mathcal{O}(-E)$ is relatively ample with respect to the blow-up map π, hence the negative current $-[E]$ is cohomologous to a smooth form θ_E which is positive along the fibers of π. As a consequence, we can slightly perturb the decomposition of $\widetilde{\alpha}$ by increasing multiplicities in the



components of E_m and adding recursively to β_m small multiples $\varepsilon_E \theta_E$ in such a way that $\widetilde{\beta}_m + \sum \varepsilon_E \theta_E$ becomes a Kähler metric on $\widetilde{X}_m$. This in turn implies that $\widetilde{X}_m$ is Kähler and we thus get the following characterization of the Fujiki class $\mathcal{C}$ of compact complex manifolds which are bimeromorphic to Kähler manifolds:

Corollary 2.12. *A compact complex manifold is bimeromorphic to a Kähler manifold* (*or equivalently, dominated by a Kähler manifold*) *if and only if it carries a Kähler current* T.

3. Numerical characterization of the Kähler cone

We describe here the main results obtained in Demailly–Păun [18]. The upshot is that the Kähler cone depends only on the intersection product of the cohomology ring, the Hodge structure and the homology classes of analytic cycles. More precisely, we have:

Theorem 3.1. *Let X be a compact Kähler manifold. Let $\mathcal{P}$ be the set of real* $(1,1)$ *cohomology classes $\{\alpha\}$ which are numerically positive on analytic cycles, i.e. such that $\int_Y \alpha^p > 0$ for every irreducible analytic set Y in X, $p = \dim Y$. Then the Kähler cone $\mathcal{K}$ of X is one of the connected components of $\mathcal{P}$.*

Corollary 3.2. *If X is projective algebraic, then $\mathcal{K} = \mathcal{P}$.*

These results (which are new even in the projective case) can be seen as a generalization of the well-known Nakai–Moishezon criterion. Recall that the Nakai–Moishezon criterion provides a necessary and sufficient criterion for a line bundle to

be ample: *a line bundle $L \to X$ on a projective algebraic manifold X is ample if and only if*

$$L^p \cdot Y = \int_Y c_1(L)^p > 0,$$

for every algebraic subset $Y \subset X$, $p = \dim Y$.

It turns out that the numerical conditions $\int_Y \alpha^p > 0$ also characterize arbitrary transcendental Kähler classes when X is projective: this is precisely the meaning of Corollary 3.2.

Example 3.3. The following example shows that the cone $\mathcal{P}$ need not be connected (and that the components of $\mathcal{P}$ need not be convex, either). Consider for instance a complex torus $X = \mathbb{C}^n/\Lambda$. It is well-known that a generic torus X does not possess any analytic subset except finite subsets and X itself. In that case the numerical positivity is expressed by the single condition $\int_X \alpha^n > 0$. However, on a torus, $(1, 1)$-classes are in one-to-one correspondence with constant hermitian forms α on $\mathbb{C}^n$. Thus, for X generic, $\mathcal{P}$ is the set of hermitian forms on $\mathbb{C}^n$ such that $\det(\alpha) > 0$, and Theorem 3.1 just expresses the elementary result of linear algebra saying that the set $\mathcal{K}$ of positive definite forms is one of the connected components of the open set $\mathcal{P} = \{\det(\alpha) > 0\}$ of hermitian forms of positive determinant (the other components, of course, are the sets of forms of signature (p, q), $p + q = n$, q even; they are not convex when $p > 0$ and $q > 0$).

Sketch of proof of Theorem 3.1 *and Corollary* 3.2. As is well known, the singularities of a closed positive current T can be measured by its *Lelong numbers*

$$\nu(T, x) = \liminf_{z \to x} \frac{\varphi(z)}{\log |z - x|},$$

where $T = \frac{i}{\pi}\partial\bar{\partial}\varphi$ near x. A fundamental theorem of Siu [56] states that the Lelong sublevel sets $E_c(T) := \{x \in X\,;\ \nu(T, x) \geq c\}$ are *analytic sets* for every $c > 0$ (this fact can nowadays be derived in a rather straightforward manner from the approximation theorem 2.10). The crucial steps of the proof of Theorem 3.1 are contained in the following statements.

Proposition 3.4 (Păun [49], [50]). *Let X be a compact complex manifold* (*or more generally a compact complex space*). *Then*

(i) *The cohomology class of a closed positive* $(1, 1)$*-current $\{T\}$ is nef if and only if the restriction $\{T\}_{|Z}$ is nef for every irreducible component Z in any of the Lelong sublevel sets $E_c(T)$.*

(ii) *The cohomology class of a Kähler current $\{T\}$ is a Kähler class* (*i.e. the class of a* smooth *Kähler form*) *if and only if the restriction $\{T\}_{|Z}$ is a Kähler class for every irreducible component Z in any of the Lelong sublevel sets $E_c(T)$.*

The proof of Proposition 3.4 is not extremely hard if we take for granted the fact that Kähler currents can be approximated by Kähler currents with logarithmic poles, a fact which was proved in Demailly [14] (see also Theorem 2.10 below). The main point then consists in an induction on dimension and a standard gluing procedure: if $T = \alpha + \frac{i}{\pi}\partial\overline{\partial}\varphi$ where φ is smooth on $X \smallsetminus Z$ and has $-\infty$ poles along Z, then we can remove the poles of φ by replacing φ with $\max(\varphi, \psi - C)$, provided ψ is smooth and defined near Z and C is a large constant. □

The next (and more substantial step) consists of the following result which is reminiscent of the Grauert–Riemenschneider conjecture (Siu [57], Demailly [11]).

Theorem 3.5 (Demailly–Păun [18]). *Let X be a compact Kähler manifold and let $\{\alpha\}$ be a nef class (i.e. $\{\alpha\} \in \overline{\mathcal{K}}$). Assume that $\int_X \alpha^n > 0$. Then $\{\alpha\}$ contains a Kähler current T, in other words $\{\alpha\} \in \mathcal{E}^\circ$.*

Proof. The basic argument is to prove that for every irreducible analytic set $Y \subset X$ of codimension p, the class $\{\alpha\}^p$ contains a closed positive (p, p)-current Θ such that $\Theta \geq \delta[Y]$ for some $\delta > 0$. We check this by observing that $\alpha + \varepsilon\omega$ is a Kähler class, hence by the Calabi–Yau theorem Yau [69] the Monge–Ampère equation

$$(\alpha + \varepsilon\omega + i\,\partial\overline{\partial}\varphi_\varepsilon)^n = f_\varepsilon$$

can be solved with an arbitrary right-hand side $f_\varepsilon > 0$ such that

$$\int_X f_\varepsilon = C_\varepsilon = \int_X (\alpha + \varepsilon\omega)^n.$$

However, by our assumption that $\int_X \alpha^n > 0$, the constant C_ε is bounded away from 0. We use this fact in order to concentrate a fixed amount of volume of the volume form f_ε in an ε-tubular neighborhood of Y. We then show that the sequence of (p, p)-forms $(\alpha + \varepsilon\omega + i\,\partial\overline{\partial}\varphi_\varepsilon)^p$ converges weakly to the desired current Θ (this part relies heavily on the theory of currents). The second and final part uses a "diagonal trick": apply the result just proved to

$$\widetilde{X} = X \times X, \quad \widetilde{Y} = \text{diagonal} \subset \widetilde{X}, \quad \widetilde{\alpha} = \mathrm{pr}_1^*\,\alpha + \mathrm{pr}_2^*\,\alpha.$$

It is then clear that $\widetilde{\alpha}$ is nef on $\widetilde{X}$ and that $\int_{\widetilde{X}} (\widetilde{\alpha})^{2n} > 0$. It follows by the above that the class $\{\widetilde{\alpha}\}^n$ contains a Kähler current Θ such that $\Theta \geq \delta[\widetilde{Y}]$ for some $\delta > 0$. Therefore the push-forward

$$T := (\mathrm{pr}_1)_*(\Theta \wedge \mathrm{pr}_2^*\,\omega)$$

is numerically equivalent to a multiple of α and dominates $\delta\omega$, and we see that T is a Kähler current. □

End of proof of Theorem 3.1. Clearly the open cone $\mathcal{K}$ is contained in $\mathcal{P}$, hence in order to show that $\mathcal{K}$ is one of the connected components of $\mathcal{P}$, we need only show

that $\mathcal{K}$ is closed in $\mathcal{P}$, i.e. that $\overline{\mathcal{K}} \cap \mathcal{P} \subset \mathcal{K}$. Pick a class $\{\alpha\} \in \overline{\mathcal{K}} \cap \mathcal{P}$. In particular $\{\alpha\}$ is nef and satisfies $\int_X \alpha^n > 0$. By Theorem 3.5 we conclude that $\{\alpha\}$ contains a Kähler current T. However, an induction on dimension using the assumption $\int_Y \alpha^p$ for all analytic subsets Y (we also use resolution of singularities for Y at this step) shows that the restriction $\{\alpha\}_{|Y}$ is the class of a Kähler current on Y. We conclude that $\{\alpha\}$ is a Kähler class by 3.4 (ii), therefore $\{\alpha\} \in \mathcal{K}$, as desired. □

The projective case 3.2 is a consequence of the following variant of Theorem 3.1.

Corollary 3.6. *Let X be a compact Kähler manifold. A $(1,1)$ cohomology class $\{\alpha\}$ on X is Kähler if and only if there exists a Kähler metric ω on X such that $\int_Y \alpha^k \wedge \omega^{p-k} > 0$ for all irreducible analytic sets Y and all $k = 1, 2, \ldots, p = \dim Y$.*

Proof. The assumption clearly implies that

$$\int_Y (\alpha + t\omega)^p > 0$$

for all $t \in \mathbb{R}_+$, hence the half-line $\alpha + (\mathbb{R}_+)\omega$ is entirely contained in the cone $\mathcal{P}$ of numerically positive classes. Since $\alpha + t_0\omega$ is Kähler for t_0 large, we conclude that the half-line in entirely contained in the connected component $\mathcal{K}$, and therefore $\alpha \in \mathcal{K}$. □

In the projective case we can take $\omega = c_1(H)$ for a given very ample divisor H, and the condition $\int_Y \alpha^k \wedge \omega^{p-k} > 0$ is equivalent to $\int_{Y \cap H_1 \cap \cdots \cap H_{p-k}} \alpha^k > 0$ for a suitable complete intersection $Y \cap H_1 \cap \cdots \cap H_{p-k}$, $H_j \in |H|$. This shows that algebraic cycles are sufficient to test the Kähler property, and the special case 3.2 follows. On the other hand, we can pass to the limit in 3.6 by replacing α by $\alpha + \varepsilon\omega$, and in this way we get also a characterization of nef classes.

Corollary 3.7. *Let X be a compact Kähler manifold. A $(1,1)$ cohomology class $\{\alpha\}$ on X is nef if and only if there exists a Kähler metric ω on X such that $\int_Y \alpha^k \wedge \omega^{p-k} \geq 0$ for all irreducible analytic sets Y and all $k = 1, 2, \ldots, p = \dim Y$.*

By a formal convexity argument one can derive from 3.6 or 3.7 the following interesting consequence about the dual of the cone $\mathcal{K}$.

Theorem 3.8. *Let X be a compact Kähler manifold. A $(1,1)$ cohomology class $\{\alpha\}$ on X is nef if and only for every irreducible analytic set Y in X, $p = \dim X$ and every Kähler metric ω on X we have $\int_Y \alpha \wedge \omega^{p-1} \geq 0$. In other words, the dual of the nef cone $\overline{\mathcal{K}}$ is the closed convex cone in $H^{n-1,n-1}_{\mathbb{R}}(X)$ generated by cohomology classes of currents of the form $[Y] \wedge \omega^{p-1}$ in $H^{n-1,n-1}(X, \mathbb{R})$, where Y runs over the collection of irreducible analytic subsets of X and $\{\omega\}$ over the set of Kähler classes of X.* □

4. Deformations of compact Kähler manifolds

If S is an analytic space, recall that a deformation of compact complex manifolds is a proper holomorphic map $\pi : \mathcal{X} \to S$ such that the fibers are smooth and such that $\mathcal{X}$ is locally the product of the base by a neighborhood of any point in any fiber (with π being the first projection of such a local decomposition). For any $t \in S$, we denote by $X_t = \pi^{-1}(t)$ the fiber over t.

Since compact Kähler manifolds share many common features with projective algebraic manifolds – e.g. good Hodge theoretic properties – rather strong properties are expected for their deformation theory. Kodaira showed in the 60s that every Kähler surface X is a limit by deformation of algebraic surfaces, namely there exists a deformation $\mathcal{X} \to S$ such that $X = X_{t_0}$ for some t_0, and X_{t_m} is projective algebraic for a sequence $t_m \to t_0$. It was therefore a natural – and long-standing – question whether a similar property holds in higher dimensions. C. Voisin showed in a series of recent papers that the general answer is negative, and in fact there exist rigid non projective compact Kähler manifolds.

Theorem 4.1 (recent results by C. Voisin). (i) *In any dimension* ≥ 4*, there exist compact Kähler manifolds which do not have the homotopy type* (*or even the homology ring*) *of a complex projective manifold* ([67]).

(ii) *In any dimension* ≥ 8*, there exist compact Kähler manifolds* X *such that no compact bimeromorphic model* X' *of* X *has the homotopy type of a complex projective manifold* ([68]).

The example in (i) is obtained by selecting a complex torus T of dimension ≥ 2 possessing a linear endomorphism φ which has non real eigenvalues (pairwise distinct and non conjugate). Then X is obtained by blowing-up the finite set of pairwise intersection points of the four subsets $T \times \{0\}$, $\{0\} \times T$, $\Delta =$ diagonal, $G_\varphi =$ graph of φ, and then their strict transforms in the first stage blow-up. By using rather elementary considerations of Hodge theory, this provides an example of a rigid Kähler variety which does not have the homotopy type of a projective variety. The example in (ii) is obtained via the Poincaré bundle on $T \times \hat{T}$; we refer to [67] and [68] for details. □

Another fundamental fact proved by Kodaira and Spencer [36] is the observation that the Kähler property is open with respect to deformation: if X_{t_0} is Kähler for some $t_0 \in S$, then the nearby fibers X_t (for t in a metric topology neighborhood of t_0 in S) is also Kähler. The proof consists in showing that the desired Kähler metrics are solutions of a suitably chosen 4-th order elliptic differential operator for which there is no jump of the kernel at t_0. However, the numerous known examples leave hopes for a much stronger openness property.

Conjecture 4.2. Let $\mathcal{X} \to S$ be a deformation with irreducible base space S such that some fiber X_{t_0} is Kähler. Then there should exist a finite (or possibly countable) union of analytic strata $S_\nu \subset S$, $S_\nu \neq S$, such that

(i) X_t is Kähler for $t \in S \setminus \bigcup S_\nu$,

(ii) X_t is bimeromorphic to a Kähler manifold for $t \in \bigcup S_\nu$.

A crucial step in analyzing the conjecture is to describe the behaviour of the Kähler cone of X_t as t approaches the "bad strata". This question is now fully understood thanks to the following result which is a direct corollary of our characterization of the Kähler cone (Theorem 3.1). As a consequence, a "collapse" of the Kähler cone could only come from a degeneration of the Hodge decomposition, the behaviour of which is complex analytic thanks to the Frölicher spectral sequence.

Theorem 4.3 (Demailly–Păun [18]). *Let $\pi : \mathcal{X} \to S$ be a deformation of compact Kähler manifolds over an irreducible base S. Then there exists a countable union $S' = \bigcup S_\nu$ of analytic subsets $S_\nu \subsetneq S$, such that the Kähler cones $\mathcal{K}_t \subset H^{1,1}(X_t, \mathbb{C})$ of the fibers $X_t = \pi^{-1}(t)$ are invariant over $S \setminus S'$ under parallel transport with respect to the $(1,1)$-projection $\nabla^{1,1}$ of the Gauss–Manin connection ∇ in the decomposition of*

$$\nabla = \begin{pmatrix} \nabla^{2,0} & * & 0 \\ * & \nabla^{1,1} & * \\ 0 & * & \nabla^{0,2} \end{pmatrix}$$

on the Hodge bundle $H^2 = H^{2,0} \oplus H^{1,1} \oplus H^{0,2}$.

Sketch of proof. The result is local on the base, hence we may assume that S is contractible. Then the family is differentiably trivial, the Hodge bundle $t \mapsto H^2(X_t, \mathbb{C})$ is the trivial bundle and $t \mapsto H^2(X_t, \mathbb{Z})$ is a trivial lattice. We use the existence of a relative cycle space $C^p(\mathcal{X}/S) \subset C^p(\mathcal{X})$ which consists of all cycles contained in the fibres of $\pi : X \to S$. It is equipped with a canonical holomorphic projection

$$\pi_p : C^p(\mathcal{X}/S) \to S.$$

We then define the S_ν's to be the images in S of those connected components of $C^p(\mathcal{X}/S)$ which do not project onto S. By the fact that the projection is proper on each component, we infer that S_ν is an analytic subset of S. The definition of the S_ν's implies that the cohomology classes induced by the analytic cycles $\{[Z]\}$, $Z \subset X_t$, remain exactly the same for all $t \in S \setminus S'$. This result implies in its turn that the conditions defining the numerically positive cones $\mathcal{P}_t$ remain the same, except for the fact that the spaces $H^{1,1}(X_t, \mathbb{R}) \subset H^2(X_t, \mathbb{R})$ vary along with the Hodge decomposition. At this point, a standard calculation implies that the $\mathcal{P}_t$ are invariant by parallel transport under $\nabla^{1,1}$. Moreover, the connected component $\mathcal{K}_t \subset \mathcal{P}_t$ cannot jump from one component to the other thanks to the already mentioned results by Kodaira–Spencer [36]. This concludes the proof. □

Theorem 4.3 was essentially already known in the cases of complex surfaces (i.e. in dimension 2), thanks to the work of N. Buchdahl [6], [7] and A. Lamari [38], [39].

Shortly after the original [18] manuscript appeared in April 2001, Daniel Huybrechts [27] informed us that Theorem 3.1 can be used to calculate the Kähler cone of

a very general hyperkähler manifold: the Kähler cone is then equal to a suitable connected component of the positive cone defined by the Beauville–Bogomolov quadratic form. In the case of an arbitrary hyperkähler manifold, S. Boucksom [Bou02] later showed that a $(1,1)$ class $\{\alpha\}$ is Kähler if and only if it lies in the positive part of the Beauville–Bogomolov quadratic cone and moreover $\int_C \alpha > 0$ for all *rational curves* $C \subset X$ (see also Huybrechts [26]).

5. Positive cones in $H^{n-1,n-1}(X)$ and Serre duality

5.1. Basic definitions. In a way which will be shown to be dual to the case of divisors and positive $(1,1)$-currents, we consider in $H^{n-1,n-1}_{\mathbb{R}}(X)$ the cone $\mathcal{N}$ generated by classes of positive currents T of type $(n-1,n-1)$ (i.e., of bidimension $(1,1)$). In the projective case we also consider the intersection of $\mathcal{N}$ with the space $N_1(X)$ generated by integral $(n-1,n-1)$-classes (by the hard Lefschetz theorem, $N_1(X)$ is just the dual of $NS_{\mathbb{R}}(X)$).

Definition 5.1. Let X be a compact Kähler manifold.

(i) We define $\mathcal{N}$ to be the (closed) convex cone in $H^{n-1,n-1}_{\mathbb{R}}(X)$ generated by classes of positive currents T of type $(n-1,n-1)$ (i.e., of bidimension $(1,1)$).

(ii) We define the cone $\mathcal{M} \subset H^{n-1,n-1}_{\mathbb{R}}(X)$ of "movable classes" to be the closure of the convex cone generated by classes of currents of the form

$$\mu_\star(\widetilde{\omega}_1 \wedge \cdots \wedge \widetilde{\omega}_{n-1})$$

where $\mu\colon \widetilde{X} \to X$ is an arbitrary modification (one could just restrict oneself to compositions of blow-ups with smooth centers), and the $\widetilde{\omega}_j$ are Kähler forms on $\widetilde{X}$. Clearly $\mathcal{M} \subset \mathcal{N}$.

(iii) Correspondingly, we introduce the intersections

$$\mathcal{N}_{\mathrm{NS}} = \mathcal{N} \cap N_1(X), \quad \mathcal{M}_{\mathrm{NS}} = \mathcal{M} \cap N_1(X)$$

in the space generated by integral bidimension $(1,1)$-classes

$$N_1(X) := (H^{n-1,n-1}_{\mathbb{R}}(X) \cap H^{2n-2}(X,\mathbb{Z})/\{\text{torsion}\}) \otimes_{\mathbb{Z}} \mathbb{R}.$$

(iv) If X is projective we define $\mathrm{NE}(X)$ to be the convex cone generated by all effective curves. Clearly $\overline{\mathrm{NE}(X)} \subset \mathcal{N}_{\mathrm{NS}}$.

(v) If X is projective we say that C is a "strongly movable" curve if

$$C = \mu_\star(\widetilde{A}_1 \cap \cdots \cap \widetilde{A}_{n-1})$$

for suitable very ample divisors $\widetilde{A}_j$ on $\widetilde{X}$, where $\mu\colon \widetilde{X} \to X$ is a modification. We let $\mathrm{SME}(X)$ be the convex cone generated by all strongly movable (effective) curves. Clearly $\overline{\mathrm{SME}(X)} \subset \mathcal{M}_{\mathrm{NS}}$.

(vi) We say that C is a movable curve if $C = C_{t_0}$ is a member of an analytic family $(C_t)_{t\in S}$ such that $\bigcup_{t\in S} C_t = X$ and, as such, is a reduced irreducible 1-cycle. We let $\mathrm{ME}(X)$ be the convex cone generated by all movable (effective) curves.

The upshot of this definition lies in the following easy observation.

Proposition 5.2. *Let X be a compact Kähler manifold. Consider the Poincaré duality pairing*

$$H^{1,1}(X,\mathbb{R}) \times H^{n-1,n-1}_{\mathbb{R}}(X) \longrightarrow \mathbb{R}, \quad (\alpha,\beta) \longmapsto \int_X \alpha\wedge\beta.$$

Then the duality pairing takes nonnegative values

(i) *for all pairs $(\alpha,\beta) \in \overline{\mathcal{K}} \times \mathcal{N}$,*

(ii) *for all pairs $(\alpha,\beta) \in \mathcal{E} \times \mathcal{M}$,*

(iii) *for all pairs (α,β) where $\alpha \in \mathcal{E}$ and $\beta = [C_t] \in \mathrm{ME}(X)$ is the class of a movable curve.*

Proof. (i) is obvious. In order to prove (ii), we may assume that $\beta = \mu_\star(\widetilde{\omega}_1 \wedge \cdots \wedge \widetilde{\omega}_{n-1})$ for some modification $\mu\colon \widetilde{X} \to X$, where $\alpha = \{T\}$ is the class of a positive $(1,1)$-current on X and $\widetilde{\omega}_j$ are Kähler forms on $\widetilde{X}$. Then

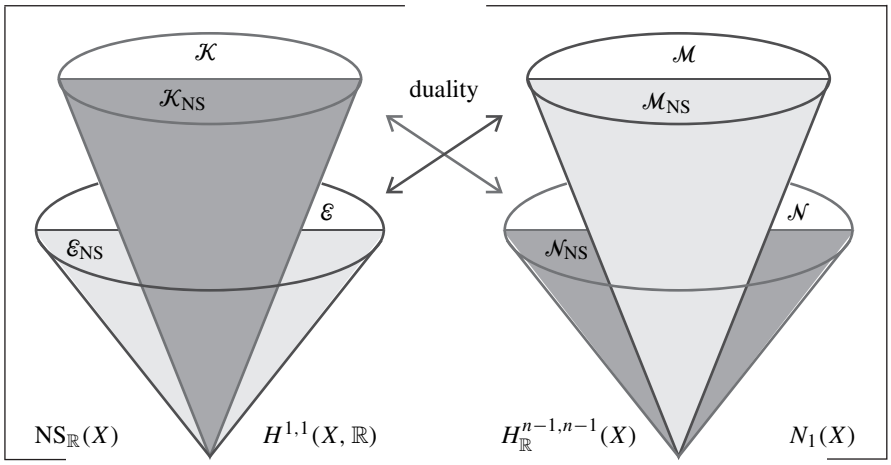
$$\int_X \alpha\wedge\beta = \int_X T \wedge \mu_\star(\widetilde{\omega}_1\wedge\cdots\wedge\widetilde{\omega}_{n-1}) = \int_X \mu^* T \wedge \widetilde{\omega}_1\wedge\cdots\wedge\widetilde{\omega}_{n-1} \geq 0.$$

Here we have used the fact that a closed positive $(1,1)$-current T always has a pull-back $\mu^\star T$, which follows from the fact that if $T = i\partial\overline{\partial}\varphi$ locally for some plurisubharmonic function in X, we can set $\mu^\star T = i\partial\overline{\partial}(\varphi\circ\mu)$. For (iii) we suppose $\alpha = \{T\}$ and $\beta = \{[C_t]\}$. Then we take an open covering (U_j) on X such that $T = i\partial\overline{\partial}\varphi_j$ with suitable plurisubharmonic functions φ_j on U_j. If we select a smooth partition of unity $\sum\theta_j = 1$ subordinate to (U_j), we then get

$$\int_X \alpha\wedge\beta = \int_{C_t} T_{|C_t} = \sum_j \int_{C_t\cap U_j} \theta_j i\partial\overline{\partial}\varphi_{j|C_t} \geq 0.$$

For this to make sense, it should be noticed that $T_{|C_t}$ is a well defined closed positive $(1,1)$-current (i.e. measure) on C_t for almost every $t \in S$, in the sense of Lebesgue measure. This is true only because (C_t) covers X, thus $\varphi_{j|C_t}$ is not identically $-\infty$ for almost every $t \in S$. The equality in the last formula is then shown by a regularization argument for T, writing $T = \lim T_k$ with $T_k = \alpha + i\partial\overline{\partial}\psi_k$ and a decreasing sequence of smooth almost plurisubharmonic potentials $\psi_k \downarrow \psi$ such that the Levi forms have a uniform lower bound $i\partial\overline{\partial}\psi_k \geq -C\omega$ (such a sequence exists by Demailly [14]). Then, writing $\alpha = i\partial\overline{\partial}v_j$ for some smooth potential v_j on U_j, we have $T = i\partial\overline{\partial}\varphi_j$ on U_j with $\varphi_j = v_j + \psi$, and this is the decreasing limit of the smooth approximations $\varphi_{j,k} = v_j + \psi_k$ on U_j. Hence $T_{k|C_t} \to T_{|C_t}$ for the weak topology of measures on C_t. □

If $\mathcal{C}$ is a convex cone in a finite dimensional vector space E, we denote by $\mathcal{C}^\vee$ the dual cone, i.e. the set of linear forms $u \in E^\star$ which take nonnegative values on all elements of $\mathcal{C}$. By the Hahn–Banach theorem, we always have $\mathcal{C}^{\vee\vee} = \overline{\mathcal{C}}$. Proposition 5.2 leads to the natural question whether the cones $(\mathcal{K}, \mathcal{N})$ and $(\mathcal{E}, \mathcal{M})$ are dual under Poincaré duality, according to the following schematic picture.



It is indeed well-known that the cone $\overline{\mathcal{K}_{\mathrm{NS}}}$ of nef divisors is dual to the cone $\mathcal{N}_{\mathrm{NS}}$ of effective curves if X is projective. The transcendental version $\mathcal{K} = \mathcal{N}^\vee$ also follows from our Theorem 3.8.

Theorem 5.3 (Demailly–Păun). *If X is Kähler, then the cones $\overline{\mathcal{K}} \subset H^{1,1}(X,\mathbb{R})$ and $\mathcal{N} \subset H^{n-1,n-1}_{\mathbb{R}}(X)$ are dual by Poincaré duality, and $\mathcal{N}$ is the closed convex cone generated by classes $[Y] \wedge \omega^{p-1}$ where $Y \subset X$ ranges over p-dimensional analytic subsets, $p = 1, 2, \ldots, n$, and ω ranges over Kähler forms.*

Proof. Indeed, Proposition 5.2 shows that the dual cone $\mathcal{K}^\vee$ contains $\mathcal{N}$ which itself contains the cone $\mathcal{N}'$ of all classes of the form $\{[Y] \wedge \omega^{p-1}\}$. The main result of Demailly–Păun [18] conversely shows that the dual of $(\mathcal{N}')^\vee$ is equal to $\overline{\mathcal{K}}$, so we must have

$$\mathcal{K}^\vee = \overline{\mathcal{N}'} = \mathcal{N}. \qquad \square$$

The other duality statement $\mathcal{E} = \mathcal{M}^\vee$ will be investigated in the next sections.

5.2. Concept of volume and movable intersections. We start with the very important concept of volume.

Definition 5.4. We define the *volume*, or *movable self-intersection* of a big class $\alpha \in \mathcal{E}^\circ$ to be

$$\mathrm{Vol}(\alpha) = \sup_{T \in \alpha} \int_{\widetilde{X}} \beta^n > 0$$

where the supremum is taken over all Kähler currents $T \in \alpha$ with logarithmic poles, and $\mu^\star T = [E] + \beta$ with respect to some modification $\mu\colon \widetilde{X} \to X$.

By Fujita [21] and Demailly–Ein–Lazarsfeld [17], if L is a big line bundle, we have

$$\mathrm{Vol}(c_1(L)) = \lim_{m\to+\infty} D_m^n = \lim_{m\to+\infty} \frac{n!}{m^n} h^0(X, mL),$$

and in these terms we get the following statement.

Proposition 5.5. *Let L be a big line bundle on the projective manifold X. Let $\varepsilon > 0$. Then there exists a modification $\mu\colon X_\varepsilon \to X$ and a decomposition $\mu^*(L) = E + \beta$ with E an effective $\mathbb{Q}$-divisor and β a big and nef $\mathbb{Q}$-divisor such that*

$$\mathrm{Vol}(L) - \varepsilon \le \mathrm{Vol}(\beta) \le \mathrm{Vol}(L).$$

It is very useful to observe that the supremum in Definition 5.4 is actually achieved by a collection of currents whose singularities satisfy a filtering property. Namely, if $T_1 = \alpha + i\partial\overline{\partial}\varphi_1$ and $T_2 = \alpha + i\partial\overline{\partial}\varphi_2$ are two Kähler currents with logarithmic poles in the class of α, then

$$T = \alpha + i\partial\overline{\partial}\varphi, \quad \varphi = \max(\varphi_1, \varphi_2) \tag{5.2}$$

is again a Kähler current with weaker singularities than T_1 and T_2. One could define as well

$$T = \alpha + i\partial\overline{\partial}\varphi, \quad \varphi = \frac{1}{2m}\log(e^{2m\varphi_1} + e^{2m\varphi_2}), \tag{5.2$'$}$$

where $m = \mathrm{lcm}(m_1, m_2)$ is the lowest common multiple of the denominators occurring in T_1, T_2. Now, take a simultaneous log-resolution $\mu_m\colon \widetilde{X}_m \to X$ for which the singularities of T_1 and T_2 are resolved as $\mathbb{Q}$-divisors E_1 and E_2. Then clearly the associated divisor in the decomposition $\mu_m^\star T = [E] + \beta$ is given by $E = \min(E_1, E_2)$.

Theorem 5.6 (Boucksom [4]). *Let X be a compact Kähler manifold. We denote here by $H^{k,k}_{\ge 0}(X)$ the cone of cohomology classes of type (k,k) which have non-negative intersection with all closed semi-positive smooth forms of bidegree $(n-k, n-k)$.*

(i) *For each $k = 1, \dots, n$, there exists a canonical "movable intersection product"*

$$\mathcal{E} \times \cdots \times \mathcal{E} \to H^{k,k}_{\ge 0}(X), \quad (\alpha_1, \dots, \alpha_k) \mapsto \langle \alpha_1 \cdot \alpha_2 \cdots \alpha_{k-1} \cdot \alpha_k \rangle$$

such that $\mathrm{Vol}(\alpha) = \langle \alpha^n \rangle$ whenever α is a big class.

(ii) *The product is increasing, homogeneous of degree 1 and superadditive in each argument, i.e.*

$$\langle \alpha_1 \cdots (\alpha_j' + \alpha_j'') \cdots \alpha_k \rangle \ge \langle \alpha_1 \cdots \alpha_j' \cdots \alpha_k \rangle + \langle \alpha_1 \cdots \alpha_j'' \cdots \alpha_k \rangle.$$

It coincides with the ordinary intersection product when the $\alpha_j \in \overline{\mathcal{K}}$ are nef classes.

(iii) *The movable intersection product satisfies the Teissier–Hovanskii inequalities*

$$\langle \alpha_1 \cdot \alpha_2 \cdots \alpha_n \rangle \geq (\langle \alpha_1^n \rangle)^{1/n} \ldots (\langle \alpha_n^n \rangle)^{1/n} \quad (\textit{with } \langle \alpha_j^n \rangle = \mathrm{Vol}(\alpha_j)\,).$$

(iv) *For $k = 1$, the above "product" reduces to a (non linear) projection operator*

$$\mathcal{E} \to \mathcal{E}_1, \quad \alpha \to \langle \alpha \rangle$$

onto a certain convex subcone $\mathcal{E}_1$ of $\mathcal{E}$ such that $\overline{\mathcal{K}} \subset \mathcal{E}_1 \subset \mathcal{E}$. Moreover, there is a "divisorial Zariski decomposition"

$$\alpha = \{N(\alpha)\} + \langle \alpha \rangle$$

where $N(\alpha)$ is a uniquely defined effective divisor which is called the "negative divisorial part" of α. The map $\alpha \mapsto N(\alpha)$ is homogeneous and subadditive, and $N(\alpha) = 0$ if and only if $\alpha \in \mathcal{E}_1$.

(v) *The components of $N(\alpha)$ always consist of divisors whose cohomology classes are linearly independent, thus $N(\alpha)$ has at most $\rho = \mathrm{rank}_{\mathbb{Z}} \mathrm{NS}(X)$ components.*

Proof. We refer to S. Boucksom's thesis [4] for details. Boucksom's treatment also covers the case of compact non Kähler manifolds, so it is fairly general. We only give a very rough construction of the movable intersection product.

First assume that all classes α_j are big, i.e. $\alpha_j \in \mathcal{E}^\circ$. We select Kähler currents $T_{j,m} \in \alpha_j$ with logarithmic poles and their approximate Zariski decompositions as in Theorem 2.10. We can then find a simultaneous log-resolution $\mu_m : \widetilde{X}_m \to X$ such that

$$\mu^\star T_{j,m} = [E_j, m] + \beta_{j,m}.$$

We consider the direct image current $\mu_{m\star}(\beta_{1,m} \wedge \cdots \wedge \beta_{k,m})$ (which is a closed positive current of bidegree (k,k) on X). It turns out by rather elementary monotonicity arguments based on the filtering property 5.2 that one can extract a weakly convergent limit

$$\langle \alpha_1 \cdot \alpha_2 \cdots \alpha_k \rangle = \lim_{m \to +\infty} \uparrow \{(\mu_m)_\star(\beta_{1,m} \wedge \beta_{2,m} \wedge \cdots \wedge \beta_{k,m})\}$$

and that the corresponding cohomology class in $H^{k,k}(X)$ is uniquely defined. Now, the intersection product can be extended to the full closed cone $\mathcal{E}$ by monotonicity again, namely by setting

$$\langle \alpha_1 \cdot \alpha_2 \cdots \alpha_k \rangle = \lim_{\delta \downarrow 0} \downarrow \langle (\alpha_1 + \delta\omega) \cdot (\alpha_2 + \delta\omega) \cdots (\alpha_k + \delta\omega) \rangle$$

for arbitrary classes $\alpha_j \in \mathcal{E}$. □

Definition 5.7. For a class $\alpha \in H^{1,1}(X, \mathbb{R})$ we define the numerical dimension $\nu(\alpha)$ to be $\nu(\alpha) = -\infty$ if α is not pseudo-effective, and

$$\nu(\alpha) = \max\{p \in \mathbb{N}\,;\ \langle \alpha^p \rangle \neq 0\}, \quad \nu(\alpha) \in \{0, 1, \ldots, n\}$$

if α is pseudo-effective.

By the results of Demailly–Peternell [18], a class is big ($\alpha \in \mathcal{E}^\circ$) if and only if $\nu(\alpha) = n$. Classes of numerical dimension 0 can be described much more precisely, again following Boucksom [4].

Theorem 5.8. *Let X be a compact Kähler manifold. Then the subset $\mathcal{D}_0$ of irreducible divisors D in X such that $\nu(D) = 0$ is countable, and these divisors are rigid as well as their multiples. If $\alpha \in \mathcal{E}$ is a pseudo-effective class of numerical dimension 0, then α is numerically equivalent to an effective $\mathbb{R}$-divisor $D = \sum_{j\in J} \lambda_j D_j$, for some finite subset $(D_j)_{j\in J} \subset \mathcal{D}_0$ such that the cohomology classes $\{D_j\}$ are linearly independent and some $\lambda_j > 0$. If such a linear combination is of numerical dimension 0, then so is any other linear combination of the same divisors.* □

Using the Iitaka fibration it is immediate to see that $\kappa(X) \le \nu(X)$ always holds true, and from the currently known examples a natural expectation would be

Conjecture 5.9 ("generalized abundance conjecture"). For an arbitrary compact Kähler manifold X, the Kodaira dimension should be equal to the numerical dimension:

$$\kappa(X) = \nu(X) := \nu(c_1(K_X)).$$

This appears to be a fairly strong statement. In fact, it is not difficult to show that the generalized abundance conjecture contains the $C_{n,m}$ conjectures about additivity of Kodaira dimension (since it is not very difficult to show that the numerical dimension is additive with respect to fibrations). A few extreme cases are known.

Theorem 5.10. *The generalized abundance conjecture is true at least in the cases $\nu(X) = -\infty$, $\nu(X) = 0$, $\nu(X) = n$.*

Proof. In fact $\nu(X) = -\infty$ means that K_X is not pseudo-effective, so no multiple of K_X can have sections and thus $\kappa(X) = -\infty$. In case $\nu(X) = n$, we have to show that K_X is big ($K_X \in \mathcal{E}^\circ$); this follows from [18] and from the solution of the Grauert–Riemenschneider conjecture in the form proven in Demailly [11]. Remains the case $\nu(X) = 0$. Then Theorem 5.8 gives $K_X \equiv \sum \lambda_j D_j$ for some effective divisor with numerically independent components such that $\nu(D_j) = 0$. It follows that the λ_j are rational and therefore

$$K_X = \sum \lambda_j D_j + F \quad \text{where } \lambda_j \in \mathbb{Q}^+,\ \nu(D_j) = 0 \text{ and } F \in \mathrm{Pic}^0(X).$$

In that case Campana and Peternell [8] have shown that F is a torsion element of $\mathrm{Pic}^0(X)$, and so $\kappa(X) = 0$.

5.3. The orthogonality estimate. The goal of this section is to show that, in an appropriate sense, approximate Zariski decompositions are almost orthogonal.

Theorem 5.11. *Let X be a projective manifold, and let $\alpha = \{T\} \in \mathcal{E}^\circ_{\mathrm{NS}}$ be a big class represented by a Kähler current T. Consider an approximate Zariski decomposition*

$$\mu_m^\star T_m = [E_m] + [D_m].$$

Then

$$(D_m^{n-1} \cdot E_m)^2 \le 20\,(C\omega)^n \big(\mathrm{Vol}(\alpha) - D_m^n\big)$$

where $\omega = c_1(H)$ is a Kähler form and $C \ge 0$ is a constant such that $\pm\alpha$ is dominated by $C\omega$ (i.e., $C\omega \pm \alpha$ is nef).

Proof. For every $t \in [0, 1]$ we have

$$\mathrm{Vol}(\alpha) = \mathrm{Vol}(E_m + D_m) \ge \mathrm{Vol}(tE_m + D_m).$$

Now, by our choice of C, we can write E_m as a difference of two nef divisors:

$$E_m = \mu^\star\alpha - D_m = \mu_m^\star(\alpha + C\omega) - (D_m + C\mu_m^\star\omega).$$

Lemma 5.12. *For all nef $\mathbb{R}$-divisors A, B we have*

$$\mathrm{Vol}(A - B) \ge A^n - nA^{n-1} \cdot B$$

as soon as the right-hand side is positive.

Proof. In case A and B are integral (Cartier) divisors, this is a consequence of the holomorphic Morse inequalities (Demailly [16], 8.5). If A and B are $\mathbb{Q}$-Cartier, we conclude by the homogeneity of the volume. The general case of $\mathbb{R}$-divisors follows by approximation using the upper semi-continuity of the volume (Boucksom [4], 3.1.26). In fact, we expect Lemma 5.12 to hold true also in the case of transcendental nef cohomology classes – unfortunately the required generalization of Morse inequalities is still missing at this point. □

End of proof of Theorem 5.11. In order to exploit the lower bound of the volume, we write

$$tE_m + D_m = A - B, \quad A = D_m + t\mu_m^\star(\alpha + C\omega),\ B = t(D_m + C\mu_m^\star\omega).$$

By our choice of the constant C, both A and B are nef. Lemma 5.12 and the binomial formula imply

$$\begin{aligned}
\mathrm{Vol}(tE_m + D_m) &\ge A^n - nA^{n-1} \cdot B \\
&= D_m^n + nt\, D_m^{n-1} \cdot \mu_m^\star(\alpha + C\omega) + \sum_{k=2}^{n} t^k \binom{n}{k} D_m^{n-k} \cdot \mu_m^\star(\alpha + C\omega)^k \\
&\quad - nt\, D_m^{n-1} \cdot (D_m + C\mu_m^\star\omega) \\
&\quad - nt^2 \sum_{k=1}^{n-1} t^{k-1} \binom{n-1}{k} D_m^{n-1-k} \cdot \mu_m^\star(\alpha + C\omega)^k \cdot (D_m + C\mu_m^\star\omega).
\end{aligned}$$

Now we use the obvious inequalities

$$D_m \le \mu_m^\star(C\omega), \quad \mu_m^\star(\alpha + C\omega) \le 2\mu_m^\star(C\omega), \quad D_m + C\mu_m^\star\omega \le 2\mu_m^\star(C\omega)$$

in which all members are nef (and where the inequality $\le$ means that the difference of classes is pseudo-effective). In this way we get

$$\mathrm{Vol}(tE_m + D_m) \ge D_m^n + nt D_m^{n-1} \cdot E_m - nt^2 \sum_{k=1}^{n-1} 2^{k+1} t^{k-1} \binom{n-1}{k} (C\omega)^n.$$

We will always take t smaller than $1/10n$ so that the last summation is bounded by $4(n-1)(1+1/5n)^{n-2} < 4ne^{1/5} < 5n$. This implies

$$\mathrm{Vol}(tE_m + D_m) \ge D_m^n + nt\, D_m^{n-1} \cdot E_m - 5n^2 t^2 (C\omega)^n.$$

Now, the choice $t = \frac{1}{10n}(D_m^{n-1} \cdot E_m)((C\omega)^n)^{-1}$ gives by substituting

$$\frac{1}{20} \frac{(D_m^{n-1} \cdot E_m)^2}{(C\omega)^n} \le \mathrm{Vol}(E_m + D_m) - D_m^n \le \mathrm{Vol}(\alpha) - D_m^n$$

(and we have indeed $t \le \frac{1}{10n}$), whence Theorem 5.11. Of course, the constant 20 is certainly not optimal. □

Corollary 5.13. *If $\alpha \in \mathcal{E}_{\mathrm{NS}}$, then the divisorial Zariski decomposition $\alpha = N(\alpha) + \langle\alpha\rangle$ is such that $\langle\alpha^{n-1}\rangle \cdot N(\alpha) = 0$.*

Proof. By replacing α by $\alpha + \delta c_1(H)$, one sees that it is sufficient to consider the case where α is big. Then the orthogonality estimate implies

$$\begin{aligned}(\mu_m)_\star(D_m^{n-1}) \cdot (\mu_m)_\star E_m &= D_m^{n-1} \cdot (\mu_m)^\star(\mu_m)_\star E_m \\ &\le D_m^{n-1} \cdot E_m \\ &\le C(\mathrm{Vol}(\alpha) - D_m^n)^{1/2}.\end{aligned}$$

Since $\langle\alpha^{n-1}\rangle = \lim(\mu_m)_\star(D_m^{n-1})$, $N(\alpha) = \lim(\mu_m)_\star E_m$ and $\lim D_m^n = \mathrm{Vol}(\alpha)$, we get the desired conclusion in the limit. □

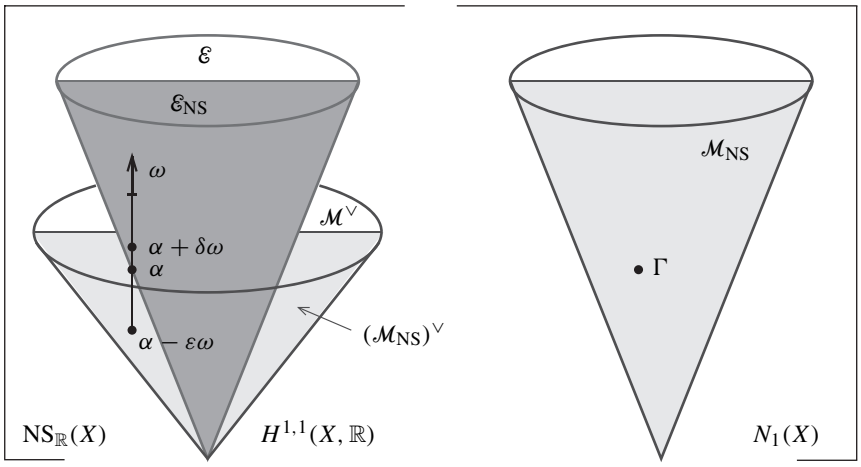
5.4. Proof of duality between $\mathcal{E}_{\mathrm{NS}}$ and $\mathcal{M}_{\mathrm{NS}}$. The main point is the following characterization of pseudo-effective classes, proved in [5] (the "only if" part already follows from 5.2 (iii)).

Theorem 5.14 (Boucksom–Demailly–Păun–Peternell [5])). *If X is projective, then a class $\alpha \in \mathrm{NS}_{\mathbb{R}}(X)$ is pseudo-effective if (and only if) it is in the dual cone of the cone $\mathrm{SME}(X)$ of strongly movable curves.*

In other words, a line bundle L is pseudo-effective if (and only if) $L \cdot C \ge 0$ for all *movable curves*, i.e., $L \cdot C \ge 0$ for every very generic curve C (not contained in a countable union of algebraic subvarieties). In fact, by definition of $\mathrm{SME}(X)$, it is enough to consider only those curves C which are images of generic complete intersections of very ample divisors on some variety $\widetilde{X}$, under a modification $\mu\colon \widetilde{X} \to X$.

By a standard blowing-up argument, it also follows that a line bundle L on a normal Moishezon variety is pseudo-effective if and only if $L \cdot C \geq 0$ for every movable curve C. The Kähler analogue should be:

Conjecture 5.15. For an arbitrary compact Kähler manifold X, the cones $\mathcal{E}$ and $\mathcal{M}$ are dual.



Proof of Theorem 5.14 (*see* [5]). We want to show that $\mathcal{E}_{\mathrm{NS}} = \mathrm{SME}(X)^\vee$. By 5.2 (iii) we have in any case

$$\mathcal{E}_{\mathrm{NS}} \subset (\mathrm{SME}(X))^\vee.$$

If the inclusion is strict, there is an element $\alpha \in \partial\mathcal{E}_{\mathrm{NS}}$ on the boundary of $\mathcal{E}_{\mathrm{NS}}$ which is in the interior of $\mathrm{SME}(X)^\vee$.

Let $\omega = c_1(H)$ be an ample class. Since $\alpha \in \partial\mathcal{E}_{\mathrm{NS}}$, the class $\alpha + \delta\omega$ is big for every $\delta > 0$, and since $\alpha \in ((\mathrm{SME}(X))^\vee)^\circ$ we still have $\alpha - \varepsilon\omega \in (\mathrm{SME}(X))^\vee$ for $\varepsilon > 0$ small. Therefore

$$\alpha \cdot \Gamma \geq \varepsilon\omega \cdot \Gamma \tag{5.4}$$

for every movable curve Γ. We are going to contradict (5.4). Since $\alpha + \delta\omega$ is big, we have an approximate Zariski decomposition

$$\mu_\delta^\star(\alpha + \delta\omega) = E_\delta + D_\delta.$$

We pick $\Gamma = (\mu_\delta)_\star(D_\delta^{n-1})$. By the Hovanskii–Teissier concavity inequality

$$\omega \cdot \Gamma \geq (\omega^n)^{1/n}(D_\delta^n)^{(n-1)/n}.$$

On the other hand

$$\begin{aligned}\alpha\cdot\Gamma &= \alpha\cdot(\mu_\delta)_\star(D_\delta^{n-1})\\ &= \mu_\delta^\star\alpha\cdot D_\delta^{n-1}\le \mu_\delta^\star(\alpha+\delta\omega)\cdot D_\delta^{n-1}\\ &= (E_\delta+D_\delta)\cdot D_\delta^{n-1} = D_\delta^n + D_\delta^{n-1}\cdot E_\delta.\end{aligned}$$

By the orthogonality estimate, we find

$$\begin{aligned}\frac{\alpha\cdot\Gamma}{\omega\cdot\Gamma} &\le \frac{D_\delta^n + \big(20(C\omega)^n(\mathrm{Vol}(\alpha+\delta\omega)-D_\delta^n)\big)^{1/2}}{(\omega^n)^{1/n}(D_\delta^n)^{(n-1)/n}}\\ &\le C'(D_\delta^n)^{1/n} + C''\frac{(\mathrm{Vol}(\alpha+\delta\omega)-D_\delta^n)^{1/2}}{(D_\delta^n)^{(n-1)/n}}.\end{aligned}$$

However, since $\alpha\in\partial\mathcal{E}_{\mathrm{NS}}$, the class α cannot be big so

$$\lim_{\delta\to 0} D_\delta^n = \mathrm{Vol}(\alpha) = 0.$$

We can also take D_δ to approximate $\mathrm{Vol}(\alpha+\delta\omega)$ in such a way that $(\mathrm{Vol}(\alpha+\delta\omega)-D_\delta^n)^{1/2}$ tends to 0 much faster than D_δ^n. Notice that $D_\delta^n\ge\delta^n\omega^n$, so in fact it is enough to take

$$\mathrm{Vol}(\alpha+\delta\omega)-D_\delta^n\le\delta^{2n}.$$

This is the desired contradiction by (5.4). □

As a corollary, we also get a solution of the "Hodge conjecture" for positive cones of $H^{n-1,n-1}(X)$, namely positive integral classes are generated by the corresponding cones of curves. This settles in the affirmative many of the conjectures made in [19].

Corollary 5.16. *Let X be a projective manifold. Then*

(i) $\mathcal{N}_{\mathrm{NS}} = \overline{\mathrm{NE}(X)}$,

(ii) $\mathcal{M}_{\mathrm{NS}} = \overline{\mathrm{SME}(X)} = \overline{\mathrm{ME}(X)}$.

Proof. (i) is indeed (mostly) a standard result of algebraic geometry, a restatement of the fact that the cone of effective curves $\mathrm{NE}(X)$ is dual to the cone $\overline{\mathcal{K}_{\mathrm{NS}}}$ of nef divisors (see e.g. [24]): clearly $\mathcal{N}_{\mathrm{NS}}\supset\overline{\mathrm{NE}(X)} = \mathcal{K}_{\mathrm{NS}}^\vee$, and the other direction $\mathcal{N}_{\mathrm{NS}}\subset\mathcal{K}_{\mathrm{NS}}^\vee$ is a consequence of 5.2 (i).

(ii) It is obvious that $\mathrm{SME}(X)\subset\mathrm{ME}(X)\subset\mathcal{M}_{\mathrm{NS}}\subset(\mathcal{E}_{\mathrm{NS}})^\vee$ (the latter inclusion follows from 5.2 (iii)). Now Theorem 5.14 implies $(\mathcal{E}_{\mathrm{NS}})^\vee = \overline{\mathrm{SME}(X)}$, and (ii) follows. □

Remark 5.17. If holomorphic Morse inequalities were known also in the Kähler case, we would infer by the same proof that "α not pseudo-effective" implies the existence of a blow-up $\mu\colon\widetilde{X}\to X$ and a Kähler metric $\widetilde{\omega}$ on $\widetilde{X}$ such that $\alpha\cdot\mu_\star(\widetilde{\omega})^{n-1}<0$. In

the special case when $\alpha = K_X$ is not pseudo-effective, we would expect the Kähler manifold X to be covered by rational curves. The main trouble is that characteristic p techniques are no longer available. On the other hand it is tempting to approach the question via techniques of symplectic geometry:

Question 5.18. Let (M, ω) be a compact real symplectic manifold. Fix an almost complex structure J compatible with ω, and for this structure assume that $c_1(M) \cdot \omega^{n-1} > 0$. Does it follow that M is covered by rational J-pseudoholomorphic curves?

5.5. Applications and conjectures. The most important special case of Theorem 5.14 is

Theorem 5.19. *If X is a projective manifold and is not uniruled, then K_X is pseudo-effective, i.e. $K_X \in \mathcal{E}_{\mathrm{NS}}$.*

Proof. If $K_X \notin \mathcal{E}_{\mathrm{NS}}$, Proposition 5.2 shows that there is a moving curve C_t such that $K_X \cdot C_t < 0$. The standard "bend-and-break" lemma of Mori then implies that there is family Γ_t of *rational* curves with $K_X \cdot \Gamma_t < 0$, so X is uniruled. □

Of course, if the "abundance conjecture" is correct, the fact that K_X is pseudo-effective would imply $\kappa(X) \geq 0$, and so every non uniruled variety should satisfy $\kappa(X) \geq 0$. This still seems beyond reach at the moment.

6. Plurigenera and the Minimal Model Program

In the case of algebraic surfaces, the Minimal Model Program (MMP) was already initiated by Italian geometers at the turn of the XXth century, and was finally completed by Zariski and Kodaira for all complex surfaces. The case of higher dimensions (starting with dimension 3) is a major endeavor of modern times, revitalized by Mori [41], Kawamata [29], [30], [31] and Shokurov [53], [54] among others (see also [33] for a good survey).

The basic question is to prove that every birational class of non uniruled algebraic varieties contains a "minimal" member X exhibiting mild singularities ("terminal singularities"), where "minimal" is taken in the sense of avoiding unnecessary blow-ups; minimality actually means that K_X is nef and not just pseudo-effective (pseudo-effectivity follows in general from Theorem 5.19). This requires performing certain birational transforms known as flips, and important questions are whether a) flips are indeed possible ("existence of flips"), b) the process terminates ("termination of flips"). Thanks to Kawamata [31] and Shokurov [53], [54], this has been proved in dimension 3 at the end of the 80s. Very recently, C. Hacon and J. McKernan [23] announced that flips exist in dimension n, if one assumes that a slightly stronger version of MMP (involving log pairs with real divisors) holds true in dimension $n-1$. As a consequence, the existence of flips obtained by Shokurov [55] in 2003 would

be achieved in dimension 4 via a more systematic method. Strongly related to these issues are the following fundamental questions.

(i) *Finiteness of the canonical ring:* is the *canonical ring* $R = \bigoplus H^0(X, mK_X)$ of a variety of general type always finitely generated?
If true, Proj(R) of this graded ring R yields of course a "canonical model" in the birational class of X.

(ii) *Boundedness of pluricanonical embeddings:* is there a bound r_n depending only on dimension $\dim X = n$, such that the pluricanonical map Φ_{mK_X} of a variety of general type yields a birational embedding in projective space for $m \geq r_n$?

(iii) *Invariance of plurigenera:* are plurigenera $p_m = h^0(X, mK_X)$ always invariant under deformation?

These questions involve taking "limits" of divisors as $m \to +\infty$, and therefore transcendental methods are a strong contender in the arena. Question (ii) was indeed solved in the affirmative by H. Tsuji [63], [64] under the assumption that the MMP program is solved, and in general by S. Takayama [61], and Ch. Hacon-J. McKernan [22] by pursuing further Tsuji's ideas. Question (iii) was completely settled by Y. T. Siu ([58] in the case of varieties of general type, and [59] for arbitrary varieties). Quite recently, M. Păun gave a very elementary proof based merely on the Ohwawa–Takegoshi extension theorem, that we briefly sketch below. Y. T. Siu's work also gives strong support for the hope that (i) can be solved by a suitable combination of the L^2 existence theorems (Skoda's division theorem being one of the main ingredients). The following is a very slight extension of results by M. Păun [52] and B. Claudon [9], which are themselves based on the ideas of Y. T. Siu [59] and S. Takayama [62].

Theorem 6.1. *Let $\pi : \mathcal{X} \to \Delta$ be a projective family over the unit disk, and let $(L_j, h_j)_{0\leq j\leq m-1}$ be (singular) hermitian line bundles with semipositive curvature currents $i\Theta_{L_j,h_j} \geq 0$ on $\mathcal{X}$. Assume that*

(i) *the restriction of h_j to the central fiber X_0 is well defined (i.e. not identically $+\infty$);*

(ii) *additionally the multiplier ideal sheaf $\mathcal{I}(h_{j|X_0})$ is trivial for $1 \leq j \leq m-1$.*

Then any section σ of $\mathcal{O}(mK_{\mathcal{X}} + \sum L_j)_{|X_0} \otimes \mathcal{I}(h_{0|X_0})$ over the central fiber X_0 extends to $\mathcal{X}$.

We first state the technical version of the Ohsawa–Takegoshi L^2 extension theorem needed for the proof, which is a special case of Theorem 2.7 (see also Siu [59]).

Lemma 6.2. *Let $\pi : \mathcal{X} \to \Delta$ be as before and let (L, h) be a (singular) hermitian line bundle with semipositive curvature current $i\Theta_{L,h} \geq 0$ on $\mathcal{X}$. Let ω be a global Kähler metric on $\mathcal{X}$, and $dV_{\mathcal{X}}$, dV_{X_0} the respective induced volume elements on*

X_0 and $\mathcal{X}$. Assume that h_{X_0} is well defined. Then any holomorphic section u of $\mathcal{O}(K_{\mathcal{X}}+L)\otimes\mathcal{I}(h_{|X_0})$ extends into a section $\widetilde{u}$ over $\mathcal{X}$ satisfying an L^2 estimate

$$\int_{\mathcal{X}}\|\widetilde{u}\|^2_{\omega\otimes h}dV_{\mathcal{X}}\le C_0\int_{X_0}\|u\|^2_{\omega\otimes h}dV_{X_0},$$

where $C_0\ge 0$ is some universal constant (independent of $\mathcal{X}$, L, ...).

Proof. We write $h_j=e^{-\varphi_j}$ in terms of local plurisubharmonic weights. Fix an auxiliary line bundle A (which will later be taken to be sufficiently ample), and define inductively a sequence of line bundles F_p by putting $F_0=A$ and

$$F_p=F_{p-1}+K_{\mathcal{X}}+L_r\quad\text{if } p=mq+r,\ 0\le r\le m-1.$$

By construction we have $F_{p+m}=F_p+mK_{\mathcal{X}}+\sum_j L_j$ and

$$F_0=A,\ F_1=A+K_{\mathcal{X}}+L_1,\ \dots,\ F_p=A+pK_{\mathcal{X}}+L_1+\cdots+L_p,\ 1\le p\le m-1.$$

The game is to construct inductively families of sections, say $(\widetilde{u}_j^{(p)})_{j=1\dots N_p}$, of F_p over $\mathcal{X}$ in such a way that

(a) for $p=0,\dots,m-1$, F_p is generated by its sections $(\widetilde{u}_j^{(p)})_{j=1\dots N_p}$;

(b) we have the m-periodicity relations $N_{p+m}=N_p$ and $\widetilde{u}_j^{(p)}$ is an extension of $u_j^{(p)}:=\sigma^q u_j^{(r)}$ over $\mathcal{X}$ for $p=mq+r$, where $u_j^{(r)}:=\widetilde{u}_{j|X_0}^{(r)}$, $0\le r\le m-1$.

Property (a) can certainly be achieved by taking A ample enough so that $F_0,\dots,F_{m-1}$ are generated by their sections, and by choosing the $\widetilde{u}_j^{(p)}$ appropriately for $p=0,\dots,m-1$. Now, by induction, we equip F_{p-1} with the tautological metric $|\xi|^2/\sum|\widetilde{u}_j^{(p-1)}(x)|^2$, and $F_p-K_{\mathcal{X}}=F_{p-1}+L_r$ with that metric multiplied by $h_r=e^{-\varphi_r}$; it is clear that these metrics have semipositive curvature currents (the metric on F_p itself if obtained by using a smooth Kähler metric ω on $\mathcal{X}$). In this setting, we apply the Ohsawa–Takegoshi theorem to the line bundle $F_{p-1}+L_r$ to extend $u_j^{(p)}$ into a section $\widetilde{u}_j^{(p)}$ over $\mathcal{X}$. By construction the pointwise norm of that section in $F_{p|X_0}$ in a local trivialization of the bundles involved is the ratio

$$\frac{|u_j^{(p)}|^2}{\sum_\ell|u_\ell^{(p-1)}|^2}e^{-\varphi_r},$$

up to some fixed smooth positive factor depending only on the metric induced by ω on $K_{\mathcal{X}}$. However, by the induction relations, we have

$$\frac{\sum_j|u_j^{(p)}|^2}{\sum_\ell|u_\ell^{(p-1)}|^2}e^{-\varphi_r}=\begin{cases}\dfrac{\sum_j|u_j^{(r)}|^2}{\sum_\ell|u_\ell^{(r-1)}|^2}e^{-\varphi_r} & \text{for } p=mq+r,\ 0<r\le m-1,\\[2ex] \dfrac{\sum_j|u_j^{(0)}|^2}{\sum_\ell|u_\ell^{(m-1)}|^2}|\sigma|^2e^{-\varphi_0} & \text{for } p\equiv 0 \mod m.\end{cases}$$

Since the sections $(u_j^{(r)})$ generate their line bundle, the ratios involved are positive functions without zeroes and poles, hence smooth and bounded (possibly after shrinking the base disc Δ, as is permitted). On the other hand, assumption (ii) and the fact that σ has coefficients in the multiplier ideal sheaf $\mathcal{I}(h_{0|X_0})$ tell us that $e^{-\varphi_r}$, $1 \le r < m$ and $|\sigma|^2 e^{-\varphi_0}$ are locally integrable on X_0. It follows that there is a constant $C_1 \ge 0$ such that

$$\int_{X_0} \frac{\sum_j |u_j^{(p)}|^2}{\sum_\ell |u_\ell^{(p-1)}|^2} e^{-\varphi_r} dV_\omega \le C_1$$

for all $p \ge 1$ (of course, the integral certainly involves finitely many trivializations of the bundles involved, whereas the integrand expression is just local in each chart). Inductively, the L^2 extension theorem produces sections $\widetilde{u}_j^{(p)}$ of F_p over $\mathcal{X}$ such that

$$\int_{\mathcal{X}} \frac{\sum_j |\widetilde{u}_j^{(p)}|^2}{\sum_\ell |\widetilde{u}_\ell^{(p-1)}|^2} e^{-\varphi_r} dV_\omega \le C_2 = C_0 C_1.$$

The next idea is to extract the limits of p-th roots of these sections to get a singular hermitian metric on $mK_{\mathcal{X}} + \sum L_j$. As the functions $e^{-\varphi_r}$ are locally bounded below (φ_r being psh), the Hölder inequality implies that

$$\int_{\mathcal{X}} \Big(\sum_j |\widetilde{u}_j^{(p)}|^2 \Big)^{1/p} dV_\omega \le C_3.$$

Jensen's inequality together with well known facts of potential theory now show that some subsequence of the sequence of plurisubharmonic functions $\frac{1}{q} \log \sum_j |\widetilde{u}_j^{(mq)}|^2$ (which should be thought of as weights on the $\mathbb{Q}$-line bundles $\frac{1}{q}(A + q(mK_{\mathcal{X}} + \sum L_j))$) converges almost everywhere to the weight ψ of a singular hermitian metric H with semi-positive curvature on $mK_{\mathcal{X}} + \sum L_j$, in the form of an upper regularized limit

$$\psi(z) = \limsup_{\zeta \to z} \lim_{\nu \to +\infty} \frac{1}{q_\nu} \log \sum_j |\widetilde{u}_j^{(mq_\nu)}(\zeta)|^2.$$

On X_0 we have

$$\lim_{q \to +\infty} \frac{1}{q} \log \sum_j |u_j^{(mq)}|^2 = \lim_{q \to +\infty} \frac{1}{q} \log \big(|\sigma|^{2q} \sum_j |u_j^{(0)}|^2 \big) = \log |\sigma|^2,$$

hence $\psi(z) \ge \log |\sigma|^2$ and $\|\sigma\|_H \le 1$. We equip the bundle

$$G = (m-1) K_{\mathcal{X}} + \sum L_j$$

with the metric $\gamma = H^{1-1/m} \prod h_j^{1/m}$, and $mK_{\mathcal{X}} + \sum L_j = K_{\mathcal{X}} + G$ with the metric $\omega \otimes \gamma$. Clearly γ has a semipositive curvature current on $\mathcal{X}$ and in a local trivialization

we have

$$\|\sigma\|^2_{\omega\otimes\gamma} \le C|\sigma|^2 \exp\Big(-\Big(1-\frac{1}{m}\Big)\psi + \frac{1}{m}\sum\varphi_j\Big) \le C\Big(|\sigma|^2\prod e^{-\varphi_j}\Big)^{1/m}$$

on X_0. Since $|\sigma|^2 e^{-\varphi_0}$ and $e^{-\varphi_r}$, $r > 0$ are all locally integrable, we see that $\|\sigma\|^2_{\omega\otimes\gamma}$ is also locally integrable on X_0 by the Hölder inequality. A new (and final) application of the L^2 extension theorem to the hermitian line bundle (G, γ) implies that σ can be extended to $\mathcal{X}$. The theorem is proved. □

The special case of the theorem obtained by taking all bundles L_j trivial tells us in particular that any pluricanonical section σ of $mK_{\mathcal{X}}$ over X_0 extends to $\mathcal{X}$. By the upper semi-continuity of $t \mapsto h^0(X_t, mK_{X_t})$, this implies

Corollary 6.3 (Siu [59]). *For any projective family $t \mapsto X_t$ of algebraic varieties, the plurigenera $p_m(X_t) = h^0(X_t, mK_{X_t})$ do not depend on t.*

At the moment it should be observed that there are no purely algebraic proofs of the invariance of plurigenera, though Y. Kawamata [32] has given an algebraic proof in the case of varieties of general type.

References

[1] Andreotti, A., Vesentini, E., Carleman estimates for the Laplace-Beltrami equation in complex manifolds. *Inst. Hautes Études Sci. Publ. Math.* **25** (1965), 81–130.

[2] Biswas, I., Narasimhan, M. S., Hodge classes of moduli spaces of parabolic bundles over the general curve. *J. Algebraic Geom.* **6** (1997), 697–715.

[3] Bochner, S., Curvature and Betti numbers; Curvature and Betti numbers. II. *Ann. of Math.* **49** (1948), 379–390; **50** (1949), 77–93.

[4] Boucksom, S., Cônes positifs des variétés complexes compactes. Thesis, Grenoble 2002.

[5] Boucksom, S., Demailly, J. P., Păun, M., Peternell, Th., The pseudo-effective cone of a compact Kähler manifold and varieties of negative Kodaira dimension. arXiv:math.AG/0405285.

[6] Buchdahl, N., On compact Kähler surfaces. *Ann. Inst. Fourier* **49** (1999), 287–302.

[7] Buchdahl, N., A Nakai-Moishezon criterion for non-Kähler surfaces. *Ann. Inst. Fourier* **50** (2000), 1533–1538.

[8] Campana, F., Peternell, Th., Geometric stability of the cotangent bundle and the universal cover of a projective manifold. arXiv:math.AG/0405093.

[9] Claudon, B., Invariance for multiples of the twisted canonical bundle. *Ann. Inst. Fourier* **57** (2007), 289–300.

[10] Demailly, J.-P., Estimations L^2 pour l'opérateur $\bar\partial$ d'un fibré vectoriel holomorphe semi-positif au-dessus d'une variété kählérienne complète. *Ann. Sci. École Norm. Sup.* (4) **15** (1982), 457–511.

[11] Demailly, J.-P., Champs magnétiques et inégalités de Morse pour la d''-cohomologie. *Ann. Inst. Fourier* **35** (1985), 189–229.

[12] Demailly, J.-P., Transcendental proof of a generalized Kawamata-Viehweg vanishing theorem. In *Geometrical and algebraical aspects in several complex variables* (Cetraro, 1989), Sem. Conf. 8, EditEl, Rende 1991, 81–94; *C. R. Acad. Sci. Paris Sér. I Math.* **309** (1989), 123–126.

[13] Demailly, J.-P., Singular hermitian metrics on positive line bundles. In *Complex algebraic varieties* (K. Hulek, T. Peternell, M. Schneider, F. Schreyer, eds.), Lecture Notes in Math. 1507, Springer-Verlag, Berlin 1992, 87–104.

[14] Demailly, J.-P., Regularization of closed positive currents and intersection theory. *J. Algebraic Geom.* **1** (1992), 361–409.

[15] Demailly, J.-P., A numerical criterion for very ample line bundles. *J. Differential Geom.* **37** (1993), 323–374.

[16] Demailly, J.-P., Multiplier ideal sheaves and analytic methods in algebraic geometry. *Lecture Notes, School on "Vanishing theorems and effective results in Algebraic Geometry"*, ICTP Trieste, April 2000, Publications of ICTP, 2001.

[17] Demailly, J.-P., Ein, L., Lazarsfeld, R., A subadditivity property of multiplier ideals. *Michigan Math. J.* **48** (Special volume in honor of William Fulton) (2000), 137–156.

[18] Demailly, J.-P., Păun, M., Numerical characterization of the Kähler cone of a compact Kähler manifold. *Ann. of Math.* **159** (2004), 1247–1274.

[19] Demailly, J.-P., Peternell, Th., Schneider, M., Holomorphic line bundles with partially vanishing cohomology. In *Proceedings of the Hirzebruch* 65 *Conference on Algebraic Geometry* (Ramat Gan, 1993), Israel Math. Conf. Proc. 9, Bar-Ilan University, Ramat Gan 1996, 165–198.

[20] Demailly, J.-P., Peternell, Th., Schneider, M., Pseudo-effective line bundles on compact Kähler manifolds. *Internat. J. Math.* **6** (2001), 689–741.

[21] Fujita, T., Approximating Zariski decomposition of big line bundles. *Kodai Math. J.* **17** (1994), 1–3.

[22] Hacon, Ch., McKernan, J., Boundedness of pluricanonical maps of varieties of general type. *Invent. Math.* **166** (2006), 1–25.

[23] Hacon, Ch., McKernan, J., On the existence of flips. arXiv:math.AG/0507597.

[24] Hartshorne, R., *Ample subvarieties of algebraic varieties.* Lecture Notes in Math. 156, Springer-Verlag, Berlin 1970.

[25] Hörmander, L., L^2 estimates and existence theorems for the $\overline{\partial}$ operator. *Acta Math.* **113** (1965), 89–152.

[26] Huybrechts, D., Compact Hyperkähler Manifolds: Basic Results. *Invent. Math.* **135** (1999), 63–113.

[27] Huybrechts, D., Compact Hyperkähler Manifolds: Basic Results, II (The Projectivity Criterion for Hyperkähler manifolds as a Consequence of the Demailly-Păun Theorem). *Invent. Math.* **152** (2003), 209–212.

[28] Kawamata, Y., A generalization of Kodaira-Ramanujam's vanishing theorem. *Math. Ann.* **261** (1982), 43–46.

[29] Kawamata, Y., The cone of curves of algebraic varieties. *Ann. of Math.* **119** (1984), 603–633.

[30] Kawamata, Y., Minimal models and the Kodaira dimension of algebraic fiber spaces. *J. Reine Angew. Math.* **363** (1985), 1–46.

[31] Kawamata, Y., Termination of log flips for algebraic 3-folds. *Internat. J. Math.* **3** (1992), 653–659.

[32] Kawamata, Y., Deformation of canonical singularities. *J. Amer. Math. Soc.* **12** (1999), 85–92.

[33] Kawamata, Y., Matsuda, K., Matsuki, K., Introduction to the minimal model program. *Adv. Stud. Pure Math.* **10** (1987), 283–360.

[34] Kleiman, S., Toward a numerical theory of ampleness. *Ann. of Math.* **84** (1966), 293–344.

[35] Kodaira, K., On Kähler varieties of restricted type. *Ann. of Math.* **60** (1954), 28–48.

[36] Kodaira, K., Spencer, D.C., On deformations of complex analytic structures. III. Stability theorems for complex structures. *Ann. of Math.* **71** (1960), 43–76.

[37] Kohn, J. J., Harmonic integrals on strongly pseudo-convex manifolds I. *Ann. of Math.* **78** (1963), 206–213.

[38] Lamari, A., Courants kählériens et surfaces compactes. *Ann. Inst. Fourier* **49** (1999), 263–285.

[39] Lamari, A., Le cone Kählérien d'une surface. *J. Math. Pures Appl.* **78** (1999), 249–263.

[40] Manivel, L., Un théorème de prolongement L^2 de sections holomorphes d'un fibré vectoriel. *Math. Z.* **212** (1993), 107–122.

[41] Mori, S., Threefolds whose canonical bundles are not numerically effective. *Ann. of Math.* **116** (1982), 133–176.

[42] Nadel, A. M., Multiplier ideal sheaves and Kähler-Einstein metrics of positive scalar curvature. *Proc. Nat. Acad. Sci. U.S.A.* **86** (1989) 7299–7300; *Ann. of Math.* **132** (1990), 549–596.

[43] Ohsawa, T., On the extension of L^2 holomorphic functions, II. *Publ. Res. Inst. Math. Sci.* **24** (1988), 265–275.

[44] Ohsawa, T., On the extension of L^2 holomorphic functions, III : negligible weights. *Math. Z.* **219** (1995), 215–225.

[45] Ohsawa, T., On the extension of L^2 holomorphic functions, IV: A new density concept. In *Geometry and analysis on complex manifolds* (T. Mabuchi et al., eds.), Festschrift for Professor S. Kobayashi's 60th birthday. World Scientific, Singapore 1994, 157–170.

[46] Ohsawa, T., On the extension of L2 holomorphic functions, V, Effects of generalization. *Nagoya Math. J.* **161** (2001), 1–21.

[47] Ohsawa, T., On the extension of L^2 holomorphic functions, VI, A limiting case. In *Explorations in complex and Riemannian geometry*, Contemp. Math. 332, Amer. Math. Soc., Providence, RI, 2003, 235–239.

[48] Ohsawa, T., Takegoshi, K., On the extension of L^2 holomorphic functions. *Math. Z.* **195** (1987), 197–204.

[49] Păun, M., Sur l'effectivité numérique des images inverses de fibrés en droites. *Math. Ann.* **310** (1998), 411–421.

[50] Păun, M., Fibré en droites numériquement effectifs et variétés Kählériennes compactes à courbure de Ricci nef. Thèse, Université de Grenoble 1, Grenoble 1998.

[51] Păun, M., Semipositive (1,1)-cohomology classes on projective manifolds. *Preprint de l'I.R.M.A.*, Strasbourg.

[52] Păun, M., Siu's invariance of plurigenera: a one-tower proof. Preprint, November 2005.

[53] Shokurov, V. V., Extremal contractions of three-dimensional algebraic varieties. *Yaroslavl Gos. Ped. Inst.* **102** (1983), 74–90 (in Russian).

[54] Shokurov, V. V., 3-fold log models. *J. Math. Sci.* **81** (1996), 2667–2699.

[55] Shokurov, V. V., Prelimiting flips. *Proc. Steklov Inst. Math.* **240** (2003), 75–213.

[56] Siu, Y.-T., Analyticity of sets associated to Lelong numbers and the extension of closed positive currents. *Invent. Math.* **27** (1974), 53–156.

[57] Siu, Y.-T., Some recent results in complex manifold theory for the semi-positive case. In *Proceedings of the Mathematisches Arbeitstagung*, Bonn 1984.

[58] Siu, Y.-T., Invariance of plurigenera. *Invent. Math.* **134** (1994), 631–639.

[59] Siu, Y.-T., Extension of twisted pluricanonical sections with plurisubharmonic weight and invariance of semipositively twisted plurigenera for manifolds not necessarily of general type. In *Complex Geometry* (Göttingen, 2000), Springer-Verlag, Berlin 2002, 223–277.

[60] Skoda, H., Morphismes surjectifs de fibrés vectoriels semi-positifs. *Ann. Sci. École Norm. Sup.* **11** (1978), 577–611.

[61] Takayama, S., Pluricanonical systems on algebraic varieties of general type. *Invent. Math.* **165** (2006), 551–587.

[62] Takayama, S., On the invariance and lower semi-continuity of plurigenera of algebraic varieties. *J. Algebraic Geom.* **16** (2007), 1–18.

[63] Tsuji, H., Pluricanonical systems of projective varieties of general type. *Osaka J. Math.* **43** (2006), 967–995.

[64] Tsuji, H., Subadjunction theorem. In *Complex analysis in several variables—Memorial Conference of Kiyoshi Oka's Centennial Birthday*, Adv. Stud. Pure Math. 42, Math. Soc. Japan, Tokyo 2004, 313–318.

[65] Viehweg, E., Vanishing theorems. *J. Reine Angew. Math.* **335** (1982), 1–8.

[66] Voisin, C., A counterexample to the Hodge conjecture extended to Kähler varieties. *Internat. Math. Res. Notices* **20** (2002), 1057–1075.

[67] Voisin, C., On the homotopy types of compact Kähler and complex projective manifolds. *Invent. Math.* **157** (2004), 329–343.

[68] Voisin, C., On the homotopy types of Kähler manifolds and the birational Kodaira problem. *J. Differential Geom.* **72** (2006), 43–71.

[69] Yau, S.-T., On the Ricci curvature of a complex Kähler manifold and the complex Monge–Ampère equation. *Comm. Pure Appl. Math.* **31** (1978), 339–411.

[70] Zucker, S., The Hodge conjecture for cubic fourfolds. *Compositio Math.* **34** (1977), 199–209.

Université de Grenoble I, Institut Fourier, 100 rue des Maths, BP 74,
38402 Saint-Martin d'Hères, France

E-mail: demailly@fourier.ujf-grenoble.fr

Optimal computation

Ronald A. DeVore*

Abstract. A large portion of computation is concerned with approximating a function u. Typically, there are many ways to proceed with such an approximation leading to a variety of algorithms. We address the question of how we should evaluate such algorithms and compare them. In particular, when can we say that a particular algorithm is optimal or near optimal? We shall base our analysis on the approximation error that is achieved with a given (computational or information) budget n. We shall see that the formulation of optimal algorithms depends to a large extent on the context of the problem. For example, numerically approximating the solution to a PDE is different from approximating a signal or image (for the purposes of compression).

Mathematics Subject Classification (2000). Primary 41-02, 46-02; Secondary 62C20, 65N30, 68Q25, 74S05.

Keywords. Optimal computation, encoding and compression, learning theory, entropy and widths.

1. Introduction

A generic scientific problem is to approximate a function u. The problem takes different forms depending on what we know about u. We describe five common settings.

The Data Fitting Problem (DFP). We are given data $\lambda_j(u)$, $j = 1, 2, \ldots, n$, where each λ_j is a linear functional. The problem is to approximate u the best we can from this information. Often the $\lambda_j(u)$'s are point values of u or averages of u over certain sets (called cells).

The Sensing Problem (SP). In this setting we may ask for the values $\lambda_j(u)$, $j = 1, \ldots, n$, of any linear functionals λ_j applied to u . We are given a budget of n such questions and we wish to determine what are the best questions to ask in order to approximate u effectively. This problem differs from DFP because we can choose the functionals to apply.

The Encoding Problem (EP). Here we have complete knowledge of u. We are given a bit budget n and we wish to transmit as much information about u as possible while

*This paper was prepared while the author was visiting Electrical and Computer Engineering Department at Rice University. The author thanks the participants of the Rice Compressed Sensing Seminar, especially Rich Baraniuk and Mike Wakin, for valuable discussions on compresses sensing. He is also grateful to Carl de Boor, Albert Cohen, Emmanuel Candès, Anna Gilbert, and Guergana Petrova for reading versions of this manuscript.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

using at most n bits. An encoder maps u into a bitstream and a decoder converts the bitstream into a function which approximates u. Both these maps are typically nonlinear.

The Computation Problem (CP). We are only given the information that u is a solution to some (linear or nonlinear) equation $A(u) = f$. We have complete knowledge of the operator A and any additional information (such as boundary or initial conditions) that are sufficient to uniquely determine u. We are given a computational budget n, say of floating point operations (flops), and we wish to approximate u as efficiently as possible within this budget. This problem is related to numerically inverting the operator A.

The Learning Problem (LP). We are given data $z_i = (x_i, y_i) \in X \times Y, i = 1, \dots, n$, which are drawn independently with respect to some unknown probability measure ρ on $X \times Y$. We wish from this data to fit a function which best represents how the response variable y is related to x. The best representation (in the sense of least squares minimization) is given by the regression function $f_\rho(x) := E(y|x)$ with E the expectation. Since we do not know ρ, we do not know f_ρ The problem is to best approximate f_ρ from the given sample data.

These problems have a long history and still remain active and important research areas. The first three of these problems are related to major areas of Approximation Theory and Information Based Complexity and our presentation is framed by core results in these disciplines. CP is the dominant area of Numerical Analysis and LP is central to Nonparametric Statistics. The complexity of algorithms is also a major topic in Theoretical Computer Science. The purpose of this lecture is not to give a comprehensive accounting of the research in these areas. In fact, space will only allow us to enter two of these topics (SP and LP) to any depth. Rather, we want to address the question of how to evaluate the myriad of algorithms for numerically resolving these problems and decide which of these is best. Namely, we ask "what are the ways in which we can evaluate algorithms?"

2. Some common elements

There are some common features to these problems which we want to underscore. The obvious starting point is that in each problem we want to approximate a function u.

2.1. Measuring performance. To measure the success of the approximation, we need a way to measure error between the target function u and any candidate approximation. For this, we use a norm $\|\cdot\|$. If u_n is our approximation to u, then the error in this approximation is measured by

$$\|u - u_n\|. \tag{2.1}$$

Thus, our problem is to make this error as small as possible within the given budget n.

The norm may be of our choosing (in which case we would want to have a theory that applies to a variety of norms) or it may be dictated by the problem at hand. The typical choices are the L_p norms, $1 \le p \le \infty$. Suppose that Ω is a domain in $\mathbb{R}^d$ where $\mathbb{R}^d$ is the d dimensional Euclidean space. We define

$$\|g\|_{L_p(\Omega)} := \begin{cases} (\int_\Omega |g(x)|^p \, dx)^{1/p}, & 1 \le p < \infty, \\ \operatorname*{esssup}_{x\in\Omega} |g(x)|, & p = \infty. \end{cases} \tag{2.2}$$

When studying the solutions to PDEs, norms involving derivatives of u are often more appropriate. We shall delay a discussion of these norms till needed.

In numerical considerations, the norms (2.2) are replaced by discrete versions. If $x \in \mathbb{R}^N$, then

$$\|x\|_{\ell_p} := \begin{cases} \left(\sum_{j=1}^N |x_j|^p\right)^{1/p}, & 0 < p < \infty, \\ \max_{j=1\dots,N} |x_j|, & p = \infty. \end{cases} \tag{2.3}$$

2.2. The form of algorithms: linear versus nonlinear. The numerical algorithms we consider will by necessity be a form of approximation. To understand them, we can use the analytical tools of approximation theory. This is a classical subject which began with the work of Weierstrass, Bernstein, Chebyshev, and Kolmogorov. The quantitative portion of approximation theory seeks to understand how different methods of approximation perform in terms of rates of convergence. If a certain method of approximation is used in the construction of an algorithm then approximation theory can tell us the optimal performance we could expect. Whether we reach that performance or something less will be a rating of the algorithm.

Approximation theory has many chapters. We will partially unfold only one of these with the aim of describing when numerical algorithms are optimal. To keep the discussion as elementary as possible we will primarily focus on approximation in Hilbert spaces where the theory is most transparent. For approximation in other spaces, the reader should consult one of the major books [16], [31].

Let $\mathcal{H}$ be a separable Hilbert space with inner product $\langle \cdot, \cdot \rangle$ and its induced norm $\|f\| := \langle f, f\rangle^{1/2}$. The prototypical examples for $\mathcal{H}$ would be the space $L_2(\Omega)$ defined in (2.2) and ℓ_2 defined in (2.3). We shall consider various types of approximation in $\mathcal{H}$ which will illustrate notions such as linear, nonlinear, and greedy approximation. At the start, we will suppose that $B := \{g_k\}_{k=1}^\infty$ is a complete orthonormal system for $\mathcal{H}$ and use linear combinations of these basis vectors to approximate u. Later, we shall consider more general settings where B is replaced by more general (redundant) systems.

We begin with linear approximation in this setting. We consider the linear spaces $V_n := \operatorname{span}\{g_k\}_{k=1}^n$. These spaces are nested: $V_n \subset V_{n+1}$, $n = 1, \dots$. Each element

$f \in \mathcal{H}$ has a unique expansion

$$f = \sum_{k=1}^{\infty} c_k g_k, \quad c_k := c_k(f) := \langle f, g_k \rangle, \ k = 1, 2, \dots. \tag{2.4}$$

For an important concrete example, the reader can have in mind the space $\mathcal{H} = L_2(\Pi)$ of 2π-periodic functions defined on $\mathbb{R}$ and the Fourier basis. Then (2.4) is just the expansion of f into its Fourier series.

Given $f \in \mathcal{H}$ the function $P_{V_n} f := \sum_{k=1}^{n} c_k(f) g_k$ is the best approximation to f from V_n and the error we incur in such an approximation is given by

$$E_n(f) := \|f - P_{V_n}(f)\| = \Big(\sum_{k=n+1}^{\infty} |c_k(f)|^2 \Big)^{1/2}, \quad n = 1, 2, \dots. \tag{2.5}$$

We are in the wonderful situation of having an explicit formula for the error of approximation in terms of the coefficients $c_k(f)$. We know that for any $f \in \mathcal{H}$ the right side of (2.5) tends to zero as n tends to infinity. The faster the rate of decay, the better we can approximate f and the nicer f is with respect to this basis.

To understand the performance of an approximation process, such as the one described above, it is useful to introduce approximation classes which gather together all functions which have a common approximation rate. For us, it will be sufficient to consider the classes $\mathcal{A}^r$, $r > 0$, consisting of all functions f that are approximated with a rate $O(n^{-r})$. For example, in the case we are discussing $\mathcal{A}^r := \mathcal{A}^r((V_n)) := \mathcal{A}^r((V_n), \mathcal{H})$ consists of all functions $f \in \mathcal{H}$ such that

$$E_n(f) \le M n^{-r}, \quad n = 1, 2, \dots. \tag{2.6}$$

The smallest M such that (2.6) holds is defined to be the norm on this space:

$$|f|_{\mathcal{A}^r} := \sup_{n \ge 1} n^r E_n(f). \tag{2.7}$$

Notice that these approximation spaces are also nested: $\mathcal{A}^r \subset \mathcal{A}^{r'}$ if $r \ge r'$. Given an $f \in \mathcal{H}$ there will be a largest value of $r = r(f, B)$ for which $f \in \mathcal{A}^{r'}$ for all $r' < r$. We can think of this value of r as measuring the smoothness of f with respect to this approximation process or what is the same thing, the smoothness of f with respect to the basis $\{g_k\}$.

For standard orthonormal systems, the approximation spaces $\mathcal{A}^r$ often have an equivalent characterization as classical smoothness spaces. For example, in the case of the Fourier basis, $\mathcal{A}^r$ is identical with the Besov space $B^r_\infty(L_2(\Pi))$. This space is slightly larger than the corresponding Sobolev space $W^r(L_2(\Pi))$. In the case that r is an integer, $W^r(L_2(\Pi))$ is the set of all $f \in L_2(\Pi)$ whose r-th derivative $f^{(r)}$ is also in $L_2(\Pi)$. We do not have the space here to go into the precise definitions of smoothness spaces, but if the reader thinks of the smoothness order as simply corresponding to the number of derivatives that will give the correct intuition.

Observe that two elements are coming into play: the basis we select and the ordering of that basis. A function f may have a faster convergent expansion with respect to one basis B than another B'. That is $r(f, B) > r(f, B')$. If we knew this in advance the better basis would be preferable. Such knowledge is only present through some additional analysis of the problem at hand, e.g. in the case of numerically solving PDEs such information could be provided by a regularity theorem for the PDE. The ordering of the basis functions also plays an important role. Reordering these basis functions results in a different rate of decay for the approximation error and therefore a different $r(f, B)$. Such reordering is done in practice through nonlinear approximation which we now discuss.

Approximation by the elements of V_n is called *linear approximation* because the approximants are taken from the linear space V_n. This is to be contrasted with the following notion of n-term approximation. For each $n \geq 1$, we let Σ_n denote the set of all functions that can be expressed as a linear combination of n terms of the orthonormal basis:

$$S = \sum_{k \in \Lambda} a_k g_k, \quad \#\Lambda \leq n, \tag{2.8}$$

where $\#\Lambda$ is the cardinality of Λ. We consider the approximation of $f \in \mathcal{H}$ by the elements of Σ_n and define the error of such approximation by

$$\sigma_n(f) := \sigma_n(f)_{\mathcal{H}} := \inf_{S \in \Sigma_n} \|f - S\|, \quad n = 1, 2, \ldots. \tag{2.9}$$

Notice that E_n is generally reserved for the error in linear approximation and σ_n for the error in nonlinear approximation.

Another view of n-term approximation is that we approximate the function f by the elements of a linear space W_n spanned by the elements of n basis functions. However, it differs from linear approximation in that we allow the space W_n to also be chosen depending on f, that is, it is not fixed in advance as was the case for linear approximation.

It is very easy to describe the best approximant to f from Σ_n and the resulting error of approximation. Given $f \in \mathcal{H}$ we denote by (c_k^*) the decreasing rearrangement of the sequence $(c_j = c_j(f))$. Thus, $|c_k^*|$ is the k-th largest of the numbers $|c_j(f)|$, $j = 1, 2, \ldots$. Each $c_k^* = c_{j_k}(f)$ for some j_k. The choice of the mapping $k \mapsto j_k$ is not unique because of possible ties in the size of coefficient but the following discussion is immune to such differences. A best approximation to $f \in \mathcal{H}$ from Σ_n is given by

$$S^* = \sum_{k=1}^{n} c_{j_k}(f) g_{j_k} = \sum_{j \in \Lambda_n^*} c_j(f) g_j, \quad \Lambda_n^* := \Lambda_n^*(f) := \{j_1, \ldots, j_n\}, \tag{2.10}$$

and the resulting error of approximation is

$$\sigma_n(f)^2 = \sum_{k > n} (c_k^*)^2 = \sum_{j \notin \Lambda_n^*} |c_j(f)|^2. \tag{2.11}$$

Indeed, if $S = \sum_{j\in\Lambda} a_j g_j$ is any element of Σ_n, then

$$\|f - S\|^2 = \sum_{j\in\Lambda}(c_j - a_j)^2 + \sum_{j\in\Lambda^c} c_j^2, \tag{2.12}$$

where Λ^c is the complement of Λ. The second sum on the right side of (2.12) is at least as large as $\sum_{k>n}(c_k^*)^2$ and so we attain the smallest error by taking a set of indices $\Lambda = \Lambda_n^*(f)$ corresponding to the n largest coefficients and then taking $a_j = c_j(f)$ for $j \in \Lambda$.

Notice that the space Σ_n is not linear. If we add two elements from Σ_n, we will generally need $2n$ terms to represent the sum. For this reason, n-term approximation is a form of *nonlinear approximation*. We can define approximation classes $\mathcal{A}^r((\Sigma_n), \mathcal{H})$ for this form of approximation by replacing $E_n(f)$ by $\sigma_n(f)$ in (2.6) and (2.7). To distinguish between linear and nonlinear approximation we will sometimes write $\mathcal{A}^r(L)$ and $\mathcal{A}^r(NL)$ for the two approximation classes thereby indicating that the one corresponds to linear approximation and the other to nonlinear approximation.

It is easy to characterize when an f belongs to $\mathcal{A}^r((\Sigma_n), \mathcal{H})$ in terms of the coefficients $c_k(f)$. For this, recall that a sequence (a_k) is said to be in the space $w\ell_p$ (weak ℓ_p) if

$$\#\{k : |a_k| \geq \eta\} \leq M^p \eta^{-p} \tag{2.13}$$

and the smallest M for which (2.13) holds is called the weak ℓ_p norm ($\|(a_k)\|_{w\ell_p}$) of this sequence. An equivalent definition is that the decreasing rearrangement of (a_k) satisfies

$$|a_k^*| \leq M^{1/p} k^{-1/p}, \quad k = 1, 2, \ldots. \tag{2.14}$$

A simple exercise proves that $f \in \mathcal{A}^r((\Sigma_n), \mathcal{H})$ if and only if $(c_k(f)) \in w\ell_p$ with $1/p = r + 1/2$, and the norms $|f|_{\mathcal{A}^r}$ and $\|(c_k(f))\|_{w\ell_p}$ are equivalent (see [30] or [16]). Notice that $\mathcal{A}^r(L) \subset \mathcal{A}^r(NL)$ but the latter set is much larger. Indeed, for linear approximation a function $f \in \mathcal{H}$ will be approximated well only if its coefficients decay rapidly with respect to the usual basis ordering but in nonlinear approximation we can reorder the basis in any way we want. As an example, consider again the Fourier basis. The space $\mathcal{A}^{1/2}(NL)$ consists of all functions whose Fourier coefficients are in $w\ell_1$. A slightly stronger condition is that the Fourier coefficients are in ℓ_1 which means the Fourier series of f converges absolutely.

In n-term approximation, the n-dimensional space used in the approximation depends on f. However, this space is restricted to be spanned by n terms of the given orthonormal basis. If we are bold, we can seek even more approximation capability by allowing the competition to come from more general collections of n-dimensional spaces. However, we would soon see that opening the competition to be too large will render the approximation process useless in computation since it would be impossible to implement such a search numerically (this topic will be discussed in more detail in Section 4).

There is a standard way to open up the possibilities of using more general families in the approximation process. We say a collection of function $\mathcal{D} = \{g\}_{g\in\mathcal{D}} \subset \mathcal{H}$ is a

dictionary if each $g \in \mathcal{D}$ has norm one ($\|g\| = 1$). We define $\Sigma_n := \Sigma_n(\mathcal{D})$ as the set of all S that are a linear combination of at most n dictionary elements: $S = \sum_{g\in\Lambda} c_g g$ with $\#(\Lambda) \le n$. The n-term approximation error σ_n and the approximation classes $\mathcal{A}^r(\mathcal{D}, \mathcal{H})$ are then defined accordingly. Notice that the elements in $\mathcal{D}$ need not be linearly independent, i.e., the dictionary allows for redundancy.

It is a bit surprising that meaningful theorems about $\mathcal{A}^r$ can be proved in this very general setting. To find good n-term approximations, we cannot simply select indices with large coefficients because of the possible redundancy in the dictionary. Rather, we proceed by an important technique known as *greedy approximation* (sometimes called *matching pursuit*). This is an iterative procedure which selects at each step a best one-term approximation to the current residual. Given $f \in \mathcal{H}$, we initially define $f_0 := 0$ and the residual $r_0 := f - f_0 = f$. Having defined the current approximation f_{n-1} and its residual $r_{n-1} := f - f_{n-1}$ for some $n \ge 1$, we will choose an element $g_n \in \mathcal{D}$ and update the approximation to f by including g_n in the n-term approximation. The usual way of proceeding is to choose g_n as

$$g_n := \operatorname*{Argmax}_{g\in\mathcal{D}} \langle r_{n-1}, g\rangle, \tag{2.15}$$

although there are important variants of this strategy. Having chosen g_n in this way, there are different algorithms depending on how we proceed. In the Pure Greedy Algorithm (PGA), we define

$$f_n := f_{n-1} + \langle f_{n-1}, g_n\rangle g_n \tag{2.16}$$

which yields the new residual $r_n := f - f_n$. We can do better, but with more computational cost, if we define

$$f_n := P_{V_n} f \tag{2.17}$$

where $V_n := \operatorname{span}\{g_1, \dots, g_n\}$. This procedure is called the Orthogonal Greedy Algorithm (OGA). There is another important variant which is analogous to numerical descent methods called Restricted Greedy Approximation(RGA). It defines

$$f_n := \alpha_n f_{n-1} + \beta_n g_n \tag{2.18}$$

where $0 < \alpha_n < 1$ and $\beta_n > 0$. Typical choices for α_n are $1 - 1/n$ or $1 - 2/n$. There are other variants in the RGA where the choice of g_n is altered. The most general procedure is to allow α, β, g to be arbitrary and choose $\alpha f_{n-1} + \beta g$ that minimizes the norm of the residual $r = f - \alpha f_{n-1} - \beta g$.

Greedy algorithms have been known for decades. Their numerical implementation and approximation properties were first championed in statistical settings ([42], [4], [46]). The approximation properties have some analogy to those for nonlinear approximation from a basis but are not as far reaching. To briefly describe some of these results, let $\mathcal{L}_1$ consist of all functions $f \in \mathcal{H}$ such that

$$f = \sum_{g\in\mathcal{D}} c_g g, \quad \sum_{g\in\mathcal{D}} |c_g| < +\infty. \tag{2.19}$$

We can define a norm on this space by

$$|f|_{\mathcal{L}_1} := \inf\Big\{ \textstyle\sum_{g\in\mathcal{D}} |c_g| : \ f = \sum_{g\in\mathcal{D}} c_g g\Big\}. \tag{2.20}$$

Thus, the unit ball of $\mathcal{L}_1$ is the convex closure of $\mathcal{D} \cup (-\mathcal{D})$.

If $f \in \mathcal{L}_1$, then both the OGA and properly chosen RGA will satisfy

$$\|f - f_n\| \le C_0 |f|_{\mathcal{L}_1} n^{-1/2}, \quad n = 1, 2, \ldots, \tag{2.21}$$

as was proved in [42] (see also [29]). The convergence rates for the PGA are more subtle (see [29]) and its convergence rate on $\mathcal{L}_1$ are not completely known. These results show that $\mathcal{L}_1 \subset \mathcal{A}^{1/2}$ which is quite similar to our characterization of this approximation class for nonlinear approximation when using a fixed orthonormal basis.

One unsatisfactory point about (2.21) is that it does not give any information about convergence rates when f is not in $\mathcal{L}_1$. Using interpolation, one can introduce function classes that guarantee approximation rates $O(n^{-r})$ when $0 < r < 1/2$ (see [5]). Also, using (2.21), one can prove that for $r > 1/2$ a sufficient condition for f to be in $\mathcal{A}^r(\mathcal{D}, \mathcal{H})$ is that it has an expansion $f = \sum_{g\in\mathcal{D}} c_g g$ with $(c_g) \in \ell_p$, $p := (r + 1/2)^{-1}$. However, this condition is generally not sufficient to ensure the convergence of the greedy algorithm at the corresponding rate n^{-r}.

Although greedy approximation is formulated in a very general context, any numerical algorithm based on this notion will have to deal with finite dictionaries. The size of the dictionary will play an important role in the number of computations needed to execute the algorithm. Greedy approximation remains an active and important area for numerical computation. A fairly up to date survey of greedy approximation is found in [56]. We will touch on greedy approximation again in our discussion of the Sensing Problem and the Learning Problem.

3. Optimality of algorithms

Our goal is to understand what is the optimal performance that we can ask from an algorithm. Recall that in each of our problems, our task is to approximate a function u. What differs in these problems is what we know in advance about u and how we can access additional information about u.

Because of the diversity of problems we are discussing, we shall not give a precise definition of an algorithm until a topic is discussed in more detail. Generically an algorithm is a sequence $\boldsymbol{A} = (A_n)$ of mappings. Here n is the parameter associated to each of our problems, e.g., it is the number of computations allotted in the computation problem. The input for the mapping A_n is different in each of our problems. For example, in the data fitting problem it is values $\lambda_j(u)$, $j = 1, \ldots, n$, that are given to us. The output of A_n is an approximation u_n to the target function u. To study the performance of the algorithm, we typically consider what happens in this

approximation as $n \to \infty$. Such a theory will miss out on important but usually very subtle questions about performance for small n.

We fix the space X and the norm $\|\cdot\| = \|\cdot\|_X$ in which to measure error. Then, for any u,

$$E(u, A_n) := \|u - u_n\|, \quad n = 1, 2, \ldots, \tag{3.1}$$

measures how well the algorithm approximates u. It is tempting to define an optimal algorithm to be a sequence (A_n^*) such that

$$E(u, A_n^*) \le \inf_{A_n} E(u, A_n), \quad u \in X,\ n = 1, 2, \ldots, \tag{3.2}$$

where the infimum is taken over all algorithms A_n. However, such a definition is meaningless, since to achieve such a performance the algorithm would typically involve a search which is prohibitive from both a theoretical and numerical perspective.

Here is another important point. An algorithm only sees the given data. In the Recovery Problem and Sensing Problem, A_n will only act on the data $\lambda_j(u)$, $j = 1, \ldots, n$. This means that many functions have the same approximation u_n. If $\mathcal{N}$ is the null space consisting of all functions v such that $\lambda_j(v) = 0$, $j = 1, \ldots, n$, then all functions $u + \eta$, $\eta \in \mathcal{N}$, have the same data and hence u_n is a common approximation to all of these functions. Since $\|\eta\|$ can be arbitrarily large, we cannot say anything about $\|u - u_n\|$ being small without additional information about u.

There are two ways to come to a meaningful notion of optimality which we shall describe: optimality on classes and instance-optimal. We begin with the first of these which is often used in statistics, approximation theory and information based complexity. Consider any compact set $K \subset X$. We define

$$E(K, A_n) := \sup_{u \in K} E(u, A_n), \quad n = 1, 2, \ldots, \tag{3.3}$$

which measures the worst performance of A_n on K. We shall say that (A_n^*) is *near optimal* on K with constant $C = C(K)$ if

$$E(K, A_n^*) \le C \inf_{A_n} E(K, A_n), \quad n = 1, 2, \ldots. \tag{3.4}$$

If $C = 1$ we say (A_n^*) is *optimal* on K. Usually, it is not possible to construct optimal algorithms, so we shall mainly be concerned with near optimal algorithms, although the size of the constant C is a relevant issue.

The deficiency of the above notion of optimality is that it depends on the choice of the class K. An appropriate class for u may not be known to us. Thus, an algorithm is to be preferred if it is near optimal for a large collection of classes K. We say that an algorithm $\boldsymbol{A}$ is *universal* for the collection $\mathcal{K}$, if the bound (3.4) holds for each $K \in \mathcal{K}$ where the constant $C = C(K)$ may depend on K .

There are two common ways to describe compact classes in a function space X. The first is through some uniform smoothness of the elements. For example, the unit ball $K = U(Y)$ of a smoothness space Y of X is a typical way of obtaining a compact

subset of X. We say that Y is compactly embedded in X if each finite ball in Y is a compact subset of X.

The classical smoothness spaces are the Sobolev and Besov spaces. The Sobolev space $W^s(L_q) = W^s(L_q(\Omega))$, $\Omega \subset \mathbb{R}^d$, consists of all functions u which have smoothness of order s in L_q. In the case $s = k$ is an integer and $1 \le q \le \infty$ this simply means that u and all its (weak) derivatives are in L_q. There are generalizations of this definition to arbitrary $s, q > 0$. The Besov spaces $B^s_\lambda(L_q)$ are also smoothness spaces of order s in L_q but they involve another parameter λ which makes subtle distinctions among these spaces. They are similar to but generally different from the Sobolev spaces. The Sobolev embedding theorem describes the smoothness spaces which are embedded in a space $X = L_p(\Omega)$ provided the domain Ω has sufficient smoothness (a C^1 smooth boundary is more than enough). This embedding theorem has a simple geometrical interpretation. We identify each space $W^s(L_q)$ (likewise $B^s_\lambda(L_q)$) with the point $(1/q, s)$ in the upper right quadrant of $\mathbb{R}^2$. Given a value $p \in (0, \infty]$, the line $s = d/q - d/p$ is called the critical line for embedding into $L_p(\Omega)$. Any Sobolev or Besov space corresponding to a point above this line is compactly embedded into $L_p(\Omega)$. Any point on or below the line is not compactly embedded into $L_p(\Omega)$. For example, if $s > d/q$, then the Sobolev space $W^s(L_q(\Omega))$ is compactly embedded into the space $C(\Omega)$ of continuous functions on Ω.

A second way to describe compact spaces is through approximation. For example, suppose that $X_n \subset X$, $n = 1, 2, \ldots$, is a sequence of linear spaces of dimension n. Then each of the approximation classes $\mathcal{A}^r$, $r > 0$, describes compact subsets of X: any finite ball in $\mathcal{A}^r$ (with the norm defined by (2.7)) gives a compact subset of X. In the same way, the approximation classes $\mathcal{A}^r$, $r > 0$, for standard methods of nonlinear approximation also give compact subsets of X.

Given the wide range of compact sets in X, it would be too much to ask that an algorithm be universal for the collection of all compact subsets of X. However, universality for large families would be reasonable. For example, if our approximation takes place in $X = L_p(\Omega)$, we could ask that the algorithm be universal for the collection $\mathcal{K}$ of all finite balls in all the Sobolev and Besov spaces with smoothness index $0 < s \le S$ that compactly embed into X. Here S is arbitrary but fixed. This would be a reasonable goal for an algorithm. There are approximation procedures that have this property. Namely, the two nonlinear methods (i) n-term wavelet approximation restricted to trees, and (ii) adaptive piecewise polynomial approximation described in the following section have this property.

In many settings, it is more comfortable to consider optimality over classes described by approximation. Suppose that we have some approximation procedure (linear or nonlinear) in hand. Then, the set $\mathcal{K} := \{B(\mathcal{A}^r) : 0 < r \le R\}$ of all finite balls of the $\mathcal{A}^r$, is a collection of compact sets and we might ask the algorithm to be universal on this collection. Notice that this collection depends very much on the given approximation procedure, and in a sense the choice of this approximation procedure is steering the form of the algorithms we are considering. Since most often, algorithms are designed on the basis of some approximation procedure, finite balls in

approximation classes are natural compact sets to consider.

In the setting of a specific approximation process, we can carry the notion of optimality even further. If $E_n(u)$ denotes the error in approximating u by the approximation procedure, then we say that the algorithm $\mathcal{A} = (A_n)$ is *instance-optimal* with constant $C > 0$ if

$$E(u, A_n) \leq C E_n(u) \quad \text{for all } u \in X. \tag{3.5}$$

In other words, the algorithm, in spite of having only partial knowledge about u, approximates, up to a constant, as well as the best approximation. Instance-optimal is a stronger notion than universality on approximation classes. Consider for example n term approximation from a dictionary $\mathcal{D}$. Then $E_n(u)$ on the right side of (3.5) is the error $\sigma_n(u)$ of n term approximation. Knowing that (3.5) is valid, we conclude immediately that the algorithm is universal on the class of approximation spaces $\mathcal{A}^r$, $r > 0$. The choice of the dictionary plays a critical role in defining these notions of optimality.

In summary, we have two possible ways to evaluate the performance of an algorithm. The first is to test its behavior over classes which leads to the notion of optimal, near optimal, and universal. If we consider algorithms based on a specific approximation process, then we can ask for the finer description of optimality described as instance-optimal.

4. Two important examples

Before returning to our main subject of optimal computation, it will be useful to have some concrete approximation processes in hand. We consider two examples of approximation systems that are used frequently in computation and serve to illustrate some basic principles.

4.1. Wavelet bases. A univariate *wavelet* is a function $\psi \in L_2(\mathbb{R})$ whose shifted dilates

$$\psi_{j,k}(x) := 2^{j/2}\psi(2^j x - k), \quad j, k \in \mathbb{Z}, \tag{4.1}$$

are a basis for $L_2(\mathbb{R})$. In the case that the functions (4.1) form a complete orthonormal system we say that ψ is an *orthogonal wavelet*. The simplest example is the Haar orthogonal wavelet

$$H(x) := \chi_{[0,1/2)} - \chi_{[1/2,1)} \tag{4.2}$$

where χ_A the indicator function of a set A. Although the Haar function was prominent in harmonic analysis and probability, it was not heavily used in computation because the function H is not very smooth and also the Haar system has limited approximation capacity. It was not until the late 1980s that it was discovered (Meyer [50] and Daubechies [26]) that there are many wavelet functions ψ and they can be constructed to meet most numerical needs. The most popular wavelets are the compactly supported orthogonal wavelets of Daubechies [26] and the biorthogonal wavelet of Cohen

and Daubechies [22]. They can be constructed from the framework of multiresolution analysis as described by Mallat [48]. Wavelet bases are easily constructed for $\mathbb{R}^d$ and more generally for domains $\Omega \subset \mathbb{R}^d$. There are several books which give far reaching discussions of wavelet decompositions (see e.g. [51] for wavelets and harmonic analysis, [27] for wavelet constructions, [49] for wavelets in signal processing, and [16] for wavelets in numerical PDEs.).

We shall denote a wavelet basis by $\{\psi_\lambda\}_{\lambda\in\Gamma}$. In the case of $\mathbb{R}^d$ or domains $\Omega \subset \mathbb{R}^d$, the index λ depends on three parameters (j, k, e). The integer j gives the dyadic level of the wavelet as in (4.1). The multi-integer $k = (k_1, \dots, k_d)$ locates the wavelet in space (it is associated to the point $2^{-j}k$). The index e corresponds to a vertex of the unit cube $[0, 1]^d$ and describes the gender of the wavelet. We can also think of the wavelets as indexed on the pairs I, $\mathbf{e}$ where $I = 2^{-j}(k + [0, 1]^d)$ is a dyadic cube. In this way, the wavelets are associated to a tree of dyadic cubes. This tree structure is important in computation.

We will always suppose that the wavelets ψ_λ are compactly supported. Each locally integrable function has a wavelet decomposition

$$f = \sum_{\lambda\in\Gamma} f_\lambda \psi_\lambda = \sum_{(I,e)} f_{I.e}\psi_{I,e}. \tag{4.3}$$

The wavelet system is an unconditional basis for L_p and many function spaces such as the Sobolev and Besov spaces.

Let Ω be a domain in $\mathbb{R}^d$ and $\{\psi_\lambda\}_{\lambda\in\Gamma}$ be an orthogonal (or more generally a biorthogonal) wavelet system for $L_2(\Omega)$. The nonlinear spaces Σ_n and their corresponding approximation spaces $\mathcal{A}^r((\psi_\lambda), L_2(\Omega))$ were already introduced in §2.2. These spaces are closely related to classical smoothness spaces. Consider for example the space $\mathcal{A}^r$ which as we know is identical with the space of functions whose wavelet coefficients are weak ℓ_p with $p = (r + 1/2)^{-1}$. While this is not a Besov space, it is closely related to the space $B_p^{rd}(L_p)$ which is contained in $\mathcal{A}^r$. This latter Besov space is characterized by saying that the wavelet coefficients are in ℓ_p.

General n-term wavelet approximation cannot be used directly in computational algorithms because the largest wavelet coefficients could appear at any scale and it is impossible to implement a search over all dyadic scales. There are two natural ways to modify n-term approximation to make it numerically realizable. The first is to simply restrict n-term approximation to dyadic levels $\le a \log n$ where $a > 0$ is a fixed parameter to be chosen depending on the problem at hand. Notice that the number of wavelets living at these dyadic levels does not exceed $C2^{ad\log n} = Cn^{ad}$. The larger the choice of a then the more intensive will be the computation.

The second way to numerically implement the ideas of n-term approximation in the wavelet setting is to take advantage of the tree structure of wavelet decompositions. Given a dyadic cube I, its *children* are the 2^d dyadic subcubes $J \subset I$ of measure $2^{-d}|I|$ and I is called the *parent* of these children. We say that T is a tree of dyadic cubes if whenever $J \in T$ with $|J| < 1$, then its parent is also in T. We define $\mathcal{T}_n$ to be

the collection of all trees of cardinality $\leq n$. We define Σ_n^t as the set of all functions

$$S = \sum_{I \in T} \sum_{e \in E_I} c_I^e \psi_I^e, \quad \#T \leq n, \tag{4.4}$$

where $E_I = E'$ if $|I| = 1$ and $E_I = E$ otherwise. Replacing Σ_n by Σ_n^t in (2.9) leads to σ_n^t and the approximation classes $\mathcal{A}^r((\Sigma_n^t))$. Tree approximation is only slightly more restrictive than n-term approximation. For example, if $B_\lambda^s(L_p)$ is a Besov space that compactly embeds into L_q then any function in this space is in $\mathcal{A}^{s/d}((\Sigma_n^t), L_q)$. This is the same approximation rate as is guaranteed by general n-term approximation for this class.

4.2. Adaptive partitioning. Much of numerical PDEs is built on approximation by piecewise polynomials on partitions of the domain Ω. A partition Π of Ω is a finite collection of sets C_i (called *cells*), $i = 1, \ldots, N$, whose interiors are pairwise disjoint and union to Ω. We have already met the partitions $\mathcal{D}_j$ of the domain $\Omega = [0, 1]^d$ into dyadic cubes.

The typical way of generating partitions is through a *refinement rule* which tells how a cell is to be subdivided. In the dyadic subdivision case, the cells are dyadic cubes and if a cell I in the partition is subdivided then it is replaced by the set $\mathcal{C}(I)$ of its children.

There are many possible refinement strategies. For simplicity, we discuss only the additional case when Ω is a polygonal domain in $\mathbb{R}^2$ and the cells are triangles. We begin with an initial triangulation Π_0. If any triangle Δ is to be refined then its children consist of $a \geq 2$ triangles which form a partition of Δ. We shall assume that the refinement rule is the same for each triangle and thus a is a fixed constant. The refinement rule induces an infinite tree T^* (called the *master tree*) whose nodes are the triangles that can arise through the refinement process.

The refinement level j of a node of T^* is the smallest number of refinements (starting from Π_0) to create this node. We denote by T_j the proper subtree consisting of all nodes with level $\leq j$ and we denote by Π_j the partition corresponding to T_j which is simply all $\Delta \in T_j$ of refinement level j, i.e., the leaves of T_j. The partitions Π_j, $j = 0, 1, \ldots$, we obtain in this way are called *uniform partitions*. The cardinality $\#(\Pi_j)$ of Π_j is $a^j \#(\Pi_0)$.

Another way of generating partitions is by refining some but not all cells. One begins with the cells in Π_0 and decides whether to refine $\Delta \in \Pi_0$ (i.e. subdivide Δ). If Δ is subdivided then it is removed from the partition and replaced by its children. Continuing in this way, we obtain finite partitions which are not necessarily uniform. They may have finer level of refinements in some regions than in others. Each such partition Π can be identified with a finite subtree $T = T(\Pi)$ of the master tree T^*. The cardinalities of Π and $T(\Pi)$ are comparable.

Given a partition Π, let us denote by $\mathcal{S}_k(\Pi)$ the space of piecewise polynomials

of degree k that are subordinate to Π. Each $S \in \mathcal{S}_k\Pi$) can be written

$$S = \sum_{I \in \Pi} P_I \chi_I, \tag{4.5}$$

where P_I is a polynomial of degree $\leq k$. The functions in $\mathcal{S}_k(\Pi)$ are not continuous. In many applications, one is interested in subspaces of $\mathcal{S}_k(\Pi)$ obtained by imposing some global smoothness conditions.

We fix $k \geq 0$ and some norm $\|\cdot\| = \|\cdot\|_X$ where X is an L_p or Sobolev space. We consider two types of approximation. The first corresponds to uniform refinement and gives the error

$$E_n(u) := E_{n,k}(u) := \inf_{S \in \mathcal{S}_k(\Pi_n)} \|u - S\|, \quad n = 0, 1, \ldots. \tag{4.6}$$

This is a form of linear approximation.

To describe an alternative to linear approximation, we let $\mathcal{P}_n$ denote the set of all partitions of size $\leq n$ obtained by using successive refinements. Each partition in $\mathcal{P}_n$ corresponds to a finite tree T contained in the master tree. We define $\Sigma_{n,k}$ as the union of all the spaces $\mathcal{S}_k(\Pi)$, $\Pi \in \mathcal{P}_n$, and the approximation error $\sigma_n(u) := \sigma_{n,k}(u)$ as usual (see (2.9)). This is a form of nonlinear approximation. Its advantage over fixed partitions is that given u, we have the possibility to refine the partition only where u is not smooth and keep it coarse where u is smooth. This means we should be able to meet a given approximation tolerance with a fewer number of cells in the partition. This is reflected in the following results. For either of the two refinement settings we are describing, approximation from $\Sigma_{n,k}$ is very similar to wavelet approximation on trees. For example, if the approximation takes place in an L_q space, then any Besov or Sobolev classes of smoothness order s that compactly embeds into L_q will be contained in $\mathcal{A}^{s/d}((\Sigma_{n,k}), L_q)$ (see [8] and [32]).

In numerical implementations of nonlinear partitioning, we need a way to decide when to refine a cell or not. An *adaptive algorithm* provides such a strategy typically by using local error estimators that monitor the error $e(I)$ between u and the current approximation on a given cell I. Constructing good error estimators in the given numerical setting is usually the main challenge in adaptive approximation.

5. The Sensing Problem

The Sensing Problem is a good illustration of the concepts of optimality that we have introduced. We are given a budget of n questions we can ask about u. These questions are required to take the form of asking for the values $\lambda_1(u), \ldots, \lambda_n(u)$ of linear functionals λ_j, $j = 1, \ldots, n$. We want to choose these functionals to capture the most information about u in the sense that from this information we can approximate u well. The sensing problem is most prominent in signal processing. Analog signals are time dependent functions. A sensor might sample the function through the linear

functionals λ_j, $j = 1, \ldots, n$, and record quantizations of these samples for later processing.

We begin the discussion by assuming that the functions u we wish to sense come from a space $X = L_p(\Omega)$ with $\Omega \subset \mathbb{R}^d$ and $1 \leq p \leq \infty$ and that we will measure the error of approximation in the norm $\|\cdot\| := \|\cdot\|_X$ for this space. An algorithm $\boldsymbol{A} = (A_n)$ takes the following form. For each $n = 1, 2, \ldots$, we have an *encoder* Φ_n which assigns to $u \in X$ the vector

$$\Phi_n(u) := (\lambda_1^n(u), \ldots, \lambda_n^n(u)) \in \mathbb{R}^n, \tag{5.1}$$

where the λ_j^n, $j = 1, \ldots, n$, are fixed linear functionals on X. The mapping $\Phi_n \colon X \to \mathbb{R}^n$ is linear and the vector $\Phi_n(u)$ is the information the sensor will extract about u. Note that we allow these questions to change with n. Another possibility is to require that these questions are progressive which means that for $n + 1$ we simply add one additional question to our current set. We will also need a *decoder* Δ_n which says how to construct an approximation to u from this given data. Thus, Δ_n will be a (possibly nonlinear) mapping from $\mathbb{R}^n$ back into X. Our approximation to u then takes the form

$$A_n(u) := \Delta_n(\Phi_n(u)), \quad n = 1, 2, \ldots. \tag{5.2}$$

Given a vector $y \in \mathbb{R}^n$, the set of functions $\mathcal{F}(y) = \{u \in X : \Phi_n(u) = y\}$ all have the same sensing information and hence will all share the same approximation $A_n(u) = \Delta_n(y)$. If u_0 is any element of $\mathcal{F}(y)$, then

$$\mathcal{F}(y) = u_0 + \mathcal{N}, \tag{5.3}$$

where $\mathcal{N} := \mathcal{N}_n := \mathcal{F}(0)$ is the null space of Φ_n. The structure of this null space is key to obtaining meaningful results.

We have emphasized that in comparing algorithms, we have two possible avenues to take. The one was optimality over classes of functions, the other was instance-optimal. If K is a compact subset of X and Φ_n is an encoder then

$$\bar{\Delta}_n(y) := \operatorname*{Argmin}_{\bar{u} \in X} \sup_{u \in \mathcal{F}(y) \cap K} \|u - \bar{u}\| \tag{5.4}$$

is an optimal decoder for Φ_n on K. Notice that $\bar{\Delta}_n$ is not a practical decoder, its only purpose is to give a benchmark on how well Φ_n is performing. This also leads to the optimal algorithm on the class K which uses the encoder

$$\Phi_n^* := \operatorname*{Argmin}_{\Phi_n} \sup_{u \in K} \|u - \bar{\Delta}_n(\Phi_n(u))\| \tag{5.5}$$

together with the optimal decoder $\bar{\Delta}_n$ associated to Φ_n^* and gives the optimal error

$$E_n^*(K) = \sup_{u \in K} \|u - \bar{\Delta}_N(\Phi_n^*(u))\|. \tag{5.6}$$

We have used the asterisk to distinguish E_n^* from the linear approximation error E_n.

$E_n^*(K)$ is essentially related to the Gelfand n-width $d^n(K)$ of K (see [47], [54] for the definition and properties of Gelfand widths). For example, if $K = -K$ and $K + K \subset C_0 K$, then $d^n(K) \le E_n^*(K) \le C_0 d^n(K)$. Gelfand widths of classical classes of functions such as unit balls of Besov and Sobolev spaces are known. The deepest results in this field are due to Kashin [44] who used probabilistic methods to find optimal sensing functionals. In Kashin's constructions, the problems are discretized and the discrete problems are solved using certain random matrices. We shall return to these ideas in a moment when we turn to discrete compressed sensing.

The usual models for signals are band-limited functions. A typical function class consists of all functions $u \in L_2$ whose Fourier transform vanishes outside of some interval $[-A\pi, A\pi]$ with $A > 0$ fixed. The famous Shannon sampling theorem says that sampling the signal u at the points n/A contains enough information to exactly recover u. The Shannon theory is the starting point for many Analog to Digital encoders. However, these encoders are severely taxed when A is large. In this case, one would like to make much fewer measurements. Since the Shannon sampling is optimal for band-limited signals, improved performance will require the introduction of new (realistic) model classes for signals. One model in this direction, that we will utilize, is to assume that the signal can be approximated well using n terms of some specified dictionary $\mathcal{D}$ of waveforms. For example, we can assume that u is in one of the approximation classes $\mathcal{A}^r((\Sigma_n), X)$ for n-term approximation by the elements of $\mathcal{D}$. We will consider the simplest model for this problem where $\mathcal{D} = B$ is an orthogonal basis B. When this basis is the wavelet basis then we have seen that $\mathcal{A}^r$ is related to Besov smoothness, so the case of classical smoothness spaces is included in these models.

The obvious way of approximating functions in these classes is to retain only the largest terms in the basis expansion of u. However, this ostensibly requires examining all of these coefficients or in other words, using as samples all of the expansion coefficients. Later we would discard most or many of these coefficients to obtain an efficient decomposition of u using only a few terms. A central question in the Sensing Problem is whether one could avoid taking such a large number of sensing samples and still retain the ability to approximate u well. Of course, we have to deal with the fact that we do not know which of these coefficients will be large. So the information will have to, in some sense, tell us both the position of the large coefficients of u and their numerical value as well.

5.1. Discrete compressed sensing. To numerically treat the sensing problem, we have to make it finite – we cannot deal with infinite expansions or computations with infinite length vectors. Discretization to finite dimensional problems is also used to prove results for function spaces. We will therefore restrict our attention to the following discrete sensing problem. We assume our signal is a vector x in $\mathbb{R}^N$ where N is large. We are given a budget of n linear measurements of x (the application of n linear functionals to x) and we ask how well we can recover x from this information.

The previously mentioned results of Kashin [44] show that using n randomly generated functionals will carry almost as much information as knowing the positions and values of the n largest coordinates of x. However, Kashin's results were never implemented into practical algorithms. It was not until the exciting results of Candès, Romberg, and Tao [12] applied to tomography that the door was opened to view the power of random sampling. This was followed by the fundamental papers [13, 15, 34] which addressed how to build practical encoder/decoders and proved the first results on their provable performance. There was a related development in the computer science community which used random measurements to sketch large data sets which we shall say a little more about later.

The discrete sensing problem can be described by an $n \times N$ matrix Φ. Row i of Φ corresponds to a vector that represents the linear functional λ_i. Thus, sensing with these linear functionals is the same as evaluating $\Phi(x) = y$. The vector y which lives in the lower dimensional space $\mathbb{R}^n$ represents the information we have about x. We are interested in how well we can recover x from this information. As we have noted, the exact way we recover x (or an approximation to x) from the information y is a significant component of the problem. A decoder for Φ is a (possibly nonlinear) mapping Δ from $\mathbb{R}^n$ to $\mathbb{R}^N$. Given $y = \Phi(x)$, then $\Delta(y)$ is our approximation to x.

In analogy with the continuous case, we can use the ℓ_p norms, defined in (2.3), to measure error. Then, the error associated to a particular algorithm A_n built on a matrix Φ and a particular decoder Δ is given by

$$E(x, A_n)_p := E(x, \Phi, \Delta)_p := \|x - \Delta(\Phi(x))\|_{\ell_p}. \tag{5.7}$$

The approximation on a class K of signals is defined as in (3.3). Let us denote by $E_n^*(K, \ell_p)$ the optimal error on K achievable by any sensing algorithm of order n (we are suppressing the dependence on N). In keeping with the main theme of this paper, let us mention the types of results we could ask of such a sensing/decoding strategy. We denote by Σ_k the space of all k-sparse vectors in $\mathbb{R}^N$, i.e., vectors with support $\leq k$. For any sequence space X, we denote by $\sigma_k(x)_X$ the error in approximating x by the elements of Σ_k in the norm $\|\cdot\|_X$.

I. Exact reconstruction of sparse signals. Given k, we could ask that

$$\Delta(\Phi(x)) = x, \quad x \in \Sigma_k. \tag{5.8}$$

We would measure the effectiveness of the algorithm by the largest value of k (depending on n and N) for which (5.8) is true.

II. Performance on classes K. We have introduced optimality and near optimality of an algorithm on a class K in §3. We will restrict our attention to the following sets K: the unit ball of the approximation space $\mathcal{A}^r((\Sigma_k), \ell_p)$; the unit ball of spaces ℓ_τ and weak ℓ_τ. We recall that the norm on $\mathcal{A}^r((\Sigma_k), \ell_p)$ is equivalent to the weak ℓ_τ norm, $1/\tau = r + 1/p$. As we have noted earlier, the optimal performance of sensing algorithms is determined by the Gelfand width of K. These widths are known for all

of the above classes (see Chapter 14 of [47], especially (5.1) and Notes 10.1 of that chapter). Since, the results are extensive, we mention only one result, for the case $p = 2$, which will orient the reader. For the unit ball $U(\ell_1)$ of ℓ_1 in $\mathbb{R}^N$, we have

$$C_1 \min(\sqrt{\frac{\log(eN/n)}{n}}, 1) \le E_n^*(U(\ell_1), \ell_2) \le C_2\sqrt{\frac{\log(eN/n)}{n}}, \qquad (5.9)$$

with absolute constants $C_1, C_2 > 0$. This is the result of Kashin improved (in the logarithm) by Gluskin. The appearance of the logarithm in (5.9) is the (small) price we pay in doing compressed sensing instead of sampling all coefficients and taking the n largest. We can use theoretical results like (5.9) to gauge the performance of any proposed algorithm.

III. Instance-optimal. Instead of asking for optimal performance on classes, we could ask that the sensing/decoding performs as well as k-term approximation on each $x \in \mathbb{R}^N$. If $\|\cdot\|_X$ is a norm on $\mathbb{R}^N$, we say the sensing encoder/decoder pair Φ/Δ is *instance-optimal* of order k if

$$E(x, \Phi, \Delta)_X \le C_0\sigma_k(x)_X, \quad x \in \mathbb{R}^N, \qquad (5.10)$$

holds for a constant independent of N and n. Given N and n, we want the largest value of k for which (5.10) holds. Since we are dealing with finite-dimensional spaces, the role of the constant C_0 is important.

In each case, some relevant issues are: (i) what are the properties of a matrix Φ that guarantee optimal or near optimal performance, (ii) which decoders work with Φ, (iii) what is the computational complexity of the decoding - how many computations are necessary to compute $\Delta(y)$ for a given y?

In [34], Donoho gave an algorithm which is optimal in the sense of II for $p = 2$ and for the unit ball of ℓ_τ, $\tau \le 1$ (hence it is universal for these sets). His approach had three main features. The first was to show that if a matrix Φ has three properties (called CS1-3), then Φ will be an optimal sensor for these classes. Secondly, he showed through probabilistic arguments that such matrices Φ exist. Finally, he showed that ℓ_1 minimization provides a near-optimal decoder for these classes. Independently Candès and Tao ([14], [15]) developed a similar theory. One of the advantages of their approach is that it is sufficient for Φ to satisfy only a version of the CS1 property and yet they obtain the same and in some cases improved results.

To describe the Candès–Tao results, we introduce the following notation. Given an $n \times N$ matrix Φ, and any set $T \subset \{1, \dots, N\}$, we denote by Φ_T the $n \times \#(T)$ matrix formed from these columns of Φ. We also use similar notation for the restriction x_T of a vector from $\mathbb{R}^N$ to T. The matrix Φ is said to have the *restricted isometry property* for k if there is a $0 < \delta_k < 1$ such that

$$(1 - \delta_k)\|x_T\|_{\ell_2} \le \|\Phi_T x_T\|_{\ell_2} \le (1 + \delta_k)\|x_T\|_{\ell_2} \qquad (5.11)$$

holds for all T of cardinality k.

Given the matrix Φ, and any $x \in \mathbb{R}^N$, the vector $y = \Phi(x)$ represents our information about x. As we have noted before, we need a decoding strategy for y. Both Candès–Romberg–Tao and Donoho suggest taking the element $\bar{x}$ that minimizes the ℓ_1 norm over all vectors which share the data y:

$$\bar{x} := \Delta(y) := \operatorname*{Arg\,min}_{z \in \mathcal{F}(y)} \|z\|_{\ell_1}. \tag{5.12}$$

Numerically, the decoding can be performed through linear programming. From our perspective, the main question is how well this encoding/decoding approximates x. The main result of [13] is that if

$$\delta_{3k} + 3\delta_{4k} < 2, \tag{5.13}$$

then

$$\|x - \bar{x}\|_{\ell_2} \le C \frac{\sigma_k(x)_{\ell_1}}{\sqrt{k}}. \tag{5.14}$$

Under the same conditions on Φ and k, the following variant of (5.14) was shown in [18]

$$\|x - \bar{x}\|_{\ell_1} \le C \sigma_k(x)_{\ell_1}. \tag{5.15}$$

By interpolation inequalities, we obtain for $1 \le p \le 2$

$$\|x - \bar{x}\|_{\ell_p} \le C \frac{\sigma_k(x)_{\ell_1}}{k^{1-1/p}}. \tag{5.16}$$

In all these inequalities, we can take C as an absolute constant once we have strict inequality in (5.13).

Before interpreting these results, let us first address the question of whether we have matrices Φ that satisfy (5.13). This is where randomness enters the picture. Consider an $n \times N$ matrix Φ whose entries are independent realizations of the Gaussian distribution with mean 0 and variance 1. Then, with high probability, the matrix Φ will satisfy (5.13) for any $k \le C_0 n / \log(N/n)$. Similar results hold if the Gaussian distribution is replaced by a Bernoulli distribution taking the values ± 1 with equal probability [2]. Here we have returned to Kashin who used such matrices in his solution of the n-width problems. Thus, there are many matrices that satisfy (5.13) and any of these can be used as sensing matrices. Unfortunately, this probabilistic formulation does not give us a vehicle for putting our hands on one with absolute certainty. This leads to the very intriguing question of concrete constructions of good sensing matrices.

Let us now return to our three formulations of optimality.

Exact reproduction of k sparse signals (Case I). If we have a matrix Φ that satisfies (5.11) and (5.13) in hand then the above encoding/decoding strategy gives an optimal solution to the Sensing Problem for the class of k-sparse signals: any signal with support k will be exactly captured by $\Delta(\Phi(x))$. Indeed, in this case $\sigma_k(x)_{\ell_1} = 0$

and therefore this follows from (5.14). Thus, for any $k \le Cn\log(N/n)$, there is a matrix Φ and a decoder Δ given by (5.12) that is optimal for the class of k sparse signals under this restriction on k. However, in this case the range of k is not optimal (the logarithm can be eliminated) as can easily be seen and was pointed out in [3]. For any k, we can create a matrix Φ of size $2k \times N$ that has the exact reproduction property of k sparse signals. For example, for $k = 1$, any two linear functionals $\sum_{i=1}^N q^i x_i$ with two distinct numbers q will have enough information to recover a one-sparse signal exactly.

The key to proving optimality of k-sparse signals is to prove that the null space $\mathcal{N}$ of Φ has no nonzero vector with support $\le 2k$. This is an algebraic property of Φ. Any matrix with this property will solve the optimality for k-sparse vectors. Such matrices are readily seen to exist. For any k and $N \ge 2k$, we can find a set Λ_N of N vectors in $\mathbb{R}^{2k}$ such that any $2k$ of them are linearly independent. The matrix Φ whose columns are the vectors in Λ_N will have the exact reproduction property. There are many examples of such sets Λ_N. For example, if $x_1 < x_2 < \cdots < x_N$ are arbitrary real numbers, then we can take the vectors $v_j \in \mathbb{R}^n$ whose entries are x_j^{i-1}, $i = 1, \dots, n$, which gives a van der Monde matrix. Such matrices are unfortunately very unstable in computation and cannot be used for the other sensing problems.

Optimality for classes K (Case II). To go further and discuss what happens in the case that x is not k-sparse, we assume first that $p = 2$, i.e., we measure error in ℓ_2. From our discussion of the existence of matrices Φ that satisfy (5.11),(5.13), we see that we can take $k = Cn/\log(N/n)$ in (5.14). Since $\sigma_k(x)_{\ell_1} \le \|x\|_{\ell_1}$, we obtain optimality on the class $U(\ell_1)$ (see (5.9)). The inequality (5.16) can be used to obtain similar results for approximation in ℓ_p.

Instance-optimal (Case III). If $\|\cdot\|_X$ is any norm on $\mathbb{R}^N$ and Φ is an $n \times N$ matrix, we say Φ has the *null space property* (NSP) for X of order k if for each $\eta \in \mathcal{N} = \mathcal{N}(\Phi)$,

$$\|\eta\|_X \le C_0 \|\eta_{T^c}\|_X, \quad \#(T) = k, \tag{5.17}$$

where T^c is the complement of T in $\{1, \dots, N\}$ and where $C_0 \ge 1$ is a fixed constant. A sufficient condition for Φ to have a decoder Δ such that the pair Φ/Δ is instance-optimal of order k is that $\mathcal{N}$ have the NSP for X of order $2k$ and a necessary condition is that $\mathcal{N}$ have the NSP for X of order k (see [18]).

In view of (5.15), the probabilistic constructions give instance-optimal sensing for $X = \ell_1$ and $k \le Cn/\log(N/n)$. On the other hand, it can be shown (see [18]) that any matrix which has the null space property for $k = 1$ in ℓ_2 will necessarily have $n \ge N/C_0^2$ rows. This means that in order to have instance-optimal for one sparse vectors in ℓ_2 requires the matrix Φ to have $O(N)$ rows. Therefore, instance-optimal is not a viable possibility for ℓ_2. For ℓ_p, $1 < p < 2$, there are intermediate results where the conditions on k relative to N, n are less severe (see [18]).

One final note about the discrete compressed sensing problem. We have taken as our signal classes the approximation spaces $\mathcal{A}^r$ which are defined by k-term approximation using the canonical basis for $\mathbb{R}^n$. In actuality the probabilistic construction

of sensing matrices works for sparsity measured by approximation using much more general bases. All we need is that the matrix representation of Φ with respect to the new basis also have properties (5.11), (5.13). Thus, the choice of a random sensing matrix Φ will encode sparsity simultaneously in many (most) bases. However, the decoding has to be done relative to the chosen basis. This is sometimes referred to as a universal property of the randomly constructed matrices Φ (see [2] for a more precise discussion of universality).

5.2. Computational issues. Notice that in compressed sensing, we have reduced greatly the number of samples n we need from the signal when compared with thresholding techniques. However, this was at the cost of severely complicating the decoding operator. The decoding by ℓ_1 minimization generally requires polynomial in N machine operations which may be prohibitive in some settings when N is large. Issues of this type are a major concern in Theoretical Computer Science (TCE) and some of the work in TCE relates to the sensing problem. For example, there has been a fairly long standing program in TCE , going back to the seminal work of Alon, Matias and Szegedy [1], to efficiently sketch large data sets (see also Henzinger, Raghavan and Rajaopalan [41]). The emphasis has been to treat streaming data with efficient computation measured not only by the number of computations but also the space required in algorithms. Streaming algorithms call for different encoders. The sensing matrix Φ needs to be constructed in a small amount of time. So their constructions typically use less randomness and sometimes are possible using coding techniques such Kerdoch codes or, more generally, Reed–Muller codes.

In some settings, the flavor of the results is also different. Rather than construct one sensing matrix Φ, one deals with a stochastic family $\Phi(\omega)$ of $n \times N$ matrices with ω taking values in some probability space Ω. An algorithm proceeds as follows. Given x, one takes a draw of an $\omega \in \Omega$ according to the probability distribution on Ω (this draw is made independent of any knowledge of x). The information recorded about x is then $\Phi(\omega)x$. There is a decoder $\Delta(\omega)$ which when applied to the information $\Phi(\omega)x$ produces the approximation $x(\omega) := \Delta(\omega)\Phi(\omega)$.

Changing the problem by demanding only good approximation in probability rather than with certainty allows for much improvement in numerical performance of decoding in the algorithm (see [36], [37], [38]). For example, in some constructions the decoding can be done using greedy algorithms with $P(n \log N)$ operations where P is a polynomial. This is a distinct advantage over decoding by ℓ_1 minimization when n is small and N is large. Also, now the spectrum of positive results also improves. For example, when calling for deterministic bounds on the error, we saw that instance-optimal in ℓ_2 is not possible (even for one-term sparsity) without requiring $n \geq c_0 N$. In this new setting, we can obtain instance-optimal performance for k with high probability even in ℓ_2 (see [18] and [24]).

6. The learning problem

This problem differs from the Data Fitting Problem in that our measurements are noisy. We shall assume that $X = [0, 1]^d$ (for simplicity) and that $Y \subset [-M, M]$. This assumption implies that f_ρ also takes values in $[-M, M]$. The measure ρ factors as the product

$$d\rho(x, y) = d\rho_X(x, y)d\rho(y|x) \tag{6.1}$$

of the marginal ρ_X and the conditional $\rho(y|x)$ measures.

Let $Z := X \times Y$. Given the data $z \in Z^n$, the problem is to find a good approximation f_z to f_ρ. We shall call a mapping $\boldsymbol{E}_n$ that associates to each $z \in Z^n$ a function f_z defined on X to be an *estimator*. By an *algorithm*, we shall mean a family of estimators $\{\boldsymbol{E}_n\}_{n=1}^\infty$. To evaluate the performance of estimators or algorithms, we must first decide how to measure the error in the approximation of f_ρ by f_z. The typical candidates to measure error are the $L_p(X, \rho_X)$ norms:

$$\|g\|_{L_p(X,\rho_X)} := \begin{cases} \left(\int_X |g(x)|^p d\rho_X\right)^{1/p}, & 1 \le p < \infty, \\ \operatorname*{esssup}_{x\in X} |g(x)|, & p = \infty. \end{cases} \tag{6.2}$$

Other standard choices in the statistical literature correspond to taking measures other than ρ_X in the L_p norm, for instance the Lebesgue measure. We shall limit our discussion to the $L_2(X, \rho_X)$ norm which we shall simply denote by $\|\cdot\|$. This is the most common and natural measurement for the error. Note that since we do not know ρ, we do not know this norm precisely. However, this will not prevent us from obtaining estimates relative to this norm.

The error $\|f_z - f_\rho\|$ depends on z and therefore has a stochastic nature. As a result, it is generally not possible to say anything about this error for a fixed z. Instead, we can look at behavior in probability as measured by

$$\rho^n\{z : \|f_\rho - f_z\| > \eta\}, \quad \eta > 0, \tag{6.3}$$

or in expectation

$$E_{\rho^n}(\|f_\rho - f_z\|) = \int_{Z^n} \|f_\rho - f_z\| \, d\rho^n, \tag{6.4}$$

where the expectation is taken over all realizations z obtained for a fixed n and ρ^n is the n-fold tensor product of ρ.

We can define optimal, near optimal, and universal algorithms as in §3. The starting point of course are the compact classes $K \subset L_2(X, \rho_X)$. For each such compact set K, we have the set $\mathcal{M}(K)$ of all Borel measures ρ on Z such that $f_\rho \in K$. There are two notions depending on whether we measure performance in expectation or probability. We enter into a competition over all estimators $\boldsymbol{E}_n : z \to f_z$ and define

$$e_n(K) := \inf_{\boldsymbol{E}_n} \sup_{\rho\in\mathcal{M}(K)} E_{\rho^n}(\|f_\rho - f_z\|_{L_2(X,\rho_X)}), \tag{6.5}$$

and

$$\boldsymbol{AC}_n(K,\eta) := \inf_{\boldsymbol{E}_n} \sup_{\rho\in\mathcal{M}(K)} \rho^n\{z : \|f_\rho - f_z\| > \eta\}. \tag{6.6}$$

As emphasized by Cucker and Smale [25] estimates in probability are to be preferred since they automatically imply estimates in expectation (by integrating with respect to $d\rho^n$). However, for the sake of simplicity of this presentation, most of our remarks will center around estimates in expectation.

Since we do not know the measure ρ_X, the compact subsets K of $L_2(X, \rho_X)$ are also not completely known to us. One way around this is to consider only compact subsets of $C(X)$ since these will automatically be compact in $L_2(X, \rho_X)$. Thus, classical spaces such as Sobolev and Besov classes which embed compactly into $C(X)$ are candidates for our analysis. A second, more robust, approach, is to consider the compact sets defined by an approximation process as described in §3.

The problem of understanding optimal performance on a compact set $K \subset L_2(X, \rho_X)$ takes a different turn from the analysis in our other estimation problems because the stochastic nature of the problem will prevent us from approximating f_ρ to accuracy comparable to best approximation on classes. This means that understanding optimality requires the establishment of both lower and upper bounds on convergence rates. There are standard techniques in statistics based on Kullback–Leibler information and Fano inequalities for establishing such lower bounds. In [28] a lower bound for the performance of an algorithm on K was established using a slight modification of Kolmogorov entropy. This result can be used to show that whenever K is a finite ball in a classical Besov or Sobolev class of smoothness order s which compactly embed into $C(X)$, then the optimal performance attainable by any algorithm is

$$e_n(K) \geq c(K)n^{-\frac{s}{2s+d}}, \quad n = 1, 2, \ldots. \tag{6.7}$$

An algorithm $(\boldsymbol{E}_n)$ is near optimal in expectation on the class K if for data z of size n, the functions f_z produced by the estimator $\boldsymbol{E}_n$ satisfy

$$E_{\rho^n}(\|f_\rho - f_z\|) \leq C(K)e_n(K), \tag{6.8}$$

whenever $f_\rho \in K$. It is often the case that estimation algorithms may miss near optimal performance because of a $\log n$ factor. We shall call such algorithms *quasi-optimal*.

There are various techniques for establishing upper bounds comparable to the best lower bounds. On a very theoretical level, there are the results of Birgé and Massart [10] which use ϵ nets for Kolmogorov entropy to establish upper bounds. While these results do not lead to practical algorithms, they do show that optimal performance is possible. Practical algorithms are constructed based on specific methods of linear or nonlinear approximation. The book [40] gives an excellent accounting of the state of the art in this regard (see Theorems 11.3 and 13.2). Let us point out the general approach and indicate some of the nuances that arise.

Suppose that we have chosen a sequence (Σ_m) of spaces Σ_m (linear or nonlinear of dimension m) to be used for the approximation of f_ρ from our given data z. How should we define our approximation? Since all that we have available to us is the data z, the natural choice for an approximation from Σ_m is the minimizer of the empirical risk

$$f_{z,\Sigma_m} := \operatorname*{Argmin}_{f\in\Sigma_m} \mathcal{E}_z(f), \quad \text{with } \mathcal{E}_z(f) := \frac{1}{n}\sum_{j=1}^{n}(y_j - f(x_j))^2. \tag{6.9}$$

In other words, f_{z,Σ_m} is the best approximation to $(y_j)_{j=1}^n$ from Σ_m in the empirical norm

$$\|g\|_z^2 := \frac{1}{n}\sum_{j=1}^{n}|g(x_j)|^2. \tag{6.10}$$

A key issue is how should we choose the dimension m. Choosing m too large results in fitting the noise (to be avoided) while choosing m too small reduces the approximation effectiveness. If we knew that f_ρ was in the approximation class $\mathcal{A}^s((\Sigma_m), L_2(X,\rho_X))$ then a choice $m \approx \left(\frac{n}{\log n}\right)^{\frac{1}{2s+1}}$ would result in an algorithm that is quasi-optimal on the class. However, we do not know s and so we need a method to get around this. The common approach is what is called model selection.

Model selection automatically chooses a good value of m (depending on z) by introducing a penalty term. For each $m = 1, 2, \ldots, n$, we have the corresponding function f_{z,Σ_m} defined by (6.9) and the empirical error

$$E_{m,z} := \frac{1}{n}\sum_{j=1}^{n}(y_j - f_{z,\Sigma_m}(x_j))^2. \tag{6.11}$$

Notice that $E_{m,z}$ is a computable quantity. In complexity regularization, one typically chooses a value of m by

$$m^* := m^*(z) := \operatorname*{Argmin}_{1\le m\le n}\left[E_{m,z} + \frac{\kappa m\log n}{n}\right], \tag{6.12}$$

with the parameter κ to be chosen (it will govern the range of s that is allowed). Then, one defines the estimator

$$\hat{f}_z := f_{z,\Sigma_{m^*}}. \tag{6.13}$$

Here is an important remark. One does not use $\hat{f}_z$ directly as the estimator of f_ρ since it is difficult to give good estimates for its performance. The main difficulty is that this function may be large even though we know that $|f_\rho| \le M$. Given this knowledge about f_ρ, it makes sense to post-truncate $\hat{f}_z$ and this turns out to be crucial in practice. For this, we define the truncation operator

$$T_M(x) := \min(|x|, M)\operatorname{sign}(x) \tag{6.14}$$

for any real number x and define

$$f_z := T_M(\hat{f}_z) \tag{6.15}$$

as our estimator to f_ρ.

One can show that under quite general conditions, the estimator (6.15) is quasi-optimal on the approximation classes $\mathcal{A}^s((\Sigma_m), L_2(X, \rho_X))$. The question arises as to which approximation process (Σ_m) should be employed. We mention some of the main issues in making this choice. First note that each approximation scheme has its own approximation classes. Without any additional knowledge about f_ρ there is from the viewpoint of approximation rates no obvious preference of one approximation process over another except that nonlinear methods are preferable to linear methods since the resulting approximation classes for nonlinear methods are larger.

A major issue, especially in implementing nonlinear methods, is computational cost. The larger the nonlinear process (e.g. the larger the dictionary in n-term approximation), then the more computation needed for minimization in the model selection (6.12). This factor is one of the major concerns in choosing the approximation scheme. It is especially critical for high space dimension d. We mention a couple of methods that can address these computational issues and relate to the methods of approximation introduced in this lecture.

Suppose we use a dictionary $\mathcal{D}$ of size n^a and employ model selection. This would require examining all m dimensional subspaces formed by elements of the dictionary for each $m = 1, 2, \ldots, n$. While the number of computations can possibly be reduced by using the fact that the data size is n, it will still involve solving $O(2^n)$ such least squares problems. This computation can be reduced considerably by using greedy algorithms. Through such an algorithm, we can find, with the evaluation of $O(n^{a+1})$ inner products, the greedy sequence $v_1, \ldots, v_n$ of the dictionary that provides near optimal empirical approximation with respect to the approximation classes described in our discussion of greedy algorithms (see [5]). We can then do model selection over the n subspaces $V_m := \text{span}\{v_1, \ldots, v_m\}$, $m = 1, \ldots, n$, to find the approximation f_z. Thus, the model selection is done over n, rather than $O(2^n)$, subspaces, after the implementation of the greedy algorithm. The price we pay for this increased efficiency is that the approximation classes for greedy algorithms are in general smaller than those for m-term approximation. This means that in general we may be losing approximation efficiency.

Another setting in which a model selection based on n-term approximation can be improved is in the use of adaptive approximation as described in §4. Here, one takes advantage of the tree structure of such adaptive methods. For a given data set z of size n, one associates to each node of the master tree T^* the empirical least squares error on the cell associated to the node. There are fast algorithms known as CART algorithms (see [33]) for assimilating the local errors and pruning the master tree to implement model selection. Another alternative put forward in [6] is to utilize empirical thresholding in a very similar fashion to wavelet tree approximation. Another advantage of adaptive algorithms is that they can be implemented on-line.

Adding one or several new data points does not require re-solving the entire empirical minimization problem but only to do tree updates. Moreover, in some cases, the analysis of adaptive algorithms can be made in probability.

7. Concluding remarks

Because of space limitations, we were only able to discuss the Sensing Problem and the Learning Problem in any detail. We will make a few brief remarks to direct the reader interested in some of the other problems.

The Data Fitting Problem is a special case of the optimal recovery problem. An excellent resource for results on optimal recovery is the survey [52] and the articles referenced in that survey. This problem, as well as aspects of the sensing problem, are also treated in the wealthy literature in Information Based Complexity (see [57] and [58] for a start) where the approach is very similar to our discussion of optimality.

The encoding problem is a main consideration in image processing and information theory. Our approach of deterministic model classes is in contrast to the usual stochastic models used in information theory. While stochastic models still dominate this field, there are a growing number of treatments addressing the image compression problem from the deterministic viewpoint. Optimal algorithms for Besov and Sobolev classes for the encoding problem can be obtained by employing wavelet thresholding and quantization (see [17]). More advanced methods of image compression model images by approximation classes based on other forms of approximation such as curvelets [11] and wedgeprints [55].

The computation problem is the most dominant area of numerical analysis. The most advanced and satisfying theory appears in the solution of elliptic equations with error measured in the energy norm. For model classes described by linear approximation (for example, classical Finite Element Methods based on piecewise polynomial approximations on fixed partitions), the Galerkin solutions relative to these spaces provide optimal algorithms. Much less is known for nonlinear methods. For model classes based on wavelet tree approximation, near optimal algorithms (in terms of total number of computations) have been given in [19], [20], [21]. For adaptive finite element methods, similar results have been given for simple model problems (the Poisson problem) in [7] by building on the results in [35], [53].

References

[1] Alon, N., Matias, Y., and Szegedy, M., The space complexity of approximating the frequency moments. In *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing* (Philadelphia, PA, 1996), ACM, New York 1996, 20–29.

[2] Baraniuk, R., Davenport, M., DeVore, R., and Wakin, M., The Johnson-Lindenstrauss lemma meets compressed sensing. Preprint

[3] Baron, D., Wakin, M., Duarte, M., Sarvotham, S., and Baraniuk, R., Distributed Compressed Sensing. Preprint.

[4] Baron, D., Universal approximation bounds for superposition of n sigmoidal functions. *IEEE Trans. Inform. Theory* **39** (1993), 930–945

[5] Barron, A., Cohen, A., Dahmen, W., and DeVore, R., Approximation and learning by greedy algorithms. Preprint.

[6] Binev, P., Cohen, A., Dahmen, W., and Temlyakov, V., Universal Algorithms for Learning Theory Part I: piecewise constant functions. *J. Mach. Learn. Res.* **6** (2005), 1297–1321.

[7] Binev, P., Dahmen, W., and DeVore, R., Adaptive Finite Element Methods with Convergence Rates. *Numer. Math.* **97** (2004), 219–268.

[8] Binev, P., Dahmen, W., DeVore, R., and Petrushev, P., Approximation Classes for Adaptive Methods. *Serdica Math. J.* **28** (2002), 391–416.

[9] Binev, P., and DeVore, R., Fast Computation in Adaptive Tree Approximation. *Numer. Math.* **97** (2004), 193–217.

[10] Birgé, L., and Massart, P., Rates of convergence for minimum contrast estimators. *Probab. Theory Related Fields* **97** (1993), 113–150.

[11] Candès, E. J., and Donoho, D. L., Continuous Curvelet Transform: I. Resolution of the Wavefront Set. *Appl. Comput. Harmon. Anal.* **19** (2005), 162–197.

[12] Candès, E. J., Romberg, J., and Tao, T., Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information. *IEEE Trans. Inform. Theory* **52** (2006), 489–509.

[13] Candès, E., Romberg, J., and Tao, T., Stable signal recovery from incomplete and inaccurate measurements. *Comm. Pure and Appl. Math.* **59** (2006), 1207–1223.

[14] Candès, E., and Tao, T., Decoding by linear programing. *IEEE Trans. Inform. Theory* **51** (2005), 4203–4215.

[15] Candès, E., and Tao, T., Near optimal signal recovery from random projections: universal encoding strategies? *IEEE Trans. Inform. Theory*, to appear.

[16] Cohen, A., *Numerical Analysis of Wavelet Methods*. Stud. Math. Appl. 32, North Holland, Amsterdam 2003.

[17] Cohen, A., Dahmen, W., Daubechies, I., and DeVore, R., Tree approximation and encoding. *Appl. Comput. Harmon. Anal.* **11** (2001), 192–226.

[18] Cohen, A., Dahmen, W., and DeVore, R., Compressed sensing and k-term approximation. In preparation.

[19] Cohen, A., Dahmen, W., DeVore, R., Adaptive wavelet methods for elliptic operator equations: convergence rates. *Math. Comp.* **70** (2001), 27–75.

[20] Cohen, A., W. Dahmen, DeVore, R., Adaptive wavelet methods II. Beyond the elliptic case. *Found. Comput. Math.* **2** (2002), 203-245.

[21] Cohen, A., Dahmen, W., and DeVore, R., Adaptive Wavelet Schemes for Nonlinear Variational Problems. *SIAM J. Numer. Anal.* **41** (2003), 1785–1823.

[22] Cohen, A., Daubechies, I., and Feauveau, J. C., Biorthogonal bases of compactly supported wavelets. *Comm. Pure Appl. Math.* **45** (1992), 485–560.

[23] Cohen, A., Daubechies, I., and Vial, P., Wavelets and fast transforms on an interval. *Appl. Comput. Harmon. Anal.* **1** (1993), 54–81.

[24] Cormode, G., and Muthukrishnan, S., Towards and algorithmic theory of compressed sensing. Technical Report 2005-25, DIMACS, 2005.

[25] Cucker, F., and Smale, S., On the mathematical foundations of learning theory. *Bull. Amer. Math. Soc.* **39** (2002), 1–49.

[26] Daubechies, I., Orthonormal bases of compactly supported wavelets. *Comm. Pure Appl. Math.* **41** (1988), 909–996.

[27] Daubechies, I., *Ten Lectures on Wavelets*. CBMS-NSF Regional Conf. Ser. in Appl. Math. 61, SIAM, Philadelphia 1992.

[28] DeVore, R., Kerkyacharian, G., Picard, D., and Temlyakov, V., Approximation Methods for Supervised Learning. *Found. Comput. Math.* **6** (2006),3–58.

[29] DeVore, R., and Temlyakov, V., Some remarks on greedy algorithms. *Adv. Comput. Math.* **5** (1996), 173–187.

[30] DeVore, R., Nonlinear approximation. *Acta Numer.* **7** (1998), 51–150.

[31] DeVore, R., and Lorentz, G. G., *Constructive Approximation*. Grundlehren Math. Wiss. 303, Springer-Verlag, Berlin, Heidelberg 1993.

[32] DeVore, R., and Yu, X.-M., Degree of adaptive approximation. *Math. Comp.* **55** (1990), 625–635.

[33] Donoho, D. L, CART and best-ortho-basis: a connection. *Ann. Statist.* **25** (1997), 1870–1911.

[34] Donoho, D., Compressed Sensing. *IEEE Trans. Inform. Theory* **52** (2006), 1289–1306.

[35] Dörfler, W., A convergent adaptive algorithm for Poisson's equation. *SIAM J. Numer. Anal.* **33** (1996), 1106–1124.

[36] Gilbert, A., Kotidis, Y., Muthukrishnan, S., and Strauss, M., How to summarize the universe: Dynamic maintenance of quantiles. *Proc. VLDB*, 2002, 454–465.

[37] Gilbert, A., Guha, S., Kotidis, Y., Indyk, P., Muthukrishnan, S., and Strauss, M., Fast, small space algorithm for approximate histogram maintenance. In *Proceedings of the thirty-fourth annual ACM symposium on the theory of computing*, ACM, New York 2002, 389–398.

[38] Gilbert, A., Guha, S., Indyk, P., Muthukrishnan, S., and Strauss, M., Near-optimal sparse Fourier estimation via sampling. *Proceedings of the thirty-fourth annual ACM symposium on the theory of computing*, ACM, New York 2002, 152–161.

[39] Goldreich, O., Levin, L., A hardcore predicate for one way functions. In *Proceedings of the twenty-first annual ACM Symposium on the Theory of Computing*, ACM, New York 1989, 25–32.

[40] Györfi, L., Kohler, M., Krzyzak, A., and Walk, H., *A Distribution -free Theory of Nonparametric Regression*. Springer Series in Statistics, Springer-Verlag, New York 2002.

[41] Henzinger, M., Raghavan, P., and Rajagopalan, S., Computing on data stream. Technical Note 1998-011, Digital systems research center, Palo Alto, May 1998.

[42] Jones, L. K., A simple lemma on greedy approximation in Hilbert spaces and convergence rates for projection pursuit regression and neural network training. *Ann. Statist.* **20** (1992), 608–613.

[43] Johnson, W., and Lindenstrauss, J., Extensions of Lipschitz maps into Hilbert space. *Contemp. Math.* **26** (1984), 189–206.

[44] Kashin, B., The widths of certain finite dimensional sets and classes of smooth functions. *Izv. Akad. Nauk SSSR Ser. Mat.* **41** (1977), 334–351; English transl. *Math. USSR-Izv.* **11** (1978), 317–333.

[45] Kushilevitz, E., Mansour, Y., Learning decision trees using the Fourier spectrum. In *Proceedings of the twenty-third annual ACM symposium on the theory of computing*, ACM, New York 1991, 455–464; *SIAM J. Comput* **22** (1993), 1331–1348.

[46] Lee, W. S., Bartlett, P., and Williamson, R. C., Efficient agnostic learning of neural networks with bounded fan-in. *IEEE Trans. Inform. Theory* **42** (1996), 2118–2132.

[47] Lorentz, G. G., von Golitschek, M., and Makovoz, Yu.. *Constructive Approximation: Advanced Problems*. Grundlehren Math. Wiss. 304, Springer-Verlag, Berlin, Heidelberg 1996.

[48] Mallat, S., Multiresolution approximation and wavelet orthonormal bases of $L^2(\mathbb{R})$. *Trans. Amer. Math. Soc.* **315** (1989), 69–88.

[49] Mallat, S., *A Wavelet Tour of Signal Processing*. Academic Press, New York 1998.

[50] Meyer, Y., Ondelettes sur l'intervalle. *Rev. Mat. Iberoamer.* **7** (1991), 115–134.

[51] Meyer, Y., *Ondelettes et Opérateurs I*. Actualites Math., Hermann, Paris 1990 (English translation by D. H. Salinger, Cambridge Stud. Adv. Math. 37, Cambridge University Press, Cambridge 1992).

[52] Micchelli, C., and Rivlin, T., A survey of optimal recovery. In *Optimal Estimation in Approximation Theory* (C. A. Micchelli and T. J. Rivlin, eds.), Plenum Press, New York 1977, 1–54.

[53] Morin, P., Nochetto, R., and Siebert, K., Data Oscillation and convergence of adaptive FEM. *SIAM J. Numer. Anal.* **38** (2000), 466–488.

[54] Pinkus, A., *n-Widths in Approximation Theory*. Ergeb. Math. Grenzgeb. 7, Springer-Verlag, Berlin 1985.

[55] Romberg, J., M. Wakin, R. Baraniuk, Approximation and Compression of Piecewise Smooth Images Using a Wavelet/Wedgelet Geometric Model. IEEE International Conference on Image Processing, Barcelona, Spain, September 2003.

[56] Temlyakov, V., Nonlinear Methods of Approximation. *Found. Comput. Math.* **3** (2003), 33–107.

[57] Traub, J., and Wozniakowski, H., *A General Theory of Optimal Algorithms*. Academic Press, New York, NY, 1980.

[58] Traub, J. F., Wasilkowski, G. W., and Woźniakowski, H., *Information-Based Complexity*. Academic Press, New York, NY, 1988.

Department of Mathematics, University of South Carolina, Columbia, SC 29208, U.S.A.
E-mail: devore@math.sc.edu

Symplectic field theory and its applications

Yakov Eliashberg*

Abstract. Symplectic field theory (SFT) attempts to approach the theory of holomorphic curves in symplectic manifolds (also called Gromov-Witten theory) in the spirit of a topological field theory. This naturally leads to new algebraic structures which seems to have interesting applications and connections not only in symplectic geometry but also in other areas of mathematics, e.g. topology and integrable PDE. In this talk we sketch out the formal algebraic structure of SFT and discuss some current work towards its applications.

Mathematics Subject Classification (2000). Primary 53D40; Secondary 53D45.

Keywords. Symplectic and contact manifolds, J-holomorphic curves, Gromov–Witten invariants, symplectic field theory.

1. Formal algebraic structure of SFT

The project of SFT was initiated by A. Givental, H. Hofer and the author in [15]. Since its inception, it has branched in different directions and now involves a large number of authors working on the foundation and the different parts of the project. SFT is closely related to the *relative Gromov–Witten theory*, see e.g. [21], [30], [35], [34], [31], as well the work of Yu. Chekanov [11] and Fukaya–Oh–Ohta–Ono project [20].

Symplectic field theory can be viewed as a functor SFT from a geometric category GEOM_{SFT} of framed Hamiltonian structures and framed cobordisms between them to an algebraic category ALG_{SFT} of certain differential D-modules and Fourier integral operators between them. We describe these categories in the next two sections.

1.1. The category $\mathbf{ALG}_{SFT}$. Roughly speaking, the objects in the category ALG_{SFT} are certain D-modules over a graded Weyl algebra with an operator $\mathbb{H}$ which satisfies the "master equation" $\mathbb{H} \circ \mathbb{H} = 0$. Before listing the algebraic structures involved, let us make a couple of general remarks. First, we will be dealing in this paper with graded objects. To simplify the exposition we will usually mean by grading a $\mathbb{Z}/2$-grading, unless it is noted otherwise. Usually, with extra work it can be upgraded to an integer grading. Second, we will systematically use $\mathbb{C}$ as the coefficient ring. In some situations it has to be changed to a certain Novikov ring, see Remark 2.1 below.

*Partially supported by NSF grants DMS-0204603 and DMS-0244663.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

Given an integer vector $\boldsymbol{d} = (d_1, \dots, d_N)$ let us denote by $\mathsf{CT}_{\boldsymbol{d}} = \mathbb{C}[T]$ a $\mathbb{Z}$-graded (super-)commutative algebra with complex coefficients, generated by graded elements of an infinite $N \times \infty$ matrix $T = (t_{ij}), i = 1, \dots, N,\ j = 0, \dots$; the $\mathbb{Z}/2$-grading of t_{ij} coincides with the parity of d_i for each $j \geq 0$ and $i = 1, \dots, N$.

An *object* in the category ALG_{SFT} is a collection of the following structures O1–O5, which satisfy axioms AO1 and AO2.

O1. A possibly infinite-dimensional space $\mathcal{P}$ with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ and a fixed basis Γ. To simplify the notation we will assume that there exists an involution $\gamma \mapsto \bar{\gamma}$, $\gamma \in \Gamma$, such that $\langle \gamma, \gamma' \rangle = \delta_{\bar{\gamma}\gamma'}$, $\gamma, \gamma' \in \Gamma$.

O2. A $\mathbb{Z}$-graded, possibly infinite-dimensional vector space $\mathbb{V} = \oplus_j \mathbb{V}_j$ over $\mathbb{C}$, called the *phase space*, with a degree 1 differential $d : \mathbb{V} \to \mathbb{V}$, such that $d^2 = 0$ (e.g. a space of differential forms on a manifold with de Rham differential d). For $\boldsymbol{d} = (d_1, \dots, d_N)$ we denote by $V^{\boldsymbol{d}}$ the space $\oplus_i^N \mathbb{V}_{d_i}$.

O3. An associative algebra $\widetilde{\mathsf{W}}$ over $\mathbb{C}$ generated by graded elements $p_{k,\gamma}$, $q_{k,\gamma}$, $\gamma \in \Gamma$, $k \geq 1$, and an even graded element $\hbar$, with the following commutation relations: all elements commute (in the graded sense) except that the (graded) commutator $[p_{k,\gamma}, q_{k,\bar{\gamma}}]$ equals $k\hbar$ for any $\gamma \in \Gamma$ and $k \geq 1$.

O4. A completion W of $\widetilde{\mathsf{W}}$, called the *Weyl algebra*, which consists of formal power series of $\hbar$ and p-variables with coefficients which are polynomials of q-variables.

O5. A smooth function $\mathbb{H} \colon \mathbb{V}^{\boldsymbol{d}} \to \frac{1}{\hbar}\mathsf{W} \otimes \mathsf{CT}_{\boldsymbol{d}}$, which associates with any $\Theta = (\theta_1, \dots, \theta_N) \in \mathbb{V}^{\boldsymbol{d}}$ an odd (in fact, of degree 1 if the integer grading is used) element $\mathbb{H}\langle\Theta\rangle \in \frac{1}{\hbar}\mathsf{W} \otimes \mathsf{CT}_{\boldsymbol{d}}$, called the *Hamiltonian*. Here smoothness is understood in the formal sense: all coefficients of the corresponding power expansions are smooth.

Before formulating the axioms let us introduce some notation. Given two vectors $\boldsymbol{d} = (d_1, \dots, d_N)$ and $\boldsymbol{d}' = (d'_1, \dots, d'_{N'})$ we denote by $\boldsymbol{d} \sqcup \boldsymbol{d}'$ the vector $(d_1, \dots, d_N, d'_1, \dots, d'_{N'})$. Similarly, for $\Theta = (\theta_1, \dots, \theta_N) \in \mathbb{V}^{\boldsymbol{d}}$ and $\Theta' = (\theta'_1, \dots, \theta'_{N'}) \in \mathbb{V}^{\boldsymbol{d}'}$ we write

$$\Theta \sqcup \Theta' = (\theta_1, \dots, \theta_N, \theta'_1, \dots, \theta'_{N'}) \in \mathbb{V}^{\boldsymbol{d} \sqcup \boldsymbol{d}'}.$$

We will also denote by t_{ij} and t'_{kl}, $i = 1, \dots, N$, $k = 1, \dots, N'$, $j, l = 1 \dots$, the generators of the algebra $\mathsf{CT}_{\boldsymbol{d} \sqcup \boldsymbol{d}'}$, and by $\pi : \mathsf{CT}_{\boldsymbol{d} \sqcup \boldsymbol{d}'} \to \mathsf{CT}_{\boldsymbol{d}}$ the projection.

The following axioms should be satisfied:

AO1.

$$\mathbb{H}\langle \Theta \sqcup d\Theta \rangle \circ \mathbb{H}\langle \Theta \sqcup d\Theta \rangle = \partial \mathbb{H}\langle \Theta \sqcup d\Theta \rangle, \tag{1}$$

where

$$\partial = \sum_{i,j} t_{ij} \frac{\partial}{\partial t'_{ij}} \tag{2}$$

is an odd differential on $\mathsf{CT}_{\boldsymbol{d}\sqcup\boldsymbol{d}'}$, $\boldsymbol{d}' = (d_1 + 1, \dots, d_N + 1)$.

Note that $\partial^2 = 0$.

AO2.

$$\mathbb{H}\langle\Theta\rangle = \pi\left(\mathbb{H}\langle\Theta \sqcup 0\rangle\right), \tag{3}$$

for $\Theta \in \mathbb{V}^{\boldsymbol{d}}$ and $0 \in \mathbb{V}^{\boldsymbol{d}'}$.

Let us note an important corollary of the axioms. Suppose that $d\Theta = 0$. Then we have

$$\mathbb{H}\langle\Theta\rangle \circ \mathbb{H}\langle\Theta\rangle = 0. \tag{4}$$

Hence, if $d\Theta = 0$ then $\left(\mathsf{W} \otimes \mathsf{CT}^{\boldsymbol{d}}, \mathbb{D}\langle\Theta\rangle\right)$ is a differential Weyl algebra with a differential

$$\mathbb{D}\langle\Theta\rangle(x) = [\mathbb{H}\langle\Theta\rangle, x], \quad x \in \mathsf{W} \otimes \mathsf{CT}^{\boldsymbol{d}}.$$

More generally, for *any* $\Theta \in \mathbb{V}^{\boldsymbol{d}}$ we can define a differential Weyl algebra

$$\left(\mathsf{W} \otimes \mathsf{CT}^{\boldsymbol{d}\sqcup\boldsymbol{d}'}, \mathbb{D}\langle\Theta \sqcup d\Theta\rangle\right)$$

with a differential

$$\mathbb{D}\langle\Theta \sqcup d\Theta\rangle(x) = \partial x + [\mathbb{H}\langle\Theta\rangle, x], \quad x \in \mathsf{W} \otimes \mathsf{CT}^{\boldsymbol{d}\sqcup\boldsymbol{d}'}.$$

Let us also consider

- a space F of formal Fourier series

$$\sum_{k=1}^{\infty} P_k e^{ikx} + Q_k e^{-ikx}, \tag{5}$$

where $P_k = \{p_{k,\gamma}\}_{\gamma\in\Gamma}$, $Q_k = \{q_{k,\gamma}\}_{\gamma\in\Gamma}$, $k = 1, \dots,$ are ordered strings of graded variables, indexed by elements of Γ; the space F is canonically *polarized*, i.e. split $\mathsf{F} = \mathsf{F}_+ \oplus \mathsf{F}_-$, where F_+ (resp. F_-) is formed by Fourier series with only positive (resp. negative) coefficients;

- a space Fock which consists of formal series $\sum_{k\geq 0} f_k \hbar^k$, where f_k are functionals on the space F_- which can be expressed as polynomials of Fourier coefficients $q_{k,\gamma}$.

Note that the space Fock can be viewed as a D-module over $\frac{1}{\hbar}\mathsf{W}$. Indeed, the quantization

$$p_{k,\gamma} \mapsto k\hbar \frac{\partial}{\partial q_{k,\bar{\gamma}}}$$

provides a representation of $\frac{1}{\hbar}\mathsf{W}$ as the algebra of differential operators acting from the left on elements of the space Fock. Given an element $A \in \frac{1}{\hbar}\mathsf{W}$ we will denote by $\lfloor A \rfloor$ the corresponding differential operator if we need to distinguish it from A.

For each Θ with $d\Theta = 0$ the equation (4) implies that the operator $\mathbb{H}(\Theta)$ is a differential on $\mathsf{Fock} \otimes \mathsf{CT}_d$. Indeed, if we define

$$D_\Theta = \lfloor \mathbb{H}\langle\Theta\rangle \rfloor f, \quad f \in \mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}},$$

then $D_\Theta^2 = 0$.

Consider now two objects $\mathcal{O}^+, \mathcal{O}^- \in \mathrm{ALG}_{SFT}$. We will label with $\pm$ all the structures associated with these objects. *Morphisms* $\mathcal{O}^+ \to \mathcal{O}^-$ are formed by the following structures:

- A graded space $\mathbb{V} = \sum_j \mathbb{V}_j$ over $\mathbb{C}$ with a differential $d\colon \mathbb{V} \to \mathbb{V}$, $d^2 = 0$, and two grading-preserving *restriction homomorphisms* $R^\pm\colon \mathbb{V} \to \mathbb{V}^\pm$;

- A graded commutative algebra A_-^+ over $\mathbb{C}$ which consists of formal power series of $\hbar$ and p^+-variables whose coefficients are polynomials of q^--variables. Note that the Weyl algebra $\frac{1}{\hbar}\mathsf{W}^-$ acts on A_-^+ on the left by quantizing

$$p^-_{k,\gamma} \mapsto k\hbar \frac{\overrightarrow{\partial}}{\partial q^-_{k,\bar\gamma}}, \tag{6}$$

  while the Weyl algebra W^+ acts on A_-^+ on the right by quantizing

$$q^+_{k,\gamma} \mapsto k\hbar \frac{\overleftarrow{\partial}}{\partial p^+_{k,\bar\gamma}}; \tag{7}$$

  given an element $D \in \frac{1}{\hbar}\mathsf{W}^\pm$ we will denote by $\lfloor D \rfloor$ and $\lceil D \rceil$ its quantizations defined by formulas (6) and (7), respectively.

- A smooth function

$$\widehat{\mathbb{V}}^{\boldsymbol{d}} \to \frac{1}{\hbar}\mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}}$$

  which associates with a string $\Theta = (\theta_1, \dots, \theta_N) \in \widehat{\mathbb{V}}^{\boldsymbol{d}}$ an even (of degree 0 in the situation of $\mathbb{Z}$-grading) element

$$\boldsymbol{\Phi}\langle\Theta\rangle = \frac{1}{\hbar}\boldsymbol{\Phi}\langle\Theta\rangle(T, q^-, p^+, \hbar) \in \mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}},$$

  called the *potential*.

The following axioms should be satisfied:

AM1.

$$\lfloor \mathbb{H}^-\langle R^-(\Theta \sqcup d\Theta)\rangle \rfloor e^{\mathbf{\Phi}\langle \Theta \sqcup d\Theta\rangle} + e^{\mathbf{\Phi}\langle \Theta \sqcup d\Theta\rangle} \lceil \mathbb{H}^+\langle R^+(\Theta \sqcup d\Theta)\rangle \rceil = \partial e^{\mathbf{\Phi}\langle \Theta\rangle}, \tag{8}$$

where the linear differential operator $\partial = \sum_{i,j} t_{ij} \frac{\partial}{\partial t'_{ij}}$ is defined above in (2).

AM2.

$$\mathbf{\Phi}\langle \Theta\rangle = \pi\left(\mathbf{\Phi}\langle \Theta \sqcup 0\rangle\right), \tag{9}$$

where $\Theta \in \mathbb{V}^{\boldsymbol{d}}$, $0 \in \mathbb{V} \in \mathbb{V}^{\boldsymbol{d}'}$, and π is the projection $\mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d} \sqcup \boldsymbol{d}'} \to \mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}}$.

An important partial case is when $d\Theta = 0$. In this case the axioms imply

$$\lfloor \mathbb{H}^-\langle R^-(\Theta)\rangle \rfloor e^{\mathbf{\Phi}\langle \Theta\rangle} + e^{\mathbf{\Phi}\langle \Theta\rangle} \lceil \mathbb{H}^+\langle R^+(\Theta)\rangle \rceil = 0. \tag{10}$$

Note that $\mathbf{\Phi}$ defines for each Θ a formal Fourier integral operator

$$\widetilde{\Phi}\langle \Theta\rangle \colon \mathsf{Fock}_+ \otimes \mathsf{CT}_{\boldsymbol{d}} \to \mathsf{Fock}_- \otimes \mathsf{CT}_{\boldsymbol{d}}$$

by the formula

$$\widetilde{\Phi}\langle \Theta\rangle(f)(T, q^-, \hbar) = \left(e^{\frac{1}{\hbar}\mathbf{\Phi}\langle \Theta\rangle(T, q^-, p^+, \hbar)} \lceil f(T, q^+, \hbar) \rceil\right)\Big|_{p^+=0}. \tag{11}$$

If $d\Theta = 0$ then the equation (10) translates into the fact that

$$\widetilde{\Phi}\langle \Theta\rangle \colon \left(\mathsf{Fock}^+ \otimes \mathsf{CT}_{\boldsymbol{d}}, D_{R^+(\Theta)}\right) \to \left(\mathsf{Fock}^- \otimes \mathsf{CT}_{\boldsymbol{d}}, D_{R^-(\Theta)}\right)$$

is a *chain map*.

Suppose now that we are given three objects $\mathcal{O}_0$, $\mathcal{O}_1$ and $\mathcal{O}_2$, and morphisms $\mathbf{\Phi}_{01} \colon \mathcal{O}_0 \to \mathcal{O}_1$ and $\mathbf{\Phi}_{12} \colon \mathcal{O}_1 \to \mathcal{O}_2$. Then their composition $\mathbf{\Phi}_{02} \colon \mathcal{O}_0 \to \mathcal{O}_2$ is defined as follows. First, we define the phase space $\mathbb{V}_{02}$ as the fiber product

$$\mathbb{V}_{02} = \{(\theta_{01}, \theta_{12});\ \theta_{01} \in \mathbb{V}_{01}, \theta_{12} \in \mathbb{V}_{12},\ R^-_{01}(\theta_{01}) = R^+_{12}(\theta_{12})\}.$$

Given $\Theta_{02} = (\Theta_{01}, \Theta_{12}) \in \mathbb{V}_{02}^{\boldsymbol{d}}$ we define an element

$$\mathbf{\Phi}_{02}\langle \Theta_{02}\rangle = \frac{1}{\hbar}\Phi_{02}\langle \Theta_{02}\rangle(T, q_2, p_0, \hbar) \in \frac{1}{\hbar}\mathsf{A}_2^0$$

by the formula

$$\begin{aligned} e^{\frac{1}{\hbar}\mathbf{\Phi}_{02}\langle \Theta_{02}\rangle(T, q_2, p_0, \hbar)} &= \left(\lfloor e^{\frac{1}{\hbar}\mathbf{\Phi}_{12}\langle \Theta_{12}\rangle(T, q_2, p_1, \hbar)} \rfloor e^{\frac{1}{\hbar}\mathbf{\Phi}_{01}\langle \Theta_{01}\rangle(T, q_1, p_0, \hbar)}\right)\Big|_{q_1=0} \\ &= \left(e^{\frac{1}{\hbar}\mathbf{\Phi}_{12}\langle \Theta_{12}\rangle(T, q_2, p_1, \hbar)} \lceil e^{\frac{1}{\hbar}\mathbf{\Phi}_{01}\langle \Theta_{01}\rangle(T, q_1, p_0, \hbar)}\right) \rceil\Big|_{p_1=0}. \end{aligned} \tag{12}$$

Note that the corresponding operator $\widetilde{\Phi}_{02}(\Theta_{02})$ is the composition:

$$\widetilde{\Phi}_{02}\langle \Theta_{02}\rangle = \widetilde{\Phi}_{12}\langle \Theta_{12}\rangle \circ \widetilde{\Phi}_{01}\langle \Theta_{12}\rangle \colon \mathsf{Fock}_0 \otimes \mathsf{CT}_{\boldsymbol{d}} \to \mathsf{Fock}_2 \otimes \mathsf{CT}_{\boldsymbol{d}}.$$

1.2. The category $\mathbf{GEOM}_{SFT}$. The exposition in this section is essentially taken from Section 4.1 in [17]. A *Hamiltonian structure* is a pair (V, Ω), where V is an oriented manifold of dimension $2n-1$ endowed with a closed 2-form Ω of maximal rank ($= 2n-2$). The tangent line field $\ell = \operatorname{Ker}\Omega$ is called the *characteristic* line field. The field ℓ integrates to a 1-dimensional *characteristic foliation* of Ω. Note that Ω defines a fiber-wise symplectic structure (and hence an orientation) on the bundle TV/ℓ. Thus the line bundle ℓ is equipped with an orientation. We will call *characteristic* any vector field R which generates ℓ and respects its orientation.

Any co-orientable hypersurface V in a symplectic manifold $(W, \widetilde{\Omega})$ inherits a Hamiltonian structure $\widetilde{\Omega}|_V$. Conversely, any Hamiltonian structure (V, Ω) embeds as a hypersurface in a symplectic manifold $(V \times (-\varepsilon, \varepsilon), \widetilde{\Omega})$ where the form $\widetilde{\Omega}$ can be constructed as follows. Let λ be any 1-form which is not vanishing on ℓ, and s the coordinate along the second factor. Then we set $\widetilde{\Omega} = \Omega + d(s\lambda)$. Note that by Darboux's theorem the Hamiltonian structure (V, Ω) determines its symplectic extension to a neighborhood of the hypersurface $V = V \times 0 \subset V \times (-\varepsilon, \varepsilon)$ uniquely up to a diffeomorphism fixed on V. We call (a germ along V of) the symplectic structure $\widetilde{\Omega}$ on $V \times (-\varepsilon, \varepsilon)$ the *symplectic extension* of (V, Ω).

A Hamiltonian structure $\mathcal{H} = (V, \Omega)$ is called *stable* (see [24]) if its symplectic extension can be realized by a form $\widetilde{\Omega}$ on $V \times (-\varepsilon, \varepsilon)$ such that the Hamiltonian structures induced on hypersurfaces $V \times s, s \in (-\varepsilon, \varepsilon)$, all have the same characteristic line field ℓ. It is easy to check (see [17]) that

Proposition 1.1. *A Hamiltonian structure $\mathcal{H} = (V, \Omega)$ is stable if and only if there exists a 1-form λ and a characteristic vector field R such that*

$$\lambda(R) = 1 \quad \textit{and} \quad i_R d\lambda = 0. \tag{13}$$

Note that in view of Cartan's formula we have $L_R\lambda = d(\lambda(R)) + i_R d\lambda$, and hence the second condition can be restated as invariance of λ under the flow of R.

A *framing* of a stable Hamiltonian structure is a pair (λ, J) where

- λ is as in (13); the form λ automatically defines the hyperplane field $\xi = \{\lambda = 0\}$, called a *cut* of the Hamiltonian structure, and the vector field R, called its *Reeb* field;
- J is an almost complex structure on ξ (also called a CR-structure on V) compatible with the symplectic form Ω.

Here are three major examples of stable framed Hamiltonian structures.

Example 1.2. (1) *Contact forms.* Let ξ be a contact structure on V, i.e. a completely non-integrable tangent hyperplane field, and λ a contact form for ξ, i.e. $\xi = \{\lambda = 0\}$. Let an almost complex structure $J : \xi \to \xi$ be compatible with $d\lambda|_\xi$. Then $\mathcal{H} = (\Omega = d\lambda, \lambda, J)$ is a framed stable Hamiltonian structure on V with the cut ξ, and R is the usual Reeb field of the contact form λ. We say in this case that the Hamiltonian structure $\mathcal{H}$ is of *contact* type.

(2) *Hamiltonian functions.* Let (M, ω) be a symplectic manifold and $H_t : M \to \mathbb{R}$, $t \in S^1 = \mathbb{R}/\mathbb{Z}$, a 1-periodic time-dependent Hamiltonian function. Set $V = M \times S^1$, $\Omega = -\omega + H_t dt$ and $\lambda = dt$. Let J be an almost complex structure on M compatible with ω. Then $\mathcal{H} = (V, \Omega, \lambda, J)$ is a framed stable Hamiltonian structure. Its Reeb vector field is given by $R = \frac{\partial}{\partial t} + \text{sgrad } H_t$, where sgrad H_t is the Hamiltonian vector field defined by H_t. We say in this case that $\mathcal{H}$ is of *Floer* type.

(3) S^1*-bundles.* Let (M, ω) be a symplectic manifold and $p : V \to M$ any S^1-bundle over it. Set $\Omega = p^*\omega$. Then Ω is a stable Hamiltonian structure on V. Indeed, one can choose any S^1-connection form λ as its framing. The corresponding Reeb vector field R is the infinitesimal generator of the S^1-action, and the cut of ξ is formed by the horizontal spaces of the connection. Let J_M be an almost complex structure on M compatible with ω, and J be the pull-back of J_M to ξ via the projection $V \to M$. We say that a framed Hamiltonian structure $\mathcal{H} = (V, \Omega, \lambda, J)$ is of *fibration* type. Note that if the cohomology class $[\omega]$ of the symplectic form is integral, then one could take as V the corresponding *pre-quantization space* , i.e. the principal S^1-bundle $p : V \to M$ with the first Chern class $[\omega]$. In this case the lift $\Omega = p^*\omega$ of the symplectic form is exact and one can choose λ to be a primitive of Ω. Hence, in this case (V, Ω, λ, J) is also of contact type.

All Hamiltonian structures which we consider in this paper will be assumed stable.

Framed Hamiltonian structures are *objects in the category* GEOM_{SFT}, while morphisms are *framed symplectic cobordisms* which we describe below.

A *symplectic cobordism* between two Hamiltonian structures $\mathcal{H}_+ = (V_+, \Omega_+)$ and $\mathcal{H}_- = (V_-, \Omega_-)$ is a symplectic manifold (W, Ω) such that $\partial W = V_+ \cup (-V_-)$ and $\Omega|_{V_\pm} = \Omega_\pm$. Note that "symplectic cobordism" is a partial order, and not an equivalence relation, because it is not symmetric. A *framed* symplectic cobordism between two framed Hamiltonian structures $\vec{\mathcal{H}}_+ = (V_+, \Omega_+, \lambda_+, J_+)$ and $\vec{\mathcal{H}}_- = (V_-, \Omega_-, \lambda_-, J_-)$ is a cobordism (W, Ω) between $\mathcal{H}_+$ and $\mathcal{H}_-$ equipped with an almost complex structure J which is compatible with Ω, and such that $J(\xi_\pm) = \xi_\pm$; here $\xi_\pm$ denotes the cut $\{\lambda_\pm = 0\}$ of the framed Hamiltonian $\vec{\mathcal{H}}_\pm$. *Morphisms* in the category GEOM_{SFT} are *multi-storied framed symplectic cobordisms*, i.e. sequences $(C_{0,1}, C_{1,2}, \ldots, C_{k-1,k})$ where $C_{j-1,j} = (W_{j-1,j}, \Omega_{j-1,j}, J_{j-1,j})$ is a framed symplectic cobordism between framed Hamiltonian structures $\vec{\mathcal{H}}_{j-1}$ and $\vec{\mathcal{H}}_j$, $j = 1, \ldots, k$. An associative operation of composition of morphisms is defined in an obvious way as concatenation of such sequences.

1.3. 2-categories. Both categories, GEOM_{SFT} and ALG_{SFT}, can be upgraded to 2-categories which are respected by the functor *SFT*.

On the geometric side, a 2-morphism is a fixed on the boundary homotopy of symplectic cobordisms and their framings. More precisely, a 2-*morphism* is a pair (Ω_s, J_s), $s \in [0, 1]$, where Ω_s is a family of symplectic forms on a cobordism W

such that $\Omega_s|_{\partial W} = \Omega_0|_{\partial W}$, $\Omega_s = d\Xi_s$, $\Xi_s|_{\partial W} = 0$, $s \in [0, 1]$, and J_s is a fixed on ∂W deformation of almost complex structures compatible with Ω_s. The notion of homotopy can be extended to morphisms represented by multi-storied cobordisms via the process, called *splitting* or *stretching the neck*. We refer the reader to [15], [8] for the precise definition.

Let us move now to the algebraic side of the story. Let $\mathbf{\Phi}^{(0)}, \mathbf{\Phi}^{(1)} \colon \mathcal{O}^+ \to \mathcal{O}^-$ be two morphisms, where for $\Theta \in \mathbb{V}^{\boldsymbol{d}}$. We have

$$\mathbf{\Phi}^{(s)}(\Theta) = \frac{1}{\hbar}\Phi^{(s)}\langle\Theta\rangle(T, q^-, p^+, \hbar) \in \frac{1}{\hbar}\mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}}, \quad s = 0, 1.$$

A 2-*morphism* between $\mathbf{\Phi}^{(0)}, \mathbf{\Phi}^{(1)}$ is a function which associates with $\Theta \in \mathbb{V}^{\boldsymbol{d}}$ a family

$$\boldsymbol{K}^{(s)}\langle\Theta\rangle = \frac{1}{\hbar}\boldsymbol{K}^{(s)}\langle\Theta\rangle(T, q^-, p^+, \hbar) \in \frac{1}{\hbar}\mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}}, \quad s \in [0, 1].$$

When $d\Theta = 0$ then $\boldsymbol{K}^{(s)}$ generates a homotopy $\mathbf{\Phi}^{(s)} = \frac{1}{\hbar}\mathbf{\Phi}^{(s)}\langle\Theta\rangle(T, q^-, p^+, \hbar)$, $s \in [0, 1]$, defined by the following differential equation:

$$\frac{d\mathbf{\Phi}^{(s)}}{ds} = e^{-\mathbf{\Phi}^{(s)}}\big([\lfloor\mathbb{H}^-\rfloor, \boldsymbol{K}^{(s)}]e^{\mathbf{\Phi}^{(s)}} + e^{\mathbf{\Phi}^{(s)}}[\lceil\mathbb{H}^+\rceil, \boldsymbol{K}^{(s)}]\big), \quad s \in [0, 1], \tag{14}$$

where we identify $\boldsymbol{K}^{(s)}$ with an operator of multiplication by $\boldsymbol{K}^{(s)}$ acting on the algebra $\mathsf{A}_-^+ \otimes \mathsf{CT}_{\boldsymbol{d}}$. More generally, for any Θ we define a homotopy $\mathbf{\Phi}^{(s)}\langle\Theta \sqcup d\Theta\rangle$ by the equation

$$\frac{d\mathbf{\Phi}^{(s)}}{ds}\langle\Theta\sqcup d\Theta\rangle = e^{-\mathbf{\Phi}^{(s)}}\big([\lfloor\mathbb{H}^-\rfloor+\partial, \boldsymbol{K}^{(s)}]e^{\mathbf{\Phi}^{(s)}}+e^{\mathbf{\Phi}^{(s)}}[\lceil\mathbb{H}^+\rceil+\partial, \boldsymbol{K}^{(s)}]\big), \quad s \in [0, 1], \tag{15}$$

where the differential operator $\partial = \sum_{i,j} t_{ij}\frac{\partial}{\partial t'_{ij}}$ is defined in (2). Let us point out an important corollary of (14) and (15). Suppose that $\mathbb{H}^{\pm}\langle R^{\pm}(\Theta)\rangle = 0$. Then *any homotopy leaves* $\mathbf{\Phi}\langle\Theta\rangle$ *unchanged.*

The category ALG_{SFT} and the functor *SFT* can be further significantly enriched. As we explain below, the construction of our Hamiltonian $\mathbb{H}$, potential $\mathbf{\Phi}$, etc., is based on the study of appropriate moduli spaces of holomorphic curves and their compactifications. In fact, all these objects, as they are described above, are analogs of the so-called *descendent potential* in the Gromov–Witten theory. A more systematic use of the topology of the moduli spaces allows one to define further enrichments of the theory (e.g. see the discussion of *satellites* in [15]).

1.4. Quasi-classical approximation. Let us consider the "quasi-classical" limit (when $\hbar \to 0$) of the structures entering the definition of the category ALG_{SFT}. This leads to the category ALG^0_{SFT} which is formed by the following structures. Let us first describe the objects.

- The Weyl algebra W is replaced by a graded *Poisson algebra* P over $\mathbb{C}$ which is formed by power series in p-variables with polynomial coefficients in q-variables. All variables Poisson commute except that the $\{p_{k,\gamma}, q_{k,\bar{\gamma}}\} = k$. It is useful, in fact, to think about P as an algebra of functions on a symplectic (super-)space S with coordinates $p_{k,\gamma}$ and $q_{k,\gamma}$, and the symplectic form

$$\sum_{\gamma\in\Gamma,k\geq 1} \frac{1}{k} dp_{k,\gamma} \wedge dq_{k,\bar{\gamma}}.$$

- Given $\Theta \in \mathbb{V}^d$, the element

$$\mathbb{H}\langle\Theta\rangle = \sum_{g=0}^{\infty} \mathbb{H}^{(g)}\langle\Theta\rangle\hbar^{g-1} \in \frac{1}{\hbar}\mathsf{W}\otimes\mathsf{CT}_{\boldsymbol{d}}$$

  is replaced by $\boldsymbol{h}\langle\Theta\rangle = \mathbb{H}^{(0)}\langle\Theta\rangle \in \mathsf{P}\otimes\mathsf{CT}_{\boldsymbol{d}}$.

- Axiom AO1 takes the form

$$\frac{1}{2}\{\boldsymbol{h}\langle\Theta\sqcup d\Theta\rangle, \boldsymbol{h}\langle\Theta\sqcup d\Theta\rangle\} = \partial\boldsymbol{h}\langle\Theta\sqcup d\Theta\rangle, \tag{16}$$

  where ∂ is defined in (2).

  In particular, if $d\Theta = 0$ the we have

$$\{\boldsymbol{h}\langle\Theta\rangle, \boldsymbol{h}\langle\Theta\rangle\} = 0. \tag{17}$$

In the definition of a morphism we replace the algebra A_-^+ by a_-^+ formed by formal power series in p^+-variables with polynomials coefficients in q^--variables. An element $\boldsymbol{\Phi}\langle\Theta\rangle = \sum_{g=0}^{\infty}\boldsymbol{\Phi}^{(g)}\langle\Theta\rangle\hbar^{g-1} \in \frac{1}{\hbar}\mathsf{A}_-^+\otimes\mathsf{CT}_{\boldsymbol{d}}$ reduces to $\boldsymbol{\phi}\langle\Theta\rangle = \boldsymbol{\Phi}^{(0)}\langle\Theta\rangle \in \mathsf{a}_-^+\otimes\mathsf{CT}_{\boldsymbol{d}}$. It is convenient to think about the function $\boldsymbol{\phi}\langle\Theta\rangle = \boldsymbol{\phi}\langle\Theta\rangle(T, q^-, p^+) \in \mathsf{a}_-^+\otimes\mathsf{CT}_{\boldsymbol{d}}$ as a Lagrangian submanifold

$$L_{\boldsymbol{\phi}} \subset \Big(\mathsf{S}_+, \sum_{\gamma\in\Gamma^+,k\geq 1}\frac{1}{k}dq_{k,\gamma}^+\wedge dp_{k,\bar{\gamma}}^+\Big)\oplus\Big(\mathsf{S}_-, \sum_{\gamma\in\Gamma^-,k\geq 1}\frac{1}{k}dp_{k,\gamma}^-\wedge dq_{k,\bar{\gamma}}\Big),$$

or rather a family of Lagrangian submanifolds parameterized by T:

$$L_{\boldsymbol{\phi}} = \Big\{p_{k,\gamma}^- = k\frac{\partial\boldsymbol{\phi}}{\partial q_{k,\bar{\gamma}}^-},\ q_{k,\gamma}^+ = k\frac{\partial\boldsymbol{\phi}}{\partial p_{k,\bar{\gamma}}^+};\ \gamma\in\Gamma, k\geq 1\Big\}. \tag{18}$$

Axiom AM1 reduces to the following equation for $\boldsymbol{\phi}$:

$$\big(\boldsymbol{h}^+\langle R^+(\Theta\sqcup d\Theta)\rangle + \boldsymbol{h}^-\langle R^-(\Theta\sqcup d\Theta)\rangle\big)\big|_{L_{\boldsymbol{\phi}}} = \partial\boldsymbol{\phi}\langle\Theta\rangle. \tag{19}$$

In particular, when $d\Theta = 0$ we have:

$$\big(\boldsymbol{h}^+\langle R^+(\Theta)\rangle + \boldsymbol{h}^-\langle R^-(\Theta)\rangle\big)\big|_{L_{\boldsymbol{\phi}}} = 0. \tag{20}$$

Similarly, the composition rule (12) becomes the Legendre transform formula

$$\phi_{02}(q^{(2)}, p^{(0)}) = \Big(\phi_{12}(q^{(2)}, p^{(1)}) + \phi_{01}(q^{(1)}, p^{(0)}) - \sum_{\gamma\in\Gamma^{(1)},k\geq 1} k^{-1} q^{(1)}_{k,\gamma} p^{(1)}_{k,\gamma}\Big)\big|_L, \tag{21}$$

where

$$L = \begin{cases} p^{(1)}_{k,\gamma} = k\frac{\partial\phi_{01}}{\partial q^{(1)}_{k,\bar\gamma}}, \\ q^{(1)}_{k,\gamma} = k\frac{\partial\phi_{12}}{\partial p^{(1)}_{k,\bar\gamma}}. \end{cases}$$

We denote here by ϕ_{01}, ϕ_{12} and ϕ_{02} the coefficient of $\hbar^{-1}$ in the $\hbar$-expansion of Φ_{01}, Φ_{12} and Φ_{02}, respectively.

The "chain-homotopy" equation (14) takes (assuming $d\Theta = 0$) the form of a Hamilton–Jacobi equation:

$$\frac{d\boldsymbol{\phi}^{(s)}}{ds} = \big\{(\boldsymbol{h}^+ + \boldsymbol{h}^-), \boldsymbol{k}^{(s)}\big\}\big|_{L_{\boldsymbol{\phi}^{(s)}}}. \tag{22}$$

1.5. SFT and differential equations. We explain in this section that the axioms of ALG_{SFT} (e.g. equations (1), (8), (14)) associate with each object an infinite system of commuting differential operators. In the quasi-classical approximation these operators reduce to systems of Poisson commuting integrals. On the other hand, morphisms provide (formal) solutions of evolution (Schrödinger) equations corresponding to these operators. In the quasi-classical version ALG^0_{SFT} morphisms provide solutions to Hamilton–Jacobi equations corresponding to the hierarchies of the commuting Hamiltonian functions.

Commuting differential operators. Consider an object in ALG_{SFT} with the Hamiltonian $\mathbb{H}$. Take $\Theta \in \mathbb{V}^{\boldsymbol{d}}$ with $d\Theta = 0$. Then $\mathbb{H}\langle\Theta\rangle \in \frac{1}{\hbar}\mathsf{W}\otimes\mathsf{CT}_{\boldsymbol{d}}$ satisfies the equation $\mathbb{H}\langle\Theta\rangle \circ \mathbb{H}\langle\Theta\rangle = 0$ for all values of the parameter $T = (t_{ij})$. Let us write $\mathbb{H}\langle\Theta\rangle = G(T, \hbar, q, p)$ and differentiate the identity $G \circ G = 0$ in T-variables. We get

$$\begin{aligned} &\left[\frac{\partial G}{\partial t_{ij}}, G\right] = 0, \\ &\left[\frac{\partial G}{\partial t_{ij}}, \frac{\partial G}{\partial t_{kl}}\right] + \left[\frac{\partial^2 G}{\partial t_{ij}\partial t_{kl}}, G\right] = 0, \end{aligned} \tag{23}$$

where the commutators are taken according to the sign rules in the graded world. The first equation means that the elements $G_{ij} = \frac{\partial G}{\partial t_{ij}} \in \frac{1}{\hbar}\mathsf{W}\otimes\mathsf{CT}_{\boldsymbol{d}}$ commute with the Hamiltonian, while the second one says that they commute among themselves *after passing to homology of* $\frac{1}{\hbar}\mathsf{W}\otimes\mathsf{CT}_{\boldsymbol{d}}$ *with the differential* $DA = [A, G], A \in \frac{1}{\hbar}\mathsf{W}\otimes\mathsf{CT}_{\boldsymbol{d}}$. Moreover, in many interesting examples we have $G|_{T=0} = 0$, and hence in this case

$$[G_{ij}|_{T=0}, G_{kl}|_{T=0}] = 0 \tag{24}$$

for all i, j, k, l. Recall that elements of $\frac{1}{\hbar}\mathsf{W}$ have a representation as differential operators on the Fock space

$$\mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}} = \Big\{ \sum_{k\geq 1} f_k(T)\hbar^k \Big\}.$$

Hence, we get an *infinite sequence of commuting differential operators* $\lfloor G_{ij}|_{T=0} \rfloor$ acting on $\mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}}$.

Let us write $G = \sum_0^\infty G^{(g)}\hbar^{g-1}$, and, respectively, $G_{ij} = \sum_0^\infty G_{ij}^{(g)}\hbar^{g-1}$, where $G_{ij}^{(g)} \in \frac{1}{\hbar}\mathsf{P} \otimes \mathsf{CT}_{\boldsymbol{d}}$. We also denote $\boldsymbol{g} := G^{(0)}$ and $\boldsymbol{g}_{ij} := G_{ij}^{(0)}$. Then in the quasi-classical approximation we get

$$\big\{ \boldsymbol{g}_{ij}|_{T=0},\ \boldsymbol{g}_{kl}|_{T=0} \big\} = 0, \tag{25}$$

provided that $\boldsymbol{g}|_{T=0} = 0$. In other words, $\boldsymbol{g}_{ij}|_{T=0} \in \mathsf{P}$, $i = 1, \ldots, N$, $j \geq 0$, are Poisson commuting integrals.

Hence, *the sequence of commuting differential operators* $G_{ij}|_{T=0} \in \frac{1}{\hbar}\mathsf{W}$ *is the* (*deformation*) *quantization of Poisson commuting Hamiltonians* $\boldsymbol{g}_{ij}|_{T=0} \in \mathsf{P}$.

Morphisms in $\mathbf{ALG}_{SFT}$ and evolution equations. Let us consider a morphism between two objects, $\boldsymbol{\Phi}\colon \mathcal{O}^+ \to \mathcal{O}^-$. Let $\mathbb{V}$ be the phase space associated with the morphism. For $\Theta \in \mathbb{V}^{\boldsymbol{d}}$, $\boldsymbol{d} = (d_1, \ldots, d_N)$, such that $R^\pm(d\Theta) = 0$, we denote

$$\begin{aligned} G^\pm(S, q^\pm, p^\pm, \hbar) &:= \mathbb{H}^\pm\langle R^\pm(\Theta)\rangle, \\ \Phi(S, T, q^-, p^+, \hbar) &:= \boldsymbol{\Phi}\langle \Theta \sqcup d\Theta\rangle, \end{aligned}$$

where the variables S, T generate $\mathsf{CT}_{\boldsymbol{d}\sqcup\boldsymbol{e}}$, $\boldsymbol{e} = (d_1 + 1, \ldots, d_N + 1)$.

Then according to (8) we have for $\Phi = \Phi(S, T, q^-, p^+, \hbar)$ that

$$\sum_{i,j} s_{ij}\frac{\partial}{\partial t_{ij}}\Phi = e^{-\Phi}\left(\lfloor G^-(S, q^-, p^-, \hbar)\rfloor e^{\Phi} + e^{\Phi}\lceil G^+(S, q^+, p^+, \hbar)\rceil\right). \tag{26}$$

By differentiating both sides of (8) in variables s_{ij} and then setting $S = 0$ we get

Proposition 1.3. *Suppose that* $G^\pm|_{S=0} = 0$. *Then* $\Phi(S, T, q^-, p^+, \hbar)$ *satisfies the system of commuting evolution equations*

$$\begin{aligned} &\frac{\partial\Phi}{\partial t_{ij}}(S, T, q^-, p_+, \hbar) \\ &\quad = e^{-\Phi(S,T,q^-,p^+,\hbar)}\big(\lfloor G_{ij}^-\rfloor e^{\Phi(S,T,q^-,p^+,\hbar)} + e^{\Phi(S,T,q^-,p^+,\hbar)}\lceil G_{ij}^-\rceil\big), \end{aligned} \tag{27}$$

where $G_{ij}^\pm := \frac{\partial G^\pm}{\partial s_{ij}}\big|_{S=0}$, $i = 1, \ldots, N$, $j \geq 0$.

In the quasi-classical approximation the system (27) reduces to a system Hamilton–Jacobi equations for the evolution of the corresponding Lagrangian submanifold under the system of commuting Hamiltonian flows:

$$\frac{d\phi}{dt_{ij}}(S, T, q^-, p^+) = \left(\boldsymbol{g}_{ij}^-(q^-, p^-) + \boldsymbol{g}_{ij}^+(q^+, p^+)\right)\Big|_{L_{\phi(S,T,q^-,p^+)}}, \qquad (28)$$

$i = 1, \dots, k$, $j \geq 0$.

2. Construction of the functor *SFT*

2.1. Beginning of the construction. The description of the functor *SFT* which we present here is very sketchy, and only gives a very general picture of the structures involved in the construction. It also omits many very important points. In particular, in order to actually define the functor *SFT* we need to restrict the geometric category by imposing certain genericity constraints. The actual construction of *SFT* is a large project which is currently well under way (e.g. see [8], [25]), but not yet fully completed.

Let $\mathcal{O} = (V, \Omega, \lambda, J)$ be an object in GEOM_{SFT}, i.e. a framed Hamiltonian structure, and R the corresponding Reeb field. Let us begin building the corresponding object $SFT(\mathcal{O}) \in \mathrm{ALG}_{SFT}$.

Denote by $\mathcal{P}$ the space of *simple* periodic orbits of the Reeb field R. Generically, periodic orbits are non-degenerate, i.e. the linearized Poincaré return map along each orbit has no eigenvalues equal to 1. If this is the case, then the number of orbits in $\mathcal{P}$ of bounded period is finite. We will assume either that R satisfies this non-degeneracy assumption, or the so-called *Morse–Bott* condition (see [5] for the precise definition) when periodic orbits are organized in submanifolds, and the flow of R satisfies a certain non-degeneracy condition in the direction complementary to critical submanifolds.

Let $H^*(\mathcal{P})$ be the (de Rham) cohomology space of $\mathcal{P}$. Choose a basis of Γ represented by a finite or countable system of differential forms on $\mathcal{P}$, such that the matrix of the Poincaré pairing has in this basis the form $\delta_{\gamma,\bar{\gamma}}$ for a certain involution $\gamma \mapsto \bar{\gamma}$ on Γ. Of course, in the non-degenerate case the space $\mathcal{P}$ is discrete, and hence in this case there is a canonical basis of 0-forms, dual to individual orbits. In this case the involution $\gamma \mapsto \bar{\gamma}$ is the identity map.

In the non-degenerate case each γ can be identified with an orbit from $\mathcal{P}$. We then associate the variables $p_{\gamma,k}$ and $q_{\gamma,k}$ with the k-multiple cover of the orbit γ. Their $\mathbb{Z}/2$-grading is determined as follows. Let $A_{\gamma,k}$ be the linearized Poincaré return map for this k-multiple orbit. Then the variables $p_{\gamma,k}$ and $q_{\gamma,k}$ are even or odd graded depending on whether the Lefschetz number $\det(1 - A_{\gamma,k})$ is positive or negative. If some extra choices are made one can define the integral grading of the variables $p_{\gamma,k}$ and $q_{\gamma,k}$ but we will not discuss it in this paper. With the graded variables $p_{\gamma,k}$ and $q_{\gamma,k}$ introduced, we can then define the Weyl algebra W and the space Fock.

We will not discuss here the Morse–Bott case in full generality and only consider its extreme case described above in Example 1.2 (3), when (V, Ω, λ, J) is of fibration type. All orbits of R are closed in this case and the space $\mathcal{P}$ of simple periodic orbits coincides with M. There exists a basis Γ of $H^*(M) = H^*(\mathcal{P})$, and an involution $\gamma \to \bar{\gamma}$ such that the Poincaré pairing in this basis is given by the matrix

$$(\gamma, \gamma') = \delta_{\gamma, \bar{\gamma}'}.$$

The $\mathbb{Z}/2$-degrees of the variables $p_{\gamma,k}$ and $q_{\gamma,k}$ coincide in this case with the degree of the corresponding cohomology classes $\gamma \in H^*(M)$. The phase space $\mathbb{V}$ associated with $SFT(\mathcal{O})$ is the space of differential forms on V with the de Rham differential.

The main part of $SFT(\mathcal{O})$, the Hamiltonian $\mathbb{H}$, is defined in terms of moduli spaces of certain holomorphic curves in the cylinder $V \times \mathbb{R}$ with an almost complex structure, still denoted by J, which is defined by the following conditions.

- J is invariant with respect to translations $(x, t) \mapsto (x, t + c)$, $(x, t) \in V \times \mathbb{R}$;
- $J\frac{\partial}{\partial t} = R$;
- the CR-structure induced on each slice $V \times t$ coincides with the given CR-structure J.

H. Hofer (see [27]) was the first who studied holomorphic curves in almost complex cylindrical manifolds of this type in his work on the Weinstein conjecture. He followed the pioneering work of M. Gromov (see [23]) who essentially created the new field of symplectic topology by introducing the technique of (pseudo-)holomorphic curves. Before considering the general case we sketch the construction in the very special, but already highly non-trivial case when $V = S^1$.

2.2. The circle. Consider Example 1.2 (3) for the special case when M is the point. In this case $V = S^1 = \mathbb{R}/\mathbb{Z}$ and $R = \frac{\partial}{\partial s}$, $s \in \mathbb{R}/\mathbb{Z}$. The complex structure J defined on the cylinder $C = S^1 \times \mathbb{R}$ at the end of the previous section coincides in this case with the standard complex structure on the cylinder $C = \mathbb{C}/\{z \sim z + 1\}$.

The space $\mathcal{P}$ consists of only one simple orbit, and hence Γ is just a point. Therefore, we have two infinite series of even variables $p_k, q_k, k = 1, \dots,$ and the space F is the space of "scalar" Fourier series $u(x) = \sum_{k=1}^{\infty} p_k e^{ikx} + q_k^{-ikx}$. The spaces F_+ and F_- are formal analogs of spaces of holomorphic functions in the unit disc and its complement, which are equal to 0 at the origin or ∞, respectively. The Weyl algebra W is generated by even elements p_k, q_k with $k = 1, \dots,$ and an even element $\hbar$, and consists of formal power series

$$\sum_{n=0}^{\infty} \sum_{I} g_{I,n}(q) \hbar^n p^I,$$

where $g_{I,n}(q)$ are polynomials, the second sum is taken over all infinite multi-indices $I = (i_1, i_2, \dots)$ with finitely many non-zero entries, and $p^I = p_1^{i_1} p_2^{i_2} \dots$. All variables commute except that $[p_k, q_k] = k\hbar$.

By quantizing $\lfloor p_k \rfloor = k\hbar \frac{\partial}{\partial q_k}$ we represent elements of $\frac{1}{\hbar}\mathsf{W}$ as linear differential operators on the space Fock formed by power series $\sum_{k\geq 0} f_k \hbar^k$, whose coefficients f_k are functionals on the space F_- (of "equal to 0 at ∞ holomorphic functions u in the complement of the unit disc") which can be expressed as polynomials of Fourier coefficients of u.

Next, we describe the Hamiltonian $\mathbb{H}$. Let (S, j) be a closed Riemann surface of genus g and $F\colon S \to \mathbb{C}P^1$ a meromorphic function with r_+ poles $(x_1, \dots, x_{r_+})$ and r_- zeroes $(y_1, \dots, y_{r_-})$ of multiplicities $c = (c_1, \dots, c_{r_+})$ and $b = (b_1, \dots, b_{r_-})$, respectively. By identifying $\mathbb{C}P^1 \setminus \{0, \infty\}$ with the cylinder

$$C = \mathbb{C}/\{z \sim z + 1\} = S^1 \times \mathbb{R}, \quad S^1 = \mathbb{R}/\mathbb{Z},$$

we can equivalently view the function F as a map

$$F = (f, a)\colon S \setminus \big(\{x_1, \dots, x_{r_+}\} \cup \{y_1, \dots, y_{r_-}\}\big) \to C. \tag{29}$$

With this interpretation we will call $X = \{x_1, \dots, x_{r_+}\}$ and $Y = \{y_1, \dots, y_{r_-}\}$ the sets of *positive* and *negative punctures*, respectively. If $z = e^{-\rho + i\varphi}$ is a local coordinate on S near a puncture $x_i \in X$ where $\rho \in (0, \infty)$, $\varphi \in \mathbb{R}/2\pi\mathbb{Z}$, then the map F near this puncture can be written as

$$s = f(\rho, \varphi),$$
$$t = a(\rho, \varphi),$$

where $f(\rho, \varphi) \underset{\rho\to\infty}{\longrightarrow} \frac{c_i \varphi}{2\pi}$ and $\frac{a(\rho,\varphi)}{\rho} \underset{\rho\to\infty}{\longrightarrow} c_i$. In other words, at x_i the map F is asymptotic to the c_i-multiple circle $S^1 = \mathbb{R}/\mathbb{Z}$ at $+\infty$ of the coordinate t. Similarly, at a puncture $y_j \in Y$ the map F is asymptotic to the $-b_j$-multiple circle $S^1 = \mathbb{R}/\,\mathbb{Z}$ at $-\infty$ of the coordinate t. For a fixed genus and fixed multiplicity vectors $c = (c_1, \dots, c_{r_+})$ and $b = (b_1, \dots, b_{r_-})$ we denote by $\mathcal{M}_g(C; c, b)$ the moduli space of equivalency classes of meromorphic functions defined in (29). The integer vectors c and b are called the *positive* and *negative ramification data*. We will also denote by $\mathcal{M}_{g,k}(C; c, b)$ a similar moduli space with k additional marked points (disjoint from X and Y and each other) $z_1, \dots, z_k$. The stability condition: $g + 2k + r_+ + r_- \geq 3$, is required to be satisfied. Notice that we do not fix a conformal structure on the surface and the configurations of punctures and marked points. Two maps are called equivalent if they differ by a conformal map $(S_g, j) \to (S_g, j')$ which preserves all punctures and marked points. We will also consider the quotient $\mathcal{M}_{g,k}(C; c, b)/\mathbb{R}$ by translations of $C = S^1 \times \mathbb{R}$ along the $\mathbb{R}$-factor.

The moduli space $\mathcal{M}_{g,k}(C; c, b)/\mathbb{R}$ can be compactified by adding *stable holomorphic buildings*, see [8]. A stable building of height 1 is a stable nodal holomorphic curve in the sense of Kontsevich, i.e. an equivalency class of holomorphic maps defined

on a possibly disconnected Riemann surface with certain pairs of marked points (called *special*) required to be mapped to one point on C. The stability condition should be satisfied for each connected component, and the source surface must become connected after identifying points of each special pair. As above, the equivalence relation identifies buildings which differ by translation of C along the $\mathbb{R}$-factor. A stable building F of height $l > 1$ is a collection of stable buildings $F_1, \dots, F_l$ of height 1, with the condition that the positive ramification data of the building F_i, $i = 1, \dots, l-1$, coincides with the negative ramification data of F_{i+1}. By definition, the negative ramification data of F_1 is the negative ramification data of F, and the positive ramification data of F_l is the positive ramification data of F. The genus of F is the genus of the surface obtained by gluing for each $i = 1, \dots, l-1$ the source surfaces of buildings F_i and F_{i+1} along their respective ends. The compactified moduli space will be denoted by $\overline{\mathcal{M}/\mathbb{R}}_{g,k}(C; c, b)$.

The evaluation map at the j-th marked points z_j defines a map

$$\mathrm{ev}_j : \overline{\mathcal{M}/\mathbb{R}}_{g,k}(C; c, b) \to S^1 = \mathbb{R}/\mathbb{Z}.$$

To define the Hamiltonian $\mathbb{H}$ we need to pick a system of forms. For our case of S^1 let us take $\Theta = (\theta_0 = 1, \theta_1 = ds)$. Then the corresponding algebra CT is generated by elements of the matrix $T = (t_{ij})$, $i = 0, 1$, $j \geq 0$, with even variables t_{0j} and odd variables t_{1j}.

As it is customary in Gromov–Witten theory, we define *correlators*

$$\langle T, \dots, T \rangle_{g,k,c,b} = \int\limits_{\overline{\mathcal{M}/\mathbb{R}}_{g,k}(C;c,b)} \Big(\sum t_{ij}\, \mathrm{ev}_1^*(\theta_i) c_1(L_1)^j \Big) \wedge \dots \wedge \Big(\sum t_{ij}\, \mathrm{ev}_k^*(\theta_i) c_1(L_k)^j \Big), \quad (30)$$

where L_j, $j = 1, \dots, k$, is a tautological line bundle over $\overline{\mathcal{M}/\mathbb{R}}_{g,k}(C; c, b)$ which associates with each holomorphic curve (building) the cotangent line at the j-th marked point z_j.[1]

Consider now the generating function $\mathbb{H} \in \frac{1}{\hbar}\mathsf{W} \otimes \mathsf{CT}_{\boldsymbol{d}}$,

$$\mathbb{H} = \sum_{g \geq 0,\, k \geq 0,\, b, d} \frac{\langle T, \dots, T \rangle_{g,k,c,b}}{k!(r_-)!(r_+)!} \hbar^{g-1} q^b p^c, \quad (31)$$

where $q^b = q_{b_1} \dots q_{b_{r_-}}$, $p^c = p_{c_1} \dots p_{c_{r_+}}$.

[1] The integration in this and other similar formulas should be understood either in the sense of the virtual cycle theory if one works in the algebro-geometric context, or literally but after an appropriate generic perturbation, see [23], [39]. In fact, to achieve transversality one needs sometimes to perturb in a class of objects more general than holomorphic curves. The relevant transversality theorem was first proven by K. Fukaya and K. Ono in [19] in the context of Floer homology theory. Following their work the transversality issues in Gromov–Witten theory were studied by several authors. H. Hofer, jointly with K. Wysocki and E. Zehnder, has recently developed a new functional analytic theory of polyfolds, which provides the most suitable set-up for handling transversality problems arising in SFT, see [25], [26]. One also needs to use *coherent orientations* of different moduli spaces, as it is described in [15].

The Hamiltonian $\mathbb{H}$ can be quite explicitly written in this case, thanks to the results of A. Okounkov and R. Pandharipande, see [41].

First of all, it follows from the parity arguments that $\mathbb{H}|_{T_1=0} = 0$, where we denote $T_i = (t_{ij})$, $j \geq 0, i = 0, 1$. Hence,

$$\mathbb{H} = \sum_{j\geq 0} t_{1j}\mathbb{H}_j + o(T) \tag{32}$$

Let us introduce a new variable y and define a *generating function* for the sequence of operators $G_j = \mathbb{H}|_{T_0=0}$:

$$G(y) = \sum_0^\infty G_j y^j.$$

Take $u(x) = \sum_{k=1}^\infty p_k e^{ikx} + q_k e^{-ikx} \in \mathsf{F}$ and denote by $\phi(x)$ the function determined by equations

$$\phi'(x) = u(x),\ \phi(0) = 0.$$

In other words,

$$\phi(x) = -i\sum_{k=1}^\infty \left(\frac{p_k}{k}e^{ikx} - \frac{q_k}{k}e^{-ikx}\right).$$

Let us also set $\hbar = \lambda^2$. Then we have

$$G(y)[u] = \frac{1}{2\pi\lambda^2 y^2\, \mathrm{s}(\lambda y)} \int_0^{2\pi} dx \left(e^{\frac{i}{\lambda}\left(\phi\left(x-\frac{i\lambda y}{2}\right)-\phi\left(x+\frac{i\lambda y}{2}\right)\right)} - 1\right), \tag{33}$$

where

$$\mathrm{s}(u) = \frac{2\sinh\frac{u}{2}}{u}.$$

Let us write explicitly a few first terms G_k:

$$\begin{aligned} G_0 &= \frac{1}{2\pi\hbar}\int_0^{2\pi} \frac{u^2}{2} dx\,; \\ G_1 &= \frac{1}{2\pi\hbar}\int_0^{2\pi} \frac{u^3}{6} dx\,; \\ G_2 &= \frac{1}{2\pi}\int_0^{2\pi} \left(\hbar^{-1}\frac{u^4}{24} + \frac{u^2}{12} - \frac{uu''}{6}\right) dx. \end{aligned} \tag{34}$$

It is interesting to note that the genus 0 term of G_k, $k \geq 0$, i.e. the coefficient of $\hbar^{-1}$, is equal to

$$G_k^{(0)} = \frac{1}{2\pi} \int_0^{2\pi} \frac{u^{k+2}}{(k+2)!}\, dx.$$

These are commuting integrals of the dispersionless KdV, or Burgers integrable hierarchy, and hence the operators $\lfloor G_k \rfloor$ acting on Fock, provides the deformation quantization of this hierarchy.

2.3. Case of a general Hamiltonian structure. In order to define $\mathbb{H}$ for a general Hamiltonian structure (V, Ω, λ, J) we consider moduli spaces of J-holomorphic curves in the cylindrical almost complex manifold $(W = V \times \mathbb{R}, J)$.

Notice that for our choice of J the cylinder $\gamma \times \mathbb{R} \subset W$ over a trajectory γ of the Reeb field R is always a J-holomorphic curve. Given a J-holomorphic map F of a punctured disk $D^2 \setminus 0 \to W$ with the coordinate $z = e^{-\rho + i\varphi}$, we say that the map $F = (f, a)$ is *asymptotically cylindrical* over a periodic orbit γ of the Reeb field R at $+\infty$ (resp. at $-\infty$) if $\lim_{\rho \to \infty} a(z) = +\infty$ (resp. $= -\infty$), and $\lim_{\rho \to \infty} f(z) = \bar{f}\big(\pm \frac{T\varphi}{2\pi}\big)$, where the map $\bar{f}\colon [0, T] \to V$ parameterizes the trajectory γ in such a way that R is its velocity vector, and T is the period of γ.

Let $S = S_g$ be a compact Riemann surface of genus g with a conformal structure j, with r_+ punctures $\boldsymbol{x} = \{x_1, \dots, x_{r_+}\}$, called positive, r_- punctures $\boldsymbol{y} = \{y_1, \dots, y_{r_-}\}$, called negative, and also k marked points $z_1, \dots, z_k$, disjoint from each other and the punctures.

Given two vectors $c = (c_1, \dots, c_{r_+})$ and $b = (b_1, \dots, b_{r_-})$ of positive integers we consider moduli spaces $\mathcal{M}_{g,k}(W, J; c, b)$ of (j, J)-holomorphic curves

$$(S_g \setminus (\boldsymbol{x} \cup \boldsymbol{y}), j) \to (W, J)$$

with k marked points $z_1, \dots, z_k$, which are asymptotically cylindrical over a c_i-multiply covered periodic orbit from $\mathcal{P}$ at the positive end at the puncture x_i, and asymptotically cylindrical over a $(-b_j)$-multiply covered periodic orbit at the negative end at the puncture y_j. We will also consider the quotient $\mathcal{M}(W, J; c, b)/\mathbb{R}$ of the space $\mathcal{M}_{g,k}(W, J; c, b)$ by translations along the $\mathbb{R}$-factor.

For our distinguished structure J, the holomorphic curve equation takes the form

$$\begin{aligned} \pi \circ df \circ j &= J \circ \pi \circ df \\ da &= (f^*\lambda) \circ j. \end{aligned} \tag{35}$$

Notice that the second equation just means that the form $f^*\lambda \circ j$ is exact on S and that the function a is a primitive of the 1-form $f^*\lambda \circ j$. Thus the holomorphicity condition for $F = (f, a)$ is essentially just a condition on its V-component f. If f satisfies the first of the equations (35) and the form $(f^*\lambda) \circ j$ is exact then the coordinate a can be reconstructed uniquely up to an additive constant on each connected component

of S. Therefore, an element $F \in \mathcal{M}_{g,k}(W, J; c, b)$ is uniquely determined by its V-component f, which is a surface bounded by multiply covered orbits from $\mathcal{P}$.

Given $\alpha \geq 0$, let us denote by $\mathcal{M}^{\alpha}_{g,k}(W, J, c, b)$ the subspace

$$\mathcal{M}_{g,k}(W, J, c, b) \cap \left\{ \int_{S_g} F^*\omega \leq \alpha \right\}.$$

The quotient space $\mathcal{M}^{\alpha}_{g,k}(W, J, c, b)$ has a compactification $\overline{\mathcal{M}/\mathbb{R}}^{\alpha}_{g,k}(W, J, c, b)$ by holomorphic buildings[2] (see [8]), similar to the one considered above for the case $V = S^1$. We denote

$$\overline{\mathcal{M}/\mathbb{R}}_{g,k}(W, J, c, b) = \bigcup_{\alpha \geq 0} \overline{\mathcal{M}/\mathbb{R}}^{\alpha}_{g,k}(W, J, c, b)$$

and

$$\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J) = \bigcup_{\substack{k,c,b \\ k+r_++r_-=m}} \overline{\mathcal{M}/\mathbb{R}}_{g,k}(W, J, c, b)$$

The space $\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J)$ may consists of different components,

$$\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J) = \bigcup C_i.$$

Given $F \in C_i$, we denote by μ_i its symplectic area $\int_{S_g} F^*\omega$, which depends only on the component C_i.

By using the notation $\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J)$ we put the punctures and the marked points on the equal footing. Keeping up with this point of view, let us consider the disjoint union

$$X = \coprod_{-\infty}^{\infty} \mathcal{P}_j,$$

where

$$\mathcal{P}_j = \begin{cases} \mathcal{P} & \text{if } j \neq 0, \\ V & \text{if } j = 0, \end{cases}$$

and supply each $\mathcal{P}_j$, $j \neq 0$, with an identical copy $\Gamma^{(j)}$ of the basis Γ of $H^*(\mathcal{P})$.

Consider an evaluation map

$$\mathrm{ev} = (\mathrm{ev}_1, \ldots, \mathrm{ev}_m) \colon \overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J) \to \underbrace{X \times \cdots \times X}_{m}$$

which associates

[2] In the Morse–Bott case one also needs to add to the compactification the so-called *generalized holomorphic buildings*, see [5] and [8].

– with each marked point z_i its value $f(z_i) \in V = \mathcal{P}_0$,

– with each positive puncture x_i the corresponding periodic orbit in the $\mathcal{P}_k$-copy of $\mathcal{P}$, where $k = c_i$ is its multiplicity,

– with each negative puncture y_i the corresponding periodic orbit in the $\mathcal{P}_{-k}$-copy of $\mathcal{P}$, where $k = b_i$ is its multiplicity.

Choose a system of closed forms $\Theta = (\theta_1, \dots, \theta_N)$ and associate with it a matrix $T = (t_{ij})$ of graded variables. Consider the following formal expression ("general cohomology class of X with descendents")

$$Z = \sum_{i=1}^{n} \sum_{j=0}^{\infty} t_{ij} \theta_i c^j + \sum_{k=1}^{\infty} \sum_{\gamma \in \Gamma} p_{\gamma,k} \gamma^{(k)} + q_{\gamma,k} \gamma^{(-k)},$$

where $\gamma^{(j)}$ denotes the copy of $\gamma \in \Gamma$ in $\Gamma^{(j)}$, $j \neq 0$, and set

$$\mathrm{ev}_l^* Z = \sum_{i=1}^{n} \sum_{j=0}^{\infty} t_{ij} \, \mathrm{ev}_l^* \theta_i \, (c_1(L_l))^j + \sum_{k=1}^{\infty} \sum_{\gamma \in \Gamma} p_{\gamma,k} \, \mathrm{ev}_l^* \, \gamma^{(k)} + q_{\gamma,k} \, \mathrm{ev}_l^* \, \gamma^{(-k)},$$

where the line bundles L_l over $\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J)$ have the same meaning as in Section 2.2 above. Define the correlator

$$\langle \underbrace{Z, \dots, Z}_{m} \rangle_g = \sum_{j=1}^{\infty} z^{\mu_j} \int_{C_j} \mathrm{ev}^* (\underbrace{Z \otimes \cdots \otimes Z}_{m}), \tag{36}$$

where the sum is taken over all components of $\overline{\mathcal{M}/\mathbb{R}}_{g,m}(W, J)$.

Remark 2.1. Note that by introducing exponents z^{μ_j} in the definition of the correlators we effectively extended the coefficient ring from $\mathbb{C}$ to a certain Novikov ring (of Puiseux power series $\sum_j a_j z^{\mu_j}$). This was done to avoid infinities in (36). However, it is not absolutely necessary to do that, and one can ignore these weights by setting $z = 1$ in most of the cases. For instance, for Hamiltonian structures of contact type there are always only finitely many terms in the sum which contribute in (36) to the coefficient of a fixed monomial of q, p and $\hbar$ variables. But even in the most general situation one can alternatively deal with this problem by requiring the string of forms Θ to contain closed 2-forms which form a basis of $H^2(V)$ (this approach is similar to the divisor equation in the Gromov–Witten theory).

Finally, we define the Hamiltonian

$$\mathbb{H}(\Theta) = \sum_{g=0}^{\infty} \sum_{m=0}^{\infty} \frac{1}{m!} \langle \underbrace{Z, \dots, Z}_{m} \rangle_g \hbar^{g-1}. \tag{37}$$

Note that all terms of $\mathbb{H}$ have the same *odd* degree (and, in fact, degree 1 if the grading is upgraded to $\mathbb{Z}$ from $\mathbb{Z}/2$), because we integrate over the moduli spaces quotiented by the $\mathbb{R}$-action.

The "master equations" (1) and (16) follow from Stokes' formula combined with the description of the boundary of the corresponding moduli spaces.

All the other necessary constructions to build the functor *SFT* are done in the same spirit. Consider, for instance, a framed cobordism (W, Ω, J) which realizes a morphism $\mathbf{\Phi}\colon \mathcal{O}^+ \to \mathcal{O}^-$ between two framed Hamiltonian structures

$$\mathcal{O}^\pm = (V^\pm, \Omega^\pm, \lambda^\pm, J^\pm).$$

The phase space $\mathbb{V}$ associated with this cobordism is the space of differential forms on W, and $R^\pm$ are the restriction homomorphisms to $V^\pm$.

Take $\Theta \in \widehat{\mathbb{V}}^d$ and associate with it the corresponding graded algebra CT_d. To define the potential $\Phi \in \frac{1}{\hbar}\mathsf{A}_-^+ \otimes \mathsf{CT}_d$ we attach to the cobordism cylindrical ends corresponding to framed Hamiltonian structures $\mathcal{O}^\pm$,

$$\widehat{W} = \left(V^- \times (-\infty, 0]\right) \cup W \cup \left(V^+ \times [0, \infty)\right),$$

and consider the compactified moduli space of holomorphic curves in $\widehat{W}$ asymptotically cylindrical to periodic orbits of the Reeb field R_+ at the positive end, and the orbits of R_- at the negative one. Then the correlators and the potential are defined by the formulas similar to (36) and (37) with one very important difference: in this situation there is no $\mathbb{R}$-action on the moduli space, and hence the integrals should be evaluated on the moduli space itself, rather than its quotient by the $\mathbb{R}$-action, as was done for the Hamiltonian. The implication of this is that the potential, unlike the Hamiltonian, has an *even* degree (in fact, degree 0 if the grading is upgraded to $\mathbb{Z}$ from $\mathbb{Z}/2$). As in the case of the Hamiltonian, the structural equation (8) is a consequence of Stokes' formula and the description of the boundary of the corresponding moduli space.

Note that if the symplectic manifold W is closed, i.e. it is a cobordism between empty Hamiltonian structures, then the corresponding SFT-potential $\mathbf{\Phi}(\Theta) \in \mathsf{CT}_{\boldsymbol{d}}$ is just the descendent potential of the Gromov–Witten theory.

2.4. The 3-sphere. Let us consider here an example when $V = S^3$, λ is the standard contact form whose Reeb field generates the Hopf fibration, J is the CR-structure induced from $\mathbb{C}^2$ on the round sphere. This is a pre-quantization space, so it fits into both, the contact and the fibration cases in the sense of Example 1.2.

The manifold (W, J) can be equivalently described here either as $\mathbb{C}^2 \setminus 0$, or the total space of the canonical degree 1 complex line bundle L over $\mathbb{C}P^1$ minus the 0-section. In the second interpretation a holomorphic curve from $\mathcal{M}(W, J, c, b)$ can be viewed as a pair (h, ψ), where $h\colon S_g \to \mathbb{C}P^1$ is a holomorphic curve, and ψ is a meromorphic section of the induced complex line bundle h^*L over S_g. The punctures

from $\boldsymbol{x}$ and $\boldsymbol{y}$ correspond to zeroes and poles of this section, respectively, while the vectors c and b appear as the multiplicities of zeroes and poles.

Take a basis of $H^*(\mathbb{C}P^1)$ which consists of $\gamma_0 = 1$ and the harmonic form γ_2 with $\int_{\mathbb{C}P^1} \gamma_2 = 1$. The Poincaré duality involution acts as $\bar{\gamma}_0 = \gamma_2$. Thus the Weyl algebra W is generated by even graded variables $p_{0k} = p_{\gamma_0,k}$, $p_{2k} = p_{\gamma_2,k}$, $q_{0k} = q_{\gamma_0,k}$, and $q_{2k} = q_{\gamma_2,k}$, $k \geq 1$. We organize them into formal Fourier series

$$u_0(x) = \sum_1^\infty p_{0k} e^{ikx} + q_{0k} e^{-ikx},\ u_2(x) = \sum_1^\infty p_{2k} e^{ikx} + q_{2k} e^{-ikx},\ u = (u_0, u_2).$$

Let us choose a basis $(\theta_0 = 1, \theta_3)$ of $H^*(S^3)$, where θ_3 is a harmonic 3-form with $\int_{S^3} \theta_3 = 1$, as the required string Θ of differential forms. The algebra $\mathsf{CT}_{\boldsymbol{d}}$ in this case is generated by $T = (T_0, T_3)$, where $T_i = (t_{ij})$, $i = 0, 3$; $j \geq 0$. The variables t_{0j} are even, while t_{3j} are odd.

As was shown in [15], the genus 0 part $\mathbb{H}^{(0)}$ of the Hamiltonian $\mathbb{H}$ can be explicitly reconstructed in terms of the genus 0 descendent Gromov–Witten potential of $\mathbb{C}P^1$ (in fact, this is a general phenomenon for all Hamiltonian structures of fibration type). In particular, we get

$$G_0 = \frac{1}{2\pi} \int_0^{2\pi} \left(\frac{(t_0 + u_0(x))^2}{2} + e^{u_2(x) - ix} \right) dx, \tag{38}$$

and the Hamiltonian equations for the Hamiltonian G_0 can be written as

$$\begin{aligned} \dot{u}_0(x) &= -i \frac{d}{dx} \left(e^{u_2(x) - ix} \right), \\ \dot{u}_2(x) &= -i \frac{du_0}{dx}(x), \end{aligned} \tag{39}$$

or $\ddot{u}_2 = -\frac{d^2}{dx^2}(e^{u_2 - ix})$, where the dot denotes the time derivative.

As was pointed out to me by B. Dubrovin, this is the continuous limit of the Toda lattice. The other G_i are Poisson commuting integrals of this integrable hierarchy. Hence, if one were to explicitly write for this example the terms of the expansion of the full Hamiltonian $\mathbb{H}$ (and not only of its genus 0 term $\mathbb{H}^{(0)}$) then this would provide the quantum commuting integrals for the quantization of the Toda system (39).[3]

Let us now use the Hamilton–Jacobi equation (28) to compute the genus 0 potential of the round 4-ball $B \subset \mathbb{C}^2$. Take a 4-form θ supported in Int B^4 with $\int_{B^4} \theta = 1$ and set $\Theta = \{\theta\}$. Let $T = (t_j)$, $j \geq 0$ be the corresponding string of even graded variables. Take the genus 0 potential $\boldsymbol{\Phi}^{(0)}(\Theta) = \Phi^{(0)}(T, p) \in \mathsf{P} \otimes \mathbb{C}[T]$, and consider its restriction $\phi(t, p)$ to the subspace $T = \{(t, 0, 0, \dots)\}$. Note that $\phi(t, p)$

[3] One can extract from the work [38] an explicit, though quite complicated recurrent procedure for writing down the expansion of the full Hamiltonian $\mathbb{H}$ in terms of the descendent Gromov–Witten potential of $\mathbb{C}P^1$.

is, in fact, a certain relative genus 0 Gromov–Witten invariant. Coefficients in its expansion in t and p variables count the numbers of rational curves in $\mathbb{C}P^2$ which pass through a given number of fixed points and have a prescribed tangency pattern to a fixed complex line $C \subset \mathbb{C}P^2$. According to (28) $\phi(t, p)$ can be computed as a solution of a Hamilton–Jacobi equation associated with the Hamiltonian flow (39). Let $E^t\colon \mathsf{F} \to \mathsf{F}$ be the (formal, i.e. understood in terms of formal power series) Hamiltonian flow defined by the equation (39). Take the Lagrangian subspace $\mathsf{F}_+ = \{(u_+, 0)\} = \{q = 0\} \subset \mathsf{F}$ and denote by L^t its image $E^t(\mathsf{F}_+)$ under the flow E^t. Then $\phi(t, p)$ is the generating function for $L^{(t)}$ in the sense of (18), i.e.

$$L^{(t)} = L_\phi = \Big\{q_{k,0} = k\frac{\partial \phi}{\partial p_{k,2}},\ q_{k,2} = k\frac{\partial \phi}{\partial p_{k,0}},\ k \geq 1\Big\}.$$

Let us switch to the (u_-, u_+)-notation, i.e. write u_- for q and u_+ for p, and apply a standard symplectic-geometric procedure for computing the generating function in terms of the Lagrangian submanifold which it defines. Let us define L_t by an explicit equation $u_- = f^t(u_+)$ (i.e. exclude v from the parametric equations $(u_+, u_-) = E^t(v, 0),\ v \in \mathsf{F}_+$). Then we have

$$\phi(t, u_+) = -\frac{i}{2\pi}\int_0^1\int_0^{2\pi}\Big\langle f^t(su_+(x)), \frac{du_+(x)}{dx}\Big\rangle dx ds, \tag{40}$$

where $\langle\cdot,\cdot\rangle$ is a bilinear form on $\mathbb{C}^2$ with the matrix $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$.

It is interesting to note that the value of the functional $\phi(t, u_+)$ at the point $\overline{u}_+ = (ze^{ix}, 0)$, i.e. the function

$$g(t, z) = \phi(t, \overline{u}_+) = z\int_0^1 f^t_{(2,1)}(sze^{ix})\, ds, \tag{41}$$

where we write

$$f^t = (f^t_0, f^t_2) = \Big(\sum_1^\infty f^t_{0,k}e^{-ikx}, \sum_1^\infty f^t_{2,k}e^{-ikx}\Big),$$

is the generating function

$$g(t, z) = \sum_{d=1}^\infty\sum_{m=1}^\infty N_{d,k}t^m z^d$$

for the numbers $N_{d,k}$ of rational curves of degree d which pass through m points in general position in the complex projective plane.[4] In order to get (41) from (40) one needs to split $\mathbb{C}P^2$ along a boundary of a tubular neighborhood of $\mathbb{C}P^1 \subset \mathbb{C}P^2$ and apply the gluing formula (21), see [15].

[4] As it is well known, the coefficients $N_{d,k}$ vanish unless $k = 3d-1$, and we have $N_{1,2} = 1$, $N_{2,5} = 1$, $N_{3,8} = 12$, $N_{4,11} = 620, \ldots$. Several recursion relations, beginning from the one discovered by M. Kontsevich in [32], are known for computing the coefficients $N_{d,k}$.

3. Invariants of contact manifolds and other applications of SFT

3.1. Invariants of contact manifolds. Defining invariants of contact manifolds was one of the primary motivations for the SFT project.

Let (V, λ, J) be a framed Hamiltonian structure of contact type. Choose a system of closed forms $\Theta = (\theta_1, \dots, \theta_N)$ which represents a basis of the cohomology $H^*(V)$ and consider the corresponding Hamiltonian

$$\mathbb{H}\langle\Theta\rangle = \sum_{g=0}^{\infty} H^{(g)}(T, q, p)\hbar^{g-1}.$$

Consider the following SFT objects which can be associated with (V, λ, J):

1. The Weyl differential algebra $(\mathsf{W} \otimes \mathsf{CT}_{\boldsymbol{d}}, \boldsymbol{D})$, where
$$\boldsymbol{D}A = [A, \mathbb{H}\langle\Theta\rangle], \quad \mathbb{H}\langle\Theta\rangle \in \frac{1}{\hbar}\mathsf{W} \otimes \mathsf{CT}_{\boldsymbol{d}}.$$
2. The space $\mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}}$ with the differential[5]
$$Df = \lfloor \mathbb{H}\langle\Theta\rangle \rfloor f, \quad f \in \mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}}.$$
3. The Poisson differential algebra $(\mathsf{P} \otimes \mathsf{CT}_{\boldsymbol{d}}, d)$ with the differential
$$dA = \{A, \mathbb{H}^{(0)}\langle\Theta\rangle\}, \quad A \in \mathsf{P} \otimes \mathsf{CT}_{\boldsymbol{d}}.$$
4. The differential algebra $(\mathsf{fock} \otimes \mathsf{CT}_{\boldsymbol{d}}, \mathfrak{d})$ where $\mathsf{Fock} = \mathsf{fock}[[\hbar]]$ and the differential $\mathfrak{d}$ is defined as follows. Consider the expansion
$$\mathbb{H}^{(0)}\langle\Theta\rangle = \sum_{\gamma\in\Gamma, k\geq 1} h_{k,\gamma}(q, T)p_{k,\gamma} + o(p). \tag{42}$$
Then we define $\mathfrak{d}q_{k,\gamma} = kh_{k,\bar{\gamma}}(q, T)$ and extend $\mathfrak{d}$ to the whole algebra using the Leibnitz rule.

In all the above cases the corresponding homology, together with all the inherited algebraic structures, is an invariant of the contact manifold $(V, \xi = \{\lambda = 0\})$ (see [15]), and thus independent of the choice of J, the contact form λ, and the representatives θ_j of the corresponding cohomology classes of $H^*(V)$. Moreover, the homotopy types of the corresponding differential algebras are also invariants of (V, ξ).

However, sometimes it is possible to define a simpler, easier computable contact invariant. Let us restrict the discussion to the case when the set of forms Θ is empty or, equivalently, set $T = 0$. The differential $\mathfrak{d}$ in Case 4 can be viewed as a vector field

$$\mathfrak{d}(q) = \sum_{k,\gamma} kh_{k,\bar{\gamma}}(q)\frac{\partial}{\partial q_{k,\gamma}}$$

[5]The algebraic structure of $(\mathsf{Fock} \otimes \mathsf{CT}_{\boldsymbol{d}}, D)$ can be described in terms of the BV_∞-formalism, see [9].

on the space with coordinates $q_{k,\gamma}$. Suppose there are constants $a_{k,\gamma} \in \mathbb{C}$ such that $\mathfrak{d}(a) = 0$, where $a = \{a_{k,\gamma}\}$. Then one can define the linearized homology of the algebra $(\mathsf{fock}, \mathfrak{d})$ at the point a. More precisely, following Yu. Chekanov [11] we define an *augmentation* of the algebra $(\mathsf{fock}, \mathfrak{d})$ as a graded chain homomorphism $\varepsilon\colon (\mathsf{fock}, \mathfrak{d}) \to (\mathbb{C}, 0)$. In other words, this means that $\mathfrak{d}(a) = 0$ where $a = \{a_{k,\gamma} = h(q_{\gamma,k})\}$ and $a_{k,\gamma} = 0$ unless $a_{k,\gamma}$ has grading 0. The linearized complex is defined as

$$\big(\mathsf{fock}_{d\geq 1}/\mathsf{fock}_{d\geq 2}, d_\varepsilon = \phi_\varepsilon \circ \mathfrak{d} \circ \phi_\varepsilon^{-1}\big), \tag{43}$$

where $\mathsf{fock}_{d\geq m}$ denotes the ideal in fock generated by monomials of degree $\geq m$, and the algebra homomorphism $\phi_\varepsilon\colon \mathsf{fock} \to \mathsf{fock}$ is defined on the generators $q_{k,\gamma}$ as the shift $q_{k,\gamma} \mapsto q_{k,\gamma} + a_{k,\gamma}$. It turns out that if the algebra $(\mathsf{fock}, \mathfrak{d})$ admits a unique augmentation for a certain choice of λ and J, then for any other choice the corresponding algebra admits an augmentation ε, and the homology of the complex (43) is independent of choices of λ, J and ε, and hence it is an invariant of the contact structure ξ, see [11] and [7]. This homology, denoted $CH_*(V, \xi)$ is usually called *cylindrical contact homology* because in all known cases when this homology is defined, there exists a class of forms for which $\mathfrak{d}(0) = 0$, and hence the differential of the linearized complex (43) is determined by holomorphic cylinders. If the cylindrical contact homology is defined then all the other algebraic structures described in examples 1–4 can be interpreted as certain (co-)homological operations on $\mathrm{CH}_*(V, \xi)$. Here are some examples when cylindrical contact homology is well defined and can be computed:

a) *Subcritical Stein-fillable contact manifolds.* (V, ξ) is called Stein fillable if it appears as a strictly pseudo-convex boundary of a Stein domain W. The subcriticality means that W has a homotopy type of a CW-complex of dimension $< \dim_{\mathbb{C}} W$. Under an additional assumption $c_1(\xi) = 0$, M.-L. Yau (see [50]) proved that the cylindrical contact homology is well defined. She also computed it in terms of $H_*(W)$. It seems likely that the condition $c_1(\xi) = 0$ can be removed.

b) *Prequantization spaces.* Cylindrical contact homology of a prequantization space (V, ξ) of a symplectic manifold (M, ω) is well defined and can be expressed through the homology $H_*(M)$, see [15] and [5]. Note that by juxtaposing the computations in a) and b) one gets non-trivial restrictions on the topology of symplectic manifolds with subcritical polarizations in the sense of [4] (e.g. complex projective manifolds admitting a hyperplane section whose complement is a subcritical Stein manifold).

c) *Spaces of co-oriented contact manifolds.* Given an oriented n-dimensional closed M, the cylindrical contact homology of its unit cotangent bundle ST^*M is always well defined, and we have $\mathrm{CH}_*(ST^*M) = H_*^{S^1}(\Lambda(M), M)$ where $H_*^{S^1}(\Lambda(M), M)$ is the equivariant homology of the free loop space modulo constant loops. See [49], [43], [1], [9] for related results.

d) *Brieskorn varieties.* I. Ustilovsky (see [48]) computed contact homology of certain Brieskorn spheres. His computation implied existence of infinitely many non-isomorphic contact structures on spheres of dimension $4k+1$. F. Bourgeois ([5]) and O. van Koert ([33]) extended Ustilovsky's computations to a large class of other Brieskorn varieties.

e) *Toroidal 3-manifolds.* It was shown in [15] and [5] that cylindrical contact homology distinguish all the contact structures on T^3 (there are infinitely many of them according to E. Giroux, see [22]). F. Bourgeois and V. Colin, see [6], generalized this computation to toroidal (i.e. containing an incompressible torus) irreducible 3-manifolds and as a consequence showed that such manifolds have infinitely many non-isotopic (universally) tight contact structures. This result should be contrasted with a theorem of V. Colin, E. Giroux and Ko Honda, see [12], which states that atoroidal irreducible 3-manifolds may admit only finitely many non-isotopic tight contact structures.

f) *Exact triangle for Legendrian surgery.* In [7] F. Bourgeois, T. Ekholm and the author found an exact triangle which relates cylindrical contact homology before and after surgery along a Legendrian sphere, and a certain cyclic complex associated to the differential algebra of the Legendrian sphere, see discussion of relative SFT in Section 3.3 below. This exact triangle is tightly related to Seidel's exact triangle describing an effect of a symplectic Dehn twist on Floer homology, see [44] and [45].

F. Bourgeois computed in his dissertation [5] cylindrical contact homology for a number of other interesting examples (e.g. for T^k-invariant contact structures constructed by R. Lutz in [37] on some $(2k+1)$-manifolds). Most recently, V. Colin and K. Honda, see [28], announced a result that the cylindrical contact homology is defined and not trivial for a large class of tight contact 3-manifolds. This theorem implies the Weinstein conjecture (i.e. existence of periodic orbits of the Reeb flow) for this class of contact 3-manifolds. It seems likely that cylindrical contact homology is well defined at least for all Stein fillable, or maybe even more generally, symplectically fillable contact manifolds. Note that the algebra $(\mathsf{fock}, \mathfrak{d})$ for symplectically fillable contact manifolds always admits an augmentation (see [7]), which is unique in all known cases for an appropriate choice of λ and J.

3.2. Topological invariants via SFT. There are several canonical constructions which associate with smooth manifolds and their submanifolds symplectic and contact manifolds and their Lagrangian and Legendrian submanifolds. Here are a few examples:

(1) Given a smooth closed n-manifold, one can associate with it its cotangent bundle T^*M with its canonical symplectic form $\omega = dp \wedge dq$, or its unit cotangent bundle (the space of co-oriented contact elements) ST^*M with its canonical contact structure ξ given by the contact form $pdq|_{ST^*M}$.

(2) Given a submanifold $K \subset M$ one can associate with K its Lagrangian conormal bundle $L_K \subset T^*M$, or its Legendrian lift $\Lambda_K \subset T^*M$, formed by co-oriented hyperplanes tangent to K.

(3) Here is another interesting variant of this construction. Let M be a compact manifold with boundary N. Choose a metric on M and take a smooth function $\rho\colon M \to \mathbb{R}_+$ which is positive on the interior of M and such that $\rho(q) = \operatorname{dist}(q, N)$ for $q \in M$ close to the boundary $N = \partial M$. Let $U \subset T^*M$ be a neighborhood of M in T^*M defined by

$$U = \{(q, p) \in T^*M;\ \|p\|^2 \leq \rho(q)\}.$$

Take the function $H(q, p) = p(\nabla\rho(q))$. Then $d(pdq - dH) = \omega$, and it is straightforward to check that the form $\lambda = (pdq - dH)|_{\partial U}$ is a contact form. In other words, $V = \partial U$ is a contact type hypersurface and the contact manifold $(V, \zeta = \{\lambda = 0\})$ depends only on the smooth manifold M, up to an isotopic to the identity contactomorphism. Then $N \subset V$ is a Legendrian submanifold in V whose Legendrian isotopy class is another smooth invariant of M.

(4) Moreover, note that the involution $\operatorname{inv}(p) = -p$ interacts well with all the above structures. For instance, it induces an anti-symplectic involution of T^*M, a contact, co-orientation reversing involution of the space of co-oriented contact elements ST^*M and of the contact manifold V in (3). In that example the Legendrian manifold N is the fixed point set of inv, while inv induces an involution of the Lagrangian L_K and Legendrian Λ_K in (2).

The author believes that all the above canonical symplectic and contact constructions retain a lot of information about the differential topology of the manifold M, or the pair (M, K). For instance, let Σ be a homotopy n-sphere with an exotic smooth structure.

Are the cotangent bundles $T^*\Sigma$ and T^*S^n symplectomorphic?[6]

Are the spaces of contact elements $ST^*\Sigma$ and ST^*S^n contactomorphic?

Can any gauge-theoretic invariants of a 4-manifold M (and maybe even its smooth type) be recovered from the symplectic and contact information about T^*M and ST^*M?

Note that as smooth manifolds, T^*M and ST^*M depend only on the (tangential) homotopy type of M, and hence all the subtle differential-topological information gets lost this way.

Recently M. Abouzaid and P. Seidel [2] developed a program for proving that certain homotopy spheres do not admit Lagrangian embeddings into T^*S^n. This would answer negatively to the first question for this class of homotopy spheres. In the Legendrian version of example (2) one can try to use the differential algebra of

[6]This question I first heard 18 years ago from G. Mess.

the Legendrian submanifold Λ_K as a tool to detect topological invariants of the knot $K \subset M$. L. Ng successfully used this construction for knots in $\mathbb{R}^3$ and recovered this way a wealth of invariants. For instance, he proved (see [40]) that even the simplest linearized version of this algebra homology already encodes the Alexander polynomial, and also, essentially, the so-called A-polynomial. In particular, this linearized homology distinguishes the unknot – any knot which has the same Ng invariant as the unknot is actually the unknot.

It is interesting to apply construction (4) to a 3- or 4-manifold whose boundary N is a sphere, and then compute the equivariant homology of the differential algebra of the Legendrian submanifold $N \subset V$. It seems plausible (and this is a current joint project of T. Ekholm and the author) that the $\mathbb{Z}/2$-equivariant homology of this algebra carries non-trivial information about the differential topology of the manifold M.

3.3. Other SFT-related development. We briefly mention in this section some recent development relating SFT with hot topics in topology.

Embedded contact homology. As it was already pointed out by M. Gromov in his pioneering paper [23], the holomorphic curve technique is especially powerful in 4-dimensional symplectic topology, because the adjunction formula allows one to control singularities and intersections of holomorphic curves by topological means. The work of C. Taubes [46] emphasized further a special role played by holomorphic curves in 4-dimensional topology. A current project of M. Hutchings, M. Sullivan and C. Taubes attempts to define a contact homology theory in the spirit of SFT, but based on embedded holomorphic curves, see [29] and [47] for partial results in this direction. When fully completed, this theory is expected to provide a unified approach to Ozsváth–Szabó homology theory for 3-manifolds ([42] and also [36]), and to a (yet to be developed) theory of holomorphic curves in near-symplectic manifolds (see [46]).

SFT and string topology. The relation between the topology of the loop space of a manifold M and the Floer homology theory of its cotangent bundle T^*M was first revealed by C. Viterbo [49], and then further developed by D. Salamon and J. Weber [43]. A. Abbondandolo and M. Schwartz [1]) related string topological operations introduced by M. Chas and D. Sullivan [10] with cohomological operations in the Floer homology of T^*M. Based on the fundamental study of Lagrangian intersection Floer homology theory in [20], K. Fukaya [18] observed that the relation between Chas–Sullivan string operations and the theory of holomorphic curves can be used to obtain new restrictions on the topology of Lagrangian submanifolds. In an ongoing project K. Cieliebak and J. Latchev [9] have further developed these ideas, and related the BV_∞-version of contact homology of ST^*M, discussed above in Example 2 of Section 3.1, with Chas–Sullivan string operations in the manifold M.

Relative SFT. Conjecturally, relative SFT is a functor defined on the geometric category of pairs (V, Λ), where V is a contact manifold and Λ its Legendrian submanifold, with morphisms realized by pairs (W, L) of symplectic cobordisms W between

contact manifolds and Lagrangian cobordisms L between Legendrian submanifolds. The target algebraic category should consist of non-commutative analogs of structures considered in Section 1.1. However, in this full form the relative SFT-functor has not yet been constructed. Yu. Chekanov (see also [16]) defined in [11] an associative differential algebra of a Legendrian link in the standard contact $\mathbb{R}^3$. This algebra (already mentioned above in Section 3.2) is a relative analog of the differential contact homology algebra in Example 4 of Section 3.1. Following a sketch in [16] and [15], T. Ekholm, J. Etnyre and M. Sullivan (see [14]) constructed an analogue of Chekanov's algebra in a context of high-dimensional Legendrian submanifolds. Currently there are two promising approaches which may lead to the construction of the full relative version of SFT. One is based on O. Cornea and F. Lalonde [13] theory of cluster Floer homology, and the other one tries to exploit the discussed above relation with string topology along the lines of [18], [20] and [9].

The author benefited a lot discussing the subject of this paper with many people. He is very grateful to all his teachers, collaborators and critical listeners.

References

[1] Abbondandolo, A., Schwarz, M., On the Floer homology of cotangent bundles. *Comm. Pure Appl. Math.* **59** (2006), 254–316.

[2] Abouzaid, M., Seidel, P., private communication.

[3] Arnold, V. I., First steps in symplectic topology. *Russian Math. Surveys* **41** (1986), 1–21.

[4] Biran, P., Cielibak, K., Symplectic topology on subcritical manifolds. *Comment. Math. Helv.* **76** (2001), 712–753.

[5] Bourgeois, F., A Morse-Bott approach to Contact Homology. Ph.D. Dissertation, Stanford University, 2002.

[6] Bourgeois, F., Colin, V., Homologie de contact des variétés toroïdales. *Geom. Topol.* **9** (2005), 299–313.

[7] Bourgeois F., Ekholm, T., Eliashberg, Y., A long exact sequence for Legendrian surgery. Preprint, 2006.

[8] Bourgeois, F., Eliashberg, Y., Hofer, H., Wysocki, K., Zehnder, E., Compactness results in Symplectic Field Theory. *Geom. Topol.* **7** (2003), 799–888.

[9] Cieliebak, K., Latschev, J., Symplectic field theory and string topology. Preprint, 2006.

[10] Chas, M., Sullivan, D., String Topology. arXiv: math.GT/9911159.

[11] Chekanov, Yu., Differential Algebra of Legendrian Links. *Invent. Math.* **150** (2002), 441–483.

[12] Colin, V., Giroux, E., Honda, K., On the coarse classification of tight contact structures. *Proc. Sympos. Pure Math.* **71** (2003), 109–120.

[13] Cornea, O., Lalonde, F., Cluster Homology. arXiv: math.SG/0508345.

[14] Ekholm, T., Etnyre, J., Sullivan, M., The Contact Homology of Legendrian Submanifolds in $\mathbb{R}^{2n+1}$. *J. Differential Geom.* **71** (2005), 177–305.

[15] Eliashberg, Y., Givental, A., Hofer, H., Introduction to Symplectic Field Theory. In *Geom. Funct. Anal.*, Special volume, Part II, (2000), 560–673.

[16] Eliashberg, Y., Invariants in Contact Topology. In *Proceedings of the International Congress of Mathematicians* (Berlin, 1998), Vol. II, Doc. Math., J. DMV, Extra Vol. ICM Berlin, 1998, 327–338.

[17] Eliashberg, Y., Kim, S.-S., Polterovich, L., Geometry of contact transformations and domains: orderability versus squeezing. *Geom. Topol.* **10** (2006), 1635–1748.

[18] Fukaya, K., Application of Floer homology of Lagrangian submanifolds to symplectic topology. In *Morse Theoretic Methods in Nonlinear Analysis and in Symplectic Topology*, Nato Science Series II: Mathematical Physics and Chemistry 217, Springer-Verlag, Dordrecht 2006, 231–276.

[19] Fukaya, K., Ono, K., Arnold conjecture and Gromov-Witten invariant. *Topology* **38** (1999), 933 –1048.

[20] Fukaya, K., Oh, Y.-G., Ohta, H., Ono, K., Lagrangian intersection Floer theory – Anomaly and Obstruction. Preprint, 2000; revised 2006.

[21] Gathmann, A., Absolute and relative Gromov-Witten invariants of very ample hypersurfaces. *Duke Math. J.* **115** (2002), 171–203.

[22] Giroux, E., Une infinité de structures de contact sur une infinité de variétés. *Invent. Math.* **135** (1999), 789–802.

[23] Gromov, M., Pseudo-holomorphic curves in symplectic manifolds. *Invent. Math.* **82** (1985), 307–347.

[24] Hofer, H., Zehnder, E., *Symplectic invariants and Hamiltonian dynamics*. Birkhäuser Adv. Texts Basler Lehrbücher, Birkhäuser, Basel 1994.

[25] Hofer, H., A General Fredholm Theory and Applications. In *Proceedings of the CDM 2004 at Harvard*, to appear.

[26] Hofer, H., Wysocki, K., Zehnder, E., Fredholm Theory and Polyfolds, Part I: Functional analytic methods. Preprint, 2006.

[27] Hofer, H., Pseudo-holomorphic curves and Weinstein conjecture in dimension three. *Invent. Math.* **114** (1993), 515–563.

[28] Honda, K., The topology and geometry of contact structures in dimension three. arXiv: math.GT/0601144.

[29] Hutchings, M., Sullivan, D., Rounding corners of polygons and the embedded contact homology of T^3. *Geom. Topol.* **10** (2006), 169–266.

[30] Ionel, E., Parker, T., Relative Gromov-Witten invariants. *Ann. of Math.* **157** (2003), 45–96.

[31] Katz, E., Formalism for Relative Gromov-Witten Invariants. arXiv math.AG/0507321.

[32] Kontsevich, M., Enumeration of rational curves via torus actions. In *The moduli space of curves*, Progr. Math. 129, Birkhäuser, Boston, MA, 1995, 335–368.

[33] Koert, O. v., Contact homology of Brieskorn manifolds. arXiv: math.SG/0410208.

[34] Li, J., A degeneration formula of GW-invariants. *J. Differential Geom.* **60** (2002), 199–293.

[35] Li, A. M., Ruan, Y.-B., Symplectic surgery and Gromov-Witten invariants of Calabi-Yau 3-folds. *Invent. Math.* **145** (2001), 151–218.

[36] Lipshitz, R., A cylindrical reformulation of Heegaard Floer homology. *Geom. Topol.* **10** (2006), 955–1097.

[37] Lutz, R., Sur la géometrie des structures de contact invariantes. *Ann. Inst. Fourier* (*Grenoble*) **29** (1979), 283–306.

[38] Maulik, D. Pandharipande, R., A topological view of Gromov-Witten theory. *Topology* **45** (2006), 887–918.

[39] McDuff, D., Salamon, D., *J-holomorphic Curves and Symplectic Topology*. Amer. Math. Soc. Colloq. Publ. 52, Amer. Math. Soc., Providence, RI, 2004.

[40] Ng, L., Knot and braid invariants from contact homology I; II. *Geom. Topol.* **9** (2005), 247–297; 1603–1637.

[41] Okounkov, A., Pandharipande, R., Gromov-Witten theory, Hurwitz theory, and completed cycles. *Ann. of Math.* **163** (2006), 517–560.

[42] Ozsváth, P., Szabó, Z., Holomorphic disks and topological invariants for closed three-manifolds. *Ann. of Math.* **159** (2004), 1027–1158.

[43] Salamon, D., Weber J., Floer homology and the heat flow. *Geom. Funct. Anal.* **16** (2006), 1050–1138.

[44] Seidel, P., Symplectic homology as Hochschild homology. arXiv: math.SG/0609037.

[45] Seidel, P., Vanishing cycles and mutation. In *European Congress of Mathematics* (Barcelona, 2000), Vol. II, Progr. Math. 202, Birkhäuser, Basel, 2001, 65–85.

[46] Taubes, C. H., *Seiberg-Witten and Gromov invariants for symplectic 4-manifolds*. First Internat. Press Lecture Ser. 2, International Press, Somerville, MA, 2000.

[47] Taubes, C. H., A compendium of pseudoholomorphic beasts in $\mathbb{R} \times S^1 \times S^2$. *Geom. Topol.* **6** (2002), 657–814.

[48] Ustilovsky, I., Infinitely many contact structures of S^{4m+1}. *Internat. Math. Res. Notices* **14** (1999), 781–791.

[49] Viterbo, C., Functors and computations in Floer cohomology with applications. I. *Geom. Funct. Anal.* **9** (1999), 985–1033; Part II, preprint.

[50] Yau, M.-L., Cylindrical contact homology of subcritical Stein-fillable contact manifolds. *Geom. Topol.* **8** (2004), 1243–1280.

Department of Mathematics, Stanford University, Stanford, CA 94305, U.S.A.
E-mail: eliash@math.stanford.edu

Knots and dynamics

Étienne Ghys

Abstract. The trajectories of a vector field in 3-space can be very entangled; the flow can swirl, spiral, create vortices etc. Periodic orbits define knots whose topology can sometimes be very complicated. In this talk, I will survey some advances in the qualitative and quantitative description of this kind of phenomenon. The first part will be devoted to vorticity, helicity, and asymptotic cycles for flows. The second part will deal with various notions of rotation and spin for surface diffeomorphisms. Finally, I will describe the important example of the geodesic flow on the modular surface, where the linking between geodesics turns out to be related to well-known arithmetical functions.

Mathematics Subject Classification (2000). Primary 37–02; Secondary 57–02.

Keywords. Low-dimensional dynamical systems, periodic orbits, knots and links.

1. Flows

1.1. Vorticity. Let us start with some historical motivation. Consider a perfect incompressible fluid moving inside some bounded domain M in 3-space, with no external forces. At time t, the velocity is described by a divergence free vector field v_t, tangent to the boundary of M, which evolves in time according to the classical Euler equation: $\frac{D}{Dt}v_t$ $(= \frac{\partial}{\partial t}v_t + v_t \cdot \nabla v_t)$ is the (opposite) gradient $-\nabla p$ of the pressure p. Denote by ϕ^t the associated flow: the trajectory of a particle initially located at $x \in M$ is the curve $t \mapsto \phi^t(x)$. The curl $\omega_t = \nabla \times v_t$ is known as the *vorticity* vector field. One of the earliest results in fluid dynamics is due to H. Helmholtz and W. Kelvin:

The vorticity ω_t is merely transported by the flow, i.e. *at any time t, one has* $\omega_t = d\phi^t(\omega_0)$.

This is not difficult to prove: take a closed loop c in M, and compute the time derivative of the circulation of v_t along the loop $c_t = \phi^t(c)$.

$$\begin{aligned}\frac{D}{Dt}\left(\oint_{c_t} v_t \cdot dc_t\right) &= \oint_{c_t}\left(\frac{Dv_t}{Dt}\cdot dc_t + v_t \cdot \frac{Ddc_t}{Dt}\right)\\ &= \oint_{c_t}(-\nabla p \cdot dc_t + v_t \cdot dv_t)\\ &= \int_{c_t} d(-p + \frac{|v_t|^2}{2}) = 0.\end{aligned}$$

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

When c reduces to an infinitesimal loop, Stokes' formula shows that $d\phi^{-t}(\omega_t)$ is indeed constant in time.

A much more conceptual proof is due to V. Arnold who realized that Euler's equation can be seen as the geodesic flow on the infinite dimensional Lie group of volume preserving diffeomorphisms of M, equipped with a natural right invariant metric [3], [5], [55]. This right invariance implies a symmetry group for the equation, which yields Helmoltz–Kelvin's result as a special case of Noether's general principle that symmetries imply conservation laws.

If one can define quantities associated to divergence free vector fields, which are invariant under conjugacies by volume preserving diffeomorphisms, these quantities evaluated on the vorticity ω_t will therefore be *constants of motion*. In this talk, we will discuss some of these invariants, of topological origin.

One consequence seemed remarkable to W. Kelvin. Suppose that at time 0, the vector field v_0 possesses a *vortex ring*: a solid torus $\mathbb{S}^1 \times \overline{\mathbb{D}}$ embedded in M in such a way that ω_0 is tangent to its boundary. Then, this ring will survive as a vortex ring under time evolution, preserving the same topology. This *stability of vortices* was the starting point of the (now forgotten) theory of "vortex atoms", trying to explain elementary "atoms" as vortex rings in ether. Even though this turned out to be physically incorrect, it represents one of the first attempts to use topology in physics. In any case, it motivated P. Tait to start a systematic study of knots, therefore creating *knot theory*. See [26] for a fascinating historical survey of this great moment of interaction between physics and mathematics.

A similar phenomenon appeared much more recently in magneto-hydrodynamics: the dynamics of electrically conducting fluids (like a plasma). If one assumes that the fluid is perfect and has no resistance (ideal MHD), the magnetic (divergence free) vector field is merely transported by the flow of the fluid [21]. For instance, if two periodic orbits of the magnetic field are linked at time $t = 0$, these orbits will survive for ever and remain linked. Again, an invariant of divergence free vector fields yields conservation laws. See for instance [5], [15].

There are many wonderful examples of vector fields in 3-space whose phase portraits exhibit a rich topology and which obviously deserve a topological study. As a typical example, the Lorenz equation also originated from fluid dynamics:

$$\frac{dx}{dt} = 10(y - x); \quad \frac{dy}{dt} = 28x - y - xz; \quad \frac{dz}{dt} = xy - 2.67z.$$

It has been extensively analyzed since the 1980s, and is now a paradigm of a "robust" dynamical system (see in particular the papers of J. Guckenheimer and R. Williams [48], [90], and the book [83]). Note that this vector field is not volume preserving, but admits many invariant measures.

Measure preserving flows do not only arise from physical considerations. Consider for instance a discrete subgroup Γ of $\mathrm{PSL}(2, \mathbb{R})$. The 3-manifold $M = \mathrm{PSL}(2, \mathbb{R}) / \Gamma$ can be endowed with a (Haar)-volume preserving flow ϕ^t given by left translations

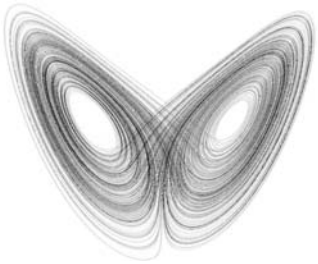


Figure 1. The Lorenz attractor.

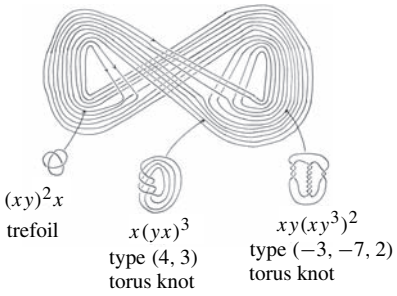


Figure 2. Some periodic orbits [17].

by diagonal matrices

$$\begin{pmatrix} \exp(t) & 0 \\ 0 & \exp(-t) \end{pmatrix}.$$

The dynamics of this kind of flow has been widely investigated in particular because of its strong links with number theory (see for instance [84], [68]). We will come back to this key example in Section 3.

Finally, a huge source of examples of volume preserving vector fields comes from the *suspension* procedure: any area preserving diffeomorphism f of a surface S yields a volume preserving vector field on the 3-manifold obtained by gluing the two boundary components of $S \times [0, 1]$ using f. We will discuss these examples in Section 2.

1.2. Knots and periodic orbits. If a vector field in the 3-sphere or in a domain of $\mathbb{R}^3$ has a periodic orbit, this defines a *knot* whose topology can be used to describe the dynamics. Starting from H. Poincaré one century ago, the quest for periodic orbits has been rewarding[1]. Here is a sample of results.

As for the existence question, after a long search around Seifert's conjecture, K. Kuperberg constructed a jewel. *There exists a nonsingular real analytic vector field in the* 3*-sphere with no periodic orbit* [59] (see also [44]). Note however that such a vector field is highly nongeneric.

H. Hofer showed that *the Reeb vector field of any contact form in the* 3*-sphere has at least one periodic orbit* [50]. H. Hofer, K. Wysocki and E. Zehnder even showed that at least one of these orbits is unknotted [51].

In between these two cases, the volume preserving case seems difficult:

Does there exist a volume preserving *real analytic nonsingular vector field in the* 3*-sphere with no periodic orbit?*

G. Kuperberg constructed examples of C^1 nonsingular aperiodic volume preserving vector fields in the 3-sphere, but they are not C^2 [58]! K. Kuperberg's examples are analytic, but not volume preserving!

[1] "Elles se sont montrées la seule brèche par où nous puissions pénétrer une place jusqu'ici réputée inabordable" (H. Poincaré).

In the opposite direction, there are vector fields in the 3-sphere with plenty of periodic orbits. R. Ghrist constructed another jewel: *an explicit real analytic vector field in the* 3*-sphere whose periodic orbits represent* all (*isotopy classes of*) *knots and links!* [41]. More recently, J. Etnyre and R. Ghrist even constructed an analytic contact form whose Reeb vector field has the same property [28].

Some vector fields have many periodic orbits representing many knots, but not all. J. Birman and R. Williams pioneered the subject and studied in great detail the case of the Lorenz equation. The main tool is Birman–Williams' *template theory*. In Figure 3 (extracted from the original paper [17]), one sees a template: an embedding of a branched surface Σ in $\mathbb{R}^3$, equipped with a semi-flow $(\psi^t)_{t\geq 0}$. The inverse limit $\widehat{\Sigma}$ of this semi-flow is the space of full orbits, *i.e.* curves $c\colon \mathbb{R} \to \Sigma$ such that $\psi^t(c(s)) = c(s+t)$ for all $s \in \mathbb{R}$ and $t \geq 0$. This is a compact space equipped with a flow $(\widehat{\psi}^t)_{(t\in\mathbb{R})}$ and an equivariant projection $\pi : \widehat{\Sigma} \to \Sigma$ (*i.e.* $\pi \circ \widehat{\psi}^t = \psi^t \circ \pi$). One can embed the abstract space $\widehat{\Sigma}$ in a small neighborhood of Σ in $\mathbb{R}^3$ in such a way that $\pi^{-1}(x)$ lies in a small neighborhood of x in $\mathbb{R}^3$ and that $\widehat{\psi}^t$ is induced by some smooth vector field in $\mathbb{R}^3$ preserving $\widehat{\Sigma}$. Any orbit of $\widehat{\psi}^t$ stays close to a full orbit of the original semi-flow ψ^t. This is the *geometric Lorenz attractor* which has been shown recently to be conjugate to the original Lorenz attractor by W. Tucker [86].

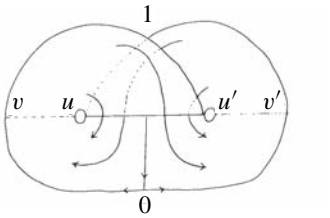


Figure 3. The Lorenz template.

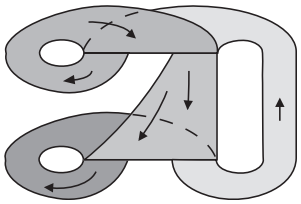


Figure 4. The Ghrist template.

In their seminal paper [17], J. Birman and R. Williams were able to reduce the topological study of the knots and links which are present in the Lorenz vector field to a combinatorial study on the template. For instance, all *Lorenz knots are prime* [91]*, are fibered knots, and have non negative signature*. Hence, Lorenz knots are numerous, but very peculiar. See also [34], [52].

Amazingly, Ghrist's original example of a vector field exhibiting all knots and links in the 3-sphere is "almost" the same as the Lorenz template (Figure 4)! See the beautiful book [42] for more information.

1.3. Asymptotic cycles. Consider a vector field v on a compact manifold M, possibly with boundary, preserving some probability measure μ, and generating a flow ϕ^t. Although there might be no periodic orbit, μ-almost every point x is recurrent (Poincaré's recurrence theorem): there is a sequence $t_n \to \infty$ such that $\phi^{t_n}(x)$ converges to x; the long arc of trajectory from x to $\phi^{t_n}(x)$ is therefore "almost closed". Choose some auxiliary generic Riemannian metric on M and, for any point x and time T, consider the

closed loop $k(T, x)$ obtained by concatenation of the arc of trajectory from x to $\phi^T(x)$ and some shortest geodesic from $\phi^T(x)$ to x. Denote by $[k(T, x)] \in H_1(M, \mathbb{R})$ the homology class of this loop. In the late 1950s, S. Schwartzman observed (in essence) that the limit $\mathcal{S}(\phi; x) = \lim_{T\to\infty}[k(T, x)]/T$ exists in the first homology group $H_1(M, \mathbb{R})$ for μ-almost every point x, and that this limit is independent of the auxiliary metric used to close the arcs [82]. The average value $\mathcal{S}(\phi) = \int_M \mathcal{S}(\phi; x)\, d\mu$ is the *Schwartzman asymptotic cycle* of the flow. Proofs are variations around Birkhoff's ergodic theorem.

As in the classical ergodic theorem, the actual value of $\mathcal{S}(\phi)$ can be computed as a space average. For each point x, consider the trajectory γ_x from x to $\phi^1(x)$ as a *de Rham* 1*-current* on M, whose boundary is the difference between a Dirac mass at $\phi^1(x)$ and a Dirac mass at x. The integral $\int_M \gamma_x\, d\mu(x)$ is a 1-cycle since the integral of boundaries vanishes (thanks to the invariance of μ). The homology class of this Schwartzman cycle is indeed equal to the above limit $\mathcal{S}(\phi)$.

In other words, a measure preserving flow defines a canonical homology class which can be considered as an "infinitely long knot". Schwartzman's point of view has been greatly generalized by D. Sullivan and W. Thurston among others [85].

1.4. Helicity. A typical application of this kind of ideas has been carried out by V. Arnold [4]. Suppose for simplicity that M is the 3-sphere, and that the measure of periodic orbits is zero. Consider two distinct points x_1, x_2 in M, and two times $T_1, T_2 > 0$. The two closed loops $k(T_1, x_1)$ and $k(T_2, x_2)$ are disjoint for almost every choice of x_1, x_2, T_1, T_2 (at least if the metric is generic), and one can consider the asymptotic behavior of their *linking number* $\mathrm{link}(k(T_1, x_1), k(T_2, x_2))$ as T_1 and T_2 tend to infinity. Again, as a consequence of Birkhoff's ergodic theorem, V. Arnold proved that for μ-almost every choice of x_1, x_2, the limit

$$\mathrm{link}(x_1, x_2) = \lim_{T_1,T_2\to\infty} \frac{1}{T_1 T_2}\mathrm{link}(k(T_1, x_1), k(T_2, x_2))$$

exists (see also [23], [36], [88]).

If μ is a volume form, V. Arnold identified the integral

$$\iint_{M\times M} \mathrm{link}(x_1, x_2)\, d\mu(x_1)\, d\mu(x_2)$$

that he called the *asymptotic Hopf invariant* as the *helicity*, which had been introduced previously by J.-J. Moreau [67] and K. Moffatt [62], [63], [64], [65], [66] and that we now recall. Since ϕ^t preserves a volume form μ, the inner product $i_v\mu$ is a *closed* 2-form, hence can be written $d\alpha$ for some 1-form α. The helicity $\mathrm{Hel}(v)$ is equal to the integral of $\alpha \wedge d\alpha$ over M (which is easily seen to be independent of the choice of the primitive α). Note the analogy with the usual definition of Hopf's invariant for maps from the 3-sphere to the 2-sphere. See also [87] for an interesting definition of helicity in the spirit of Witten's approach to Jones' polynomial.

The helicity $\mathrm{Hel}(v)$ defines a quadratic form on the Lie algebra of divergence free vector fields, which is invariant under the adjoint action of smooth volume preserving diffeomorphisms. V. Arnold suggests that $\mathrm{Hel}(v)$ is some "Killing form" for this Lie algebra.

The main open question concerning helicity has been raised by V. Arnold [4]:

Suppose two smooth volume preserving flows are conjugate by some volume preserving homeomorphism (*which is orientation preserving*). *Does it follow that the two flows have the same helicity?*

The qualitative description of helicity as a limit of linking numbers suggests a positive answer, but one should be cautious that a homeomorphism might entangle the small geodesic arcs that were used to close the trajectories. However, we will see in Section 2 that helicity is indeed a topological invariant for flows with a cross section.

Similarly, V. Arnold asked for a *definition of helicity for volume preserving* topological *flows*: this problem seems to be wide open.

1.5. Digression: the Gordian space. For almost every point x, the curve $k(T, x)$ is a knot, *i.e.* has no double point. However, since we are using some auxiliary metric to close the trajectory arc, this knot does depend on the metric. The idea behind the previous constructions is that these knots are "approximately well defined" when T tends to infinity. This suggests looking at *the space of knots, as a rough metric space, à la Gromov.*

Denote by $\mathcal{K}$ the (countable) set of (isotopy classes of) knots in 3-space. There is a natural *Gordian distance* d_{Gordian} on $\mathcal{K}$ that we now define. Given two knots $k_0, k_1 \colon S^1 \hookrightarrow \mathbb{R}^3$, one considers homotopies $(k_t)_{t\in[0,1]} \colon \mathbb{S}^1 \looparrowright \mathbb{R}^3$ which connect the two knots and are such that for each $t \in [0, 1]$, the curve k_t is an immersion with at most one double point, this double point being generic (the two local arcs that intersect have distinct tangents at the intersection). Denote by $D((k_t)_{t\in[0,1]})$ the total number of double points of this family of curves. The Gordian distance between the two knots k_0 and k_1 is the minimum of $D((k_t)_{t\in[0,1]})$ for all such homotopies connecting the knots.

The global geometry of this (discrete) metric space is quite intriguing and probably very intricate. Note for instance that this space is not locally finite (an infinite number of knots can be made trivial by allowing one crossing). We propose two kinds of "dual" questions.

One could try to *prove* (*or disprove*) *that a given metric space* (E, d) *can be embedded quasi-isometrically in* $(\mathcal{K}, d_{\mathrm{Gordian}})$. Recall that a map $u \colon E \to \mathcal{K}$ is a quasi-isometric embedding if there are constants $C, C' > 0$ such that

$$C^{-1}d(x, y) - C' \leq d_{\mathrm{Gordian}}(u(x), u(y)) \leq Cd(x, y) + C'$$

for all x, y. For instance, we proved in [39] that *every Euclidean space can be embedded quasi-isometrically in* $(\mathcal{K}, d_{\mathrm{Gordian}})$ and J. Marché showed that *a countable*

tree such that every vertex has countable valency can also be quasi-isometrically embedded [61].

Can one embed quasi-isometrically the Poincaré disk (*or some higher rank symmetric space*) *in the Gordian space?*

In a second approach, one could try to *find maps* $I\colon (\mathcal{K}, d_{\text{Gordian}}) \to (E, d)$ *which are quasi-Lipschitz:* $d(I(x), I(y)) \leq C d_{\text{Gordian}}(x, y) + C'$ *for some suitable metric space* (E, d). Any such invariant I would be a candidate for an adaptation to vector fields since $I(k(T, x))$ would not be very sensitive to the choice of the auxiliary Riemannian metric, and the ambiguity could disappear in the asymptotic behavior of $I(k(T, x))$ as T tends to infinity. Very few examples of such invariants I seem to be known. The most trivial one is of course the *unknotting number*, Gordian distance to the unknot, but this invariant is hard to compute. Equally hard to compute is the *genus*, *i.e.* the smallest genus of a Seifert surface. A very interesting (and easy to compute) classical invariant is the *signature* of knots $\text{sign}\colon \mathcal{K} \to \mathbb{Z}$ which is 2-Lipschitz for elementary reasons, as well as its twisted versions sign_ω, associated to complex numbers of modulus 1 (see [37], [38], [39], [53]).

In [37], we consider a measure preserving vector field v in a bounded domain M of $\mathbb{R}^3$, and we prove that the limit $\text{sign}(v; x) = \lim_{T\to\infty} \text{sign}(k(T, x))/T^2$ exists for almost every point x. Its average $\text{sign}(v) = \int_M \text{sign}(v; x)\, d\mu(x)$ is the *signature* of the vector field. When v is ergodic with respect to the invariant measure, this signature coincides (surprisingly?) with (one half of) the helicity.

Some other "new" invariants have this Lipschitz property, like the τ invariant of P. Ozsváth and Z. Szabó, and the s invariant of J. Rasmussen. *Do they lead to new dynamical invariants for flows?*

In a similar vein, it would be interesting to get some information on *the rough geometry of the space of* (*homeomorphism types of*) *closed* 3*-manifolds* where the distance between two manifolds is defined as the minimum number of Morse surgeries which are necessary to transform one into the other.

2. Diffeomorphisms of surfaces

Braids are useful to study knots and links mainly because they form a group. In the same way, surface diffeomorphisms are useful to study flows, and also form a group, so that we can use algebraic tools.

If f is a diffeomorphism of a surface S, its *suspension* is obtained by identifying $(x, 0)$ and $(f(x), 1)$ in the cylinder $S \times [0, 1]$. The corresponding manifold S_f is equipped with a flow and a cross section on which the first return map is precisely f. If f preserves a measure or an area form, the suspension preserves a natural measure or volume form. In this section, we describe many invariants measuring some kind of twisting in surface diffeomorphisms.

2.1. The Calabi homomorphism. Denote by $G = \mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \text{area})$ the group of area preserving diffeomorphisms (say of class C^∞) of the closed disk, which are the identity near the boundary. E. Calabi defined a homomorphism

$$\mathcal{C}: \mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \text{area}) \to \mathbb{R}$$

in the following way [19]. Choose a primitive α of the area form in the disk. For each element f of G, the form $f^\star\alpha - \alpha$ is closed and is therefore the differential dH of a unique function H on the disk which is zero near the boundary. Then $\mathcal{C}(f)$ is defined as the integral of H.

There is an intuitive description of Calabi's homomorphism which is due to A. Fathi (unpublished), expressing it as an "average amount of rotation". The group G is contractible. Choose some isotopy $(f_t)_{t\in[0,1]}$ connecting $f_0 = \mathrm{id}$ and $f_1 = f$. If x_1, x_2 are distinct points in the disk, the argument of the nonzero vector $f_t(x_1) - f_t(x_2)$ in $\mathbb{R}^2 \setminus \{(0,0)\}$ rotates by some angle $\mathrm{Angle}(f; x_1, x_2)$ when t goes from 0 to 1 (as a unit for angles, we use the full turn). It is easy to see that this definition is independent of the chosen isotopy. It turns out that

$$\mathcal{C}(f) = \iint_{\overline{\mathbb{D}}\times\overline{\mathbb{D}}} \mathrm{Angle}(f; x_1, x_2)\, dx_1\, dx_2.$$

This interpretation enables a proof of topological invariance for Calabi's invariant [36]:

If f and g are two elements of G which are conjugate by some area preserving homeomorphism *h of the disk, which is the identity near the boundary, then $\mathcal{C}(f) = \mathcal{C}(g)$.*

Indeed, even though h is not assumed to be smooth, one can define the number $\mathrm{Angle}(h; x_1, x_2)$, and it is obvious that

$$\begin{aligned}\mathrm{Angle}(f; x_1, x_2) - \mathrm{Angle}(g; h(x_1), h(x_2))\\ = \mathrm{Angle}(h; x_1, x_2) - \mathrm{Angle}(h; f(x_1), f(x_2)).\end{aligned}$$

Note that $\mathrm{Angle}(h; -, -)$ is a continuous function on the complement of the diagonal in $\overline{\mathbb{D}} \times \overline{\mathbb{D}}$, and could be nonintegrable if h is not smooth (there could be an unbounded local twist). However, the left hand side of the previous equality is bounded since f and g are assumed to be smooth. As for the right hand side, it is easy to see that its integral, which is defined, has to vanish (for instance approximating $\mathrm{Angle}(h; -, -)$ by a sequence of bounded functions). Hence $\mathcal{C}(f) = \mathcal{C}(g)$.

Observe that Calabi's definition extends to more general symplectic manifolds on which the symplectic form is exact. However, *no analogous interpretation as an average rotation is known.*

The suspension of a diffeomorphism f in G defines a flow $\hat{f}$ on a solid torus $\overline{\mathbb{D}} \times \mathbb{S}^1$. If one embeds this solid torus in $\mathbb{R}^3$ *in a standard way*, one can compute the helicity of the suspended flow. In [36], we proved that this helicity is equal to (an explicit multiple of) *Calabi's invariant* of f. (One has to be slightly careful with

definitions in nonsimply connected manifolds, see [36]). This follows rather easily from Fathi's interpretation of Calabi's invariant and Arnold's interpretation of helicity.

As a consequence of the topological invariance of Calabi's number, we get the *topological invariance of helicity for flows which are suspensions of area preserving diffeomorphisms of the disk.* This is a positive answer to a special case of V. Arnold's question mentioned above.

2.2. Some algebraic properties of diffeomorphism groups. The kernel of Calabi's homomorphism $\mathcal{C}$ is a simple group [8], [9]. However, the following fundamental question remains open:

Is the group Homeo($\overline{\mathbb{D}}$, $\partial\overline{\mathbb{D}}$, area) *of area preserving* homeomorphisms *of the disk which are the identity near the boundary a simple group?*

One could try to extend Calabi's homomorphism to this group of homeomorphisms, but the obvious idea of using the integral of Angle$(h; -, -)$ does not work! If one assumes some rather low regularity for the homeomorphisms, one can nevertheless use this idea, as in the quasi-conformal case [49].

Consider now a closed surface S, equipped with some area form ω (say of total area 1), and let $\mathrm{Diff}_0(S, \omega)$ denote the identity component of the group of smooth (say of class C^∞) diffeomorphisms preserving ω. The question of the simplicity of these groups has been settled in the early 1980s (see [7], [9]).

• The group $\mathrm{Diff}_0(\mathbb{S}^2, \text{area})$ of area (and orientation) preserving *diffeomorphisms* of the 2-sphere is a simple group. As above, the question of the simplicity of the group of area preserving *homeomorphisms* of the sphere is open.

• If S is a compact oriented surface of genus at least 2, there is a *flux homomorphism* $\mathcal{F}$: $\mathrm{Diff}_0(S, \text{area}) \to \mathrm{H}_1(S, \mathbb{R}) \simeq \mathbb{R}^{2g}$ whose kernel is simple, as proved by A. Banyaga. The definition of $\mathcal{F}$, due to E. Calabi, is in the spirit of Schwartzman [19]. Let $f \in \mathrm{Diff}_0(S, \text{area})$, and choose some isotopy $(f_t)_{t\in[0,1]}$ connecting the identity to f. For each point $x \in S$, the curve $\gamma_x : t \in [0, 1] \mapsto f_t(x) \in S$ can be considered as a 1-current, and the integral $\int_S \gamma_x \, d\,\text{area}(x)$ is a 1-cycle whose homology class $\mathcal{F}(f)$ is independent of the choice of the isotopy (this follows from the contractibility of $\mathrm{Diff}_0(S, \text{area})$). The kernel of $\mathcal{F}$ consists of *Hamiltonian diffeomorphisms* of S.

• $\mathrm{Diff}_0(\mathbb{T}^2, \text{area})$ is not contractible, but retracts to the subgroup of translations, isomorphic to $\mathbb{T}^2$. It follows that the flux is well defined on the universal cover or, better, is defined as a homomorphism $\mathcal{F}$: $\mathrm{Diff}_0(\mathbb{T}^2, \text{area}) \to \mathrm{H}_1(\mathbb{T}^2, \mathbb{R})/\mathrm{H}_1(\mathbb{T}^2, \mathbb{Z}) \simeq \mathbb{R}^2/\mathbb{Z}^2$. Again, the kernel of the flux is the simple group of Hamiltonian diffeomorphisms of the torus.

Note that these flux homomorphisms can easily be extended to the groups of area preserving *homeomorphisms* which are homotopic to the identity. In particular, *these fluxes are invariant under topological area preserving conjugacy.*

2.3. Dynamical quasi-morphisms. A map F from a group G to $\mathbb{R}$ is a *quasi-morphism* if $|F(g_1g_2) - F(g_1) - F(g_2)|$ is uniformly bounded (see for instance [57]). One says that F is *homogeneous* if $F(g^n) = nF(g)$ for every $n \in \mathbb{Z}$ and $g \in G$. For

every quasi-morphism, the limit $\overline{F}(g) = \lim_{n\to\infty} F(g^n)/n$ exists, and this *homogenization* defines a quasi-morphism such that $|\overline{F} - F|$ is bounded.

Some quasi-morphisms have a dynamical flavor. Let $\widetilde{\mathrm{Homeo}}(\mathbb{S}^1)$ be the universal cover of the group of orientation preserving homeomorphisms of the circle, seen as the group of homeomorphisms of $\mathbb{R}$ commuting with integral translations. The map $f \in \widetilde{\mathrm{Homeo}}(\mathbb{S}^1) \mapsto f(0) \in \mathbb{R}$ is a quasi-morphism whose homogenization is precisely *Poincaré's rotation number* (see for instance [46]).

Given a group G, the existence of quasi-morphisms which are nontrivial (*i.e.* not at a bounded distance from a homomorphism) is related to the second bounded cohomology group of G (see [47]). In turn, this is related to the *commutator length*. If an element g belongs to the first derived group $[G, G]$, it can be written, by definition, as a product of commutators. Let us denote by $\mathrm{comm}(g)$ the smallest length of such a product, and set $\overline{\mathrm{comm}}(g) = \lim_{n\to\infty} \mathrm{comm}(g^n)/n$. It turns out that nontrivial quasi-morphisms exist if and only if $\overline{\mathrm{comm}}$ does not vanish identically on $[G, G]$ [12]. For instance, if Γ is a nonelementary Gromov hyperbolic group, the space of homogeneous quasi-morphisms is infinite dimensional [27]. In the opposite direction, if Γ is a uniform lattice in a simple Lie group of real rank at least 2, then every homogeneous quasi-morphism is trivial: a strong improvement of the now classical vanishing of the first Betti number of such lattices [18].

Since we know all homomorphisms from $\mathrm{Diff}_0(S, \mathrm{area})$ to $\mathbb{R}$ (and they are not so numerous), it is tempting to try to understand nontrivial quasi-morphisms, in the spirit of Poincaré's rotation number, as an attempt to measure some amount of "twisting", or "rotation", or "braiding", contained in some area preserving diffeomorphism. In the next subsections, we will sketch several constructions showing that:

For every closed oriented surface S, the space of homogeneous quasi-morphisms from $\mathrm{Diff}_0(S, \mathrm{area})$ *to* $\mathbb{R}$ *is infinite dimensional* [38].

Hopefully, such invariants could be numerous enough to provide a precise description of the topological dynamics, as in the case of circle homeomorphisms (see for instance [46]). As a motivation, let us recall a (generalization of a) conjecture of R. Zimmer which attracted a lot of attention [93]:

Suppose that a lattice in a simple Lie group of real rank r acts faithfully by homeomorphisms on some compact *manifold M of dimension d. Does it follow that $d \geq r$?*

Some very special cases of this conjecture are known to be true:

• *In dimension $d = 1$*, the conjecture is settled for smooth actions of general lattices [18], [29], [45], and even for groups with Kazdhan's property T [69]. It is open for topological actions of general lattices. It has been proved for topological actions for some specific lattices (typically lattices commensurable to $\mathrm{SL}(n, \mathbb{Z})$ $(n \geq 3)$) [60], [92].

• *In dimension* 2, the conjecture is open in full generality. However, it has been proved by very different techniques for specific lattices (for instance lattices commensurable to $\mathrm{SL}(n, \mathbb{Z})$ with $n \geq 3$) under some additional assumptions: in [32], [33]

for smooth area preserving actions; in [76] for smooth area preserving actions on a closed oriented surface of genus at least 1; in [43] for real analytic actions on closed surfaces different from the torus, and in [79] for the torus case.

• *In higher dimension*, not much is known, unless one adds strong conditions on the action, like assuming that the action preserves a connection [31], or is holomorphic on a Kaehler manifold [20], or for specific lattices acting analytically on 4-manifolds with non zero Euler–Poincaré characteristic [30] etc.

One of the first nontrivial open cases of this conjecture is the following.

Can a uniform *lattice in a simple Lie group of real rank at least* 2 *act faithfully on a compact surface by area preserving diffeomorphisms?*

Suppose a group Γ embeds in $\mathrm{Diff}_0(S, \mathrm{area})$, and let F be a quasi-morphism on $\mathrm{Diff}_0(S, \mathrm{area})$. This produces a quasi-morphism on Γ. For instance, if Γ is a uniform lattice in $\mathrm{SL}(n, \mathbb{R})$ ($n \geq 3$), we already mentioned that such a quasi-morphism has to be trivial. If one could construct a wealth of quasi-morphisms on $\mathrm{Diff}_0(S, \mathrm{area})$ with strong dynamical content, this vanishing result could lead to strong dynamical restrictions on possible actions of lattices on surfaces, by area preserving diffeomorphisms.

The previous comments on quasi-morphisms imply that it might be relevant to search for quasi-morphisms on $\mathrm{Diff}_0(S, \mathrm{area})$. The next few sections will survey some recent progress in this direction.

2.4. Ruelle's rotation numbers. The following construction is due to D. Ruelle (in a higher dimensional symplectic situation [80]), and was placed in the setting of bounded cohomology in [11].

Let f be an element of $\mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area})$, and choose an isotopy $(f_t)_{t\in[0,1]}$ between $f_0 = \mathrm{id}$ and $f_1 = f$. For each point x in the disk, consider the differential $df_t(x)$. Using the natural trivialization of the tangent bundle of the disk, we can consider this differential as a 2×2 matrix, element of $\mathrm{SL}(2, \mathbb{R})$. The first column $v_t(x)$ of $df_t(x)$ is a non zero vector in $\mathbb{R}^2$. Denote by $\mathrm{Angle}(f; x) \in \mathbb{R}$ the variation of the angle of this curve $v_t(x)$ of nonzero vectors when t runs from 0 to 1. This number does not depend on the choice of the isotopy f_t since $\mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area})$ is contractible. Let us define

$$r(f) = \int_{\overline{\mathbb{D}}} \mathrm{Angle}(f; x)\, d\,\mathrm{area}(x).$$

Consider now two elements f and g of $\mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area})$, and choose two isotopies f_t and g_t as above. Using the concatenation of these isotopies, one sees that

$$|\,\mathrm{Angle}(fg; x) - \mathrm{Angle}(g; x) - \mathrm{Angle}(f; g(x))| < 1/2.$$

It follows that r is a quasi-morphism. After homogenization, we get *Ruelle's homogeneous quasi-morphism*

$$\mathcal{R}_{\overline{\mathbb{D}}}(f) = \lim_{n\to+\infty} \frac{1}{n}\, r(f^n).$$

It is not difficult to check on simple examples that $\mathcal{R}_{\overline{\mathbb{D}}}$ is indeed nontrivial. For instance, let $H : \overline{\mathbb{D}} \to \mathbb{R}$ be a (Hamiltonian) function on the disk which vanishes near the boundary, and suppose for simplicity that the critical points of H consist of a finite number of nondegenerate critical points x_i, together with some annular neighborhood of the boundary (on which $H = 0$). Denote by X_H the symplectic gradient of H, and by $H^{(1)}$ the time 1 diffeomorphism defined by X_H. Then

$$\mathcal{R}_{\overline{\mathbb{D}}}(H^{(1)}) = \sum_i \varepsilon_i H(x_i),$$

where $\varepsilon_i = +1$ if x_i is a local extremum and -1 if it is a saddle point (up to some irrelevant multiplicative constant, compare [36]).

This construction can readily be extended to $\mathrm{Diff}_0(\mathbb{T}^2, \text{area})$. Indeed, since the tangent bundle of $\mathbb{T}^2$ is trivial, the differential $df_t(x)$ can still be considered as a matrix. One has to be careful since the isotopy is not unique up to homotopy, but any loop in $\mathrm{Diff}_0(\mathbb{T}^2, \text{area})$ is homotopic to a loop in the translation subgroup and this guarantees that $\mathrm{Angle}(g; x)$ is indeed well defined. Hence, we get a Ruelle quasi-morphism $\mathcal{R}_{\mathbb{T}^2}$ on $\mathrm{Diff}_0(\mathbb{T}^2, \text{area})$.

The case of closed surfaces of higher genus S is more subtle since the tangent bundle is nontrivial! However, one can proceed in the following way [38]. Choose a hyperbolic Riemannian metric on S, and let $f \in \mathrm{Diff}_0(S, \text{area})$. Choose as usual some isotopy f_t from the identity to f, a point x in S, and a unit vector u tangent at x. Consider the curve $df_t(u)$ in the tangent bundle of S, and lift it as a curve $\tilde{df}_t(u)$ to the tangent bundle of the Poincaré disk. Every nonzero tangent vector in the Poincaré disk defines a geodesic ray which converges to some point at infinity, so that one gets a curve in the circle at infinity. We denote by $\mathrm{Angle}(f; u, x)$ the number of full turns made by this curve at infinity. This is independent of the choices of the hyperbolic metric, of the isotopy f_t, and of the lift. Moreover, $\mathrm{Angle}(f; u, x)$ changes by at most 1 when one changes u, keeping f and x fixed, so that one can now define $\mathrm{Angle}(f; x)$ to be the minimum value of $\mathrm{Angle}(f; u, x)$. As before, we now define $r(f) = \int_{\overline{\mathbb{D}}} \mathrm{Angle}(f; x)\, d\,\mathrm{area}(x)$, and finally $\mathcal{R}_S(f)$ by homogenization of r.

The definitions of Ruelle's quasi-morphisms on the disk and the torus use the triviality of the tangent bundle of these surfaces, and the definition on higher genus surfaces uses some kind of "quasi" triviality of the tangent bundle given by the circle at infinity. *We now give a definition in the case of the sphere* [38]. Instead of using the action on tangent vectors, we use the action on *pairs* of tangent vectors. Denote by $T_2(\mathbb{S}^2)$ the space of pairs of nonzero tangent vectors $(\delta x_1, \delta x_2)$ at distinct points x_1, x_2 of the sphere. Observe that the fundamental group of $T_2(\mathbb{S}^2)$ is isomorphic to $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$, so that it does make sense to say that a curve in $T_2(\mathbb{S}^2)$ turns. In order to give a quantitative statement, we identify the sphere with the Riemann sphere $\mathbb{C} \cup \{\infty\}$. The complex differential form

$$\theta = \frac{dx_1 dx_2}{(x_1 - x_2)^2}$$

can be seen as a holomorphic form on the space of pairs of distinct points on $\mathbb{C}\boldsymbol{P}^1$, or as a function on $T_2(\mathbb{S}^2)$. Note that this form is invariant under the projective action of $\mathrm{PGL}(2,\mathbb{C})$, and in particular θ is well defined and nonsingular when x_1 or x_2 is at infinity. As for the geometrical meaning of θ, observe that θ is the cross ratio of the four points "$x_1, x_1+\delta x_1, x_1, x_2+\delta x_2$". Given a curve $c\colon [0,1] \to T_2(\mathbb{S}^2)$, we define $\mathrm{Angle}(c) \in \mathbb{R}$ as the variation of the argument of the complex number $\theta(c)$. This is invariant under homotopies fixing the endpoints.

We can proceed as in the case of the disk. Start with a diffeomorphism f in $\mathrm{Diff}_0(\mathbb{S}^2, \mathrm{area})$. Choose an isotopy $(f_t)_{t\in[0,1]}$ and an element $v = (x_1, \delta x_1; x_2, \delta x_2)$ of $T_2(\mathbb{S}^2)$. We can consider the image v_t of v by the differential of f_t. This gives a curve in $T_2(\mathbb{S}^2)$ and therefore defines some $\mathrm{Angle}(f; x_1, \delta x_1; x_2, \delta x_2)$. Fixing x_1 and x_2 and changing the tangent vectors δx_1, δx_2 changes this rotation angle by at most 2 full turns. We can therefore define $\mathrm{Angle}(f; x_1, x_2)$ as the minimum of $\mathrm{Angle}(f; x_1, \delta x_1; x_2, \delta x_2)$ over all choices of δx_1, δx_2. We now define $r(f)$ as the double integral of $\mathrm{Angle}(f; x_1, x_2)$ and $\mathcal{R}_{\mathbb{S}^2}$ as the homogenization of r. Clearly this defines a homogeneous quasi-morphism on $\mathrm{Diff}_0(\mathbb{S}^2, \mathrm{area})$ that we call *Ruelle's quasi-morphism* on the sphere.

All these Ruelle quasi-morphisms turn out to be topological invariants:

Two elements of $\mathrm{Diff}_0(S, \mathrm{area})$ *which are conjugate by some area preserving homeomorphism, respecting orientation, have the same Ruelle invariants* [38]. *Can one extend their definitions to homeomorphisms?*

Note that one can also define a Ruelle invariant for a nonsingular flow on a 3-manifold with trivialized normal bundle (for example on the 3-sphere). One looks at the rotation action of the differential of the flow on a plane field containing the flow. Similar methods imply its topological invariance.

2.5. Quasi-fluxes, quasi-translation numbers. Let S be a closed surface equipped with a metric with curvature -1. Let $f \in \mathrm{Diff}_0(S, \mathrm{area})$, and choose some isotopy f_t from the identity to f. For each point x in S, consider the unique geodesic arc $\gamma(f; x)$ connecting x and $f(x)$ which is homotopic to the curve $t \mapsto f_t(x)$. If one considers $\gamma(f; x)$ as a 1-current, the integral $t(f) = \int_S \gamma(f; x)\, d\,\mathrm{area}(x)$ is a 1-cycle, and the homogenization $\mathcal{T}(f) = \lim t(f^n)/n$ exists in the space of 1-cycles with the weak topology. Indeed, let f, g denote two elements of $\mathrm{Diff}_0(S, \mathrm{area})$ and, for x in S, denote by $\Delta(x, g(x), fg(x))$ the (immersed) geodesic triangle whose boundary consists of $\gamma(g; x)$, $\gamma(f; g(x))$ and $\gamma(g^{-1}f^{-1}; fg(x))$. For any 1-form α on S, one can compute

$$(t(fg) - t(f) - t(g))(\alpha) = \int_S \left(\int_{\Delta(x, g(x), fg(x))} d\alpha \right) d\,\mathrm{area}(x)$$

which is bounded by π times the supremum of the norm of $d\alpha$ since the areas of triangles in the Poincaré disk are bounded by π. Hence, for every 1-form α, the evaluation $t(f)(\alpha)$ is a quasi-morphism, so that the homogenization is indeed well

defined. In other words, we defined a *quasi-flux with values in the space $Z_1(S)$ of 1-cycles*:

$$\mathcal{T}_S\colon \mathrm{Diff}_0(S, \mathrm{area}) \to Z_1(S).$$

Of course, the homology class of $\mathcal{T}_S$ reduces to Calabi's flux homomorphism. In [38], we proved that the image of $\mathcal{T}_S$ does not lie in a finite dimensional subspace. It is not difficult, using methods from [10], to show that the image of $\mathcal{T}_S$ actually spans a dense subspace of the space of cycles.

Note that this construction obviously extends to area preserving *homeomorphisms*.

2.6. Braiding. We have seen that Calabi's invariant of a diffeomorphism of the disk measures the average rotation on pairs of points. It is natural to look at the action on n-tuples of points [40]. Recall that the *braid group* B_n is the fundamental group of the space $X_n(\overline{\mathbb{D}})$ of unordered n-tuples of distinct points in a disk. We choose n distinct base points $(x_1^0, \ldots, x_n^0)$ in the disk so that a braid can be visualized as a union of n disjoint arcs in $\overline{\mathbb{D}} \times [0, 1]$ transversal to each disk $\overline{\mathbb{D}} \times \{\star\}$ and connecting $\{x_1^0, \ldots, x_n^0\} \times \{0\}$ to $\{x_1^0, \ldots, x_n^0\} \times \{1\}$. By closing these arcs in $\mathbb{R}^3$ in a canonical way outside $\overline{\mathbb{D}} \times [0, 1] \subset \mathbb{R}^3$, we see that every braid β defines a link $\hat{\beta}$ in $\mathbb{R}^3$.

Suppose f is an element of $\mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area})$, and choose some isotopy $(f_t)_{t\in[0,1]}$ connecting $f_0 = \mathrm{id}$ to $f_1 = f$. For every n-tuple of distinct points $(x_1, \ldots, x_n)$ in the disk, we get a curve $(f_t(x_1), \ldots, f_t(x_n))$ in $X_n(\overline{\mathbb{D}})$. Of course, this curve does not define a braid since it is not a loop, but one can easily construct a braid as we did when we closed trajectories of flows by short geodesics. More precisely, for each i we concatenate three curves; the first (resp. third) connects x_i^0 to x_i (resp. $f_1(x_i)$ to x_i^0) in an affine way, and the second is the curve $f_t(x_i)$. These curves now define a closed loop in the space of n-tuples, which is contained in the space of n-tuples of *distinct* points for almost every $(x_1, \ldots, x_n)$. In other words, we get a (pure) braid $\beta(f; x_1, \ldots, x_n)$ in B_n. As before this is independent of the choice of the isotopy, and this provides a *cocycle*, *i.e.* for f, g in $\mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area})$ and almost every n-tuple, one has

$$\beta(fg; x_1, \ldots, x_n) = \beta(g; x_1, \ldots, x_n)\beta(f; g(x_1), \ldots, g(x_n)).$$

Consider now some quasi-morphism $F\colon B_n \to \mathbb{R}$. One can average the value of $F(\beta(f; x_1, \ldots, x_n))$ over the space of n-tuples of distinct points if this is integrable. This strategy is valid for the *signature quasi-morphism*. Indeed, the map which associates to each braid β the signature of its closure $\hat{\beta}$ is a quasi-morphism. This follows from the Lipschitz property of the signature in the Gordian space, that we mentioned earlier (see also [39] for a description of the coboundary of this quasi-morphism). As in the case of Calabi's homomorphism, it is not difficult to check that $\mathrm{sign}(\beta(f; x_1, \ldots, x_n))$ is indeed an integrable function. After integration over the space of n-tuples and homogenization, we get for each $n \geq 2$ a quasi-morphism:

$$\mathrm{Sign}_{n,\overline{\mathbb{D}}}\colon \mathrm{Diff}(\overline{\mathbb{D}}, \partial\overline{\mathbb{D}}, \mathrm{area}) \to \mathbb{R}.$$

Although it is not defined for homeomorphisms, one can also prove its topological invariance.

One can compute explicitly these invariants on simple examples. For instance, let $h\colon [0,1] \to \mathbb{R}$ be a smooth function, which is equal to 0 in a neighborhood of 1, define a Hamiltonian function H on the disk by $H(x) = h(\|x\|^2)$, and consider the associated time 1 diffeomorphism $H^{(1)}$. Then one has

$$\mathrm{Sign}_{n,\overline{\mathbb{D}}}(H^{(1)}) = \int_0^1 h(u)(u^{n-2}+1)\,du$$

(up to some explicit multiplicative constant [38]). Of course, the case $n = 2$ reduces to (a constant multiple of) Calabi's invariant ($B_2 \simeq \mathbb{Z}$). Note that these numbers determine all moments of h and therefore the function h itself. This is a (small) hint that these quasi-morphisms give a good description of the dynamics.

One can proceed in a similar way with diffeomorphisms of the sphere except that we now get a cocycle with values in the pure braid group of the sphere $P_n(\mathbb{S}^2)$ (fundamental group of the space of ordered n-tuples of distinct points on $\mathbb{S}^2$). It is not difficult to express $P_n(\mathbb{S}^2)$ as a central extension of the standard pure braid group $P_{n-1}(\overline{\mathbb{D}})$ (*i.e.* the pure braid group of the disk):

$$0 \to \mathbb{Z} \to P_{n-1}(\overline{\mathbb{D}}) \to P_n(\mathbb{S}^2) \to 1.$$

In this exact sequence, the central $\mathbb{Z}$ is generated by a "double full turn" in SO(2) (which is homotopically trivial in SO(3)). The projection from $P_{n-1}(\overline{\mathbb{D}})$ to $P_n(\mathbb{S}^2)$ consists in "adding a strand at infinity". On $P_{n-1}(\overline{\mathbb{D}})$, we have a nontrivial homomorphism lk_{n-1} onto $\mathbb{Z}$ given by the total linking number of the strands, and a quasi-morphism given by the signature. A suitable linear combination $\mathrm{sign}_{n-1} - c_n\,\mathrm{lk}_{n-1}$ descends to a quasi-morphism on $P_n(\mathbb{S}^2)$ that we simply called the signature of a spherical braid in [38]. As before, we can use these spherical signatures to define quasi-morphisms $\mathrm{Sign}_{n,\mathbb{S}^2}$ on $\mathrm{Diff}_0(\mathbb{S}^2, \mathrm{area})$ which are again topological invariants.

If we think of $\mathbb{S}^2$ as the unit sphere in $\mathbb{R}^3$, and we consider some Hamiltonian function only depending on the third coordinate z through a smooth function $h\colon [-1,1] \to \mathbb{R}$, the invariant of the associated time 1 diffeomorphism $H^{(1)}$ is given by the following formula (up to some irrelevant multiplicative constant and for n even):

$$\mathrm{Sign}_{n,\mathbb{S}^2}(H^{(1)}) = \int_{-1}^{+1} \big((n-1)u^{n-2} - 1\big)\,h(u)\,du.$$

The first interesting case is $n = 4$ and deserves special attention. Let us give some interpretation of $\mathrm{Sign}_{4,\mathbb{S}^2}$ as an "amount of braiding". Given four distinct points z_1, z_2, z_3, z_4 of the sphere, seen as the Riemann sphere, their crossratio $[z_1, z_2, z_3, z_4] = \frac{(z_3-z_1)}{(z_3-z_2)}\frac{(z_4-z_2)}{(z_4-z_1)}$ is in $\overline{\mathbb{C}} \setminus \{0, 1, \infty\}$. The universal cover of a sphere minus three points can be identified with the Poincaré disk $\mathbb{D}$. More precisely, there is a covering map from $\mathbb{D}$ onto $\overline{\mathbb{C}} \setminus \{0, 1, \infty\}$ and the inverse images of points of $\overline{\mathbb{R}} \setminus \{0, 1, \infty\}$ define a tesselation of $\mathbb{D}$ by ideal triangles.

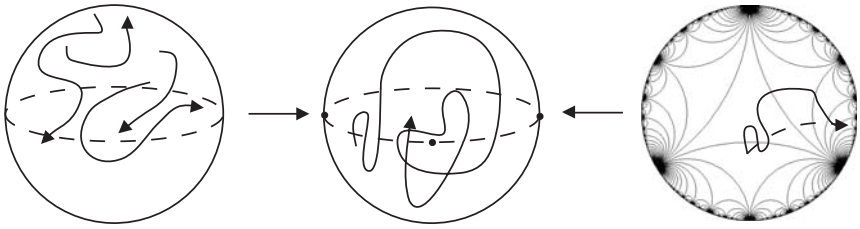


Figure 5. Lifting the crossratio of 4 moving points to the disc.

Let f_t be some isotopy of the sphere from $f_0 = \mathrm{id}$ to some area preserving diffeomorphism f. Choose four distinct points z_1, z_2, z_3, z_4 in the sphere, consider the path $[f_t(z_1), f_t(z_2), f_t(z_3), f_t(z_4)]$ in the sphere minus three points, lift it to the disk, and finally consider the geodesic arc connecting the end points of this lift. Each time this geodesic enters and exits one of the ideal triangles, the exit may be the left or the right side of the triangle, as seen from the entrance side. Counting the number of left exits minus the number of right exits, one gets an integer $t(f; z_1, z_2, z_3, z_4)$ that one can integrate on the space of 4-tuples. After homogenization, one produces a quasi-morphism on $\mathrm{Diff}_0(\mathbb{S}^2, \mathrm{area})$ which turns out to be (a constant multiple of) $\mathrm{Sign}_{4,\mathbb{S}^2}$ [38], [39]. We will meet again this left-right exits count in the last section, in relation with the so-called Rademacher function. See also [13], [14].

2.7. Calabi quasi-morphisms on surfaces: Py's construction. Consider a closed connected surface S equipped with an area form, and denote by $\mathrm{Ham}(S, \mathrm{area})$ the group of Hamiltonian diffeomorphisms of S. Let $D \subset S$ be some open set diffeomorphic to a disk. One can consider the group $\mathrm{Diff}_c(D, \mathrm{area})$ of area preserving diffeomorphisms of D with compact support as a subgroup of $\mathrm{Ham}(S, \mathrm{area})$, extending by the identity outside D. Note that $\mathrm{Ham}(S, \mathrm{area})$ is a simple group, but that $\mathrm{Diff}_c(D, \mathrm{area})$ is not simple since it surjects onto $\mathbb{R}$ by Calabi's homomorphism.

M. Entov and L. Polterovich suggested looking for *Calabi quasi-morphisms,* i.e. *homogeneous quasi-morphisms* $F : \mathrm{Ham}(S, \mathrm{area}) \to \mathbb{R}$ *which restrict to Calabi's homomorphisms on subgroups of the form* $\mathrm{Diff}_c(D, \mathrm{area})$ *if* D *is "small enough"*. They proved the remarkable result that such a Calabi quasi-morphism does exist when S is the sphere (and for many other higher dimensional symplectic manifolds) where "small enough" means "of area less than one half of the area of the sphere". P. Py succeeded with the same task when S is of genus at least 2 and D is any disk [77].

It is unknown if there exists a Calabi quasi-morphism in the case of the torus.[2]

We begin with a description of Py's invariant since it is more elementary and more in the spirit of the previous discussion.

Choose a Riemannian metric with curvature -1 on S, and denote by $p : T^1S \to S$ its unit tangent bundle, seen as a principal SO(2) bundle with a natural connection.

[2] *Note added in proof.* P. Py constructed recently such a quasimorphism: Quasi-morphismes de Calabi et graphe de Reeb sur le tore. C. R. Math. Acad. Sci. Paris 343 (5) (2006), 323–328.

Denote by $\partial/\partial\theta$ the vector field generating the SO(2) action. Note that the map which associates to any vector field X on S its horizontal lift $\overline{X}$ in T^1S is *not* a Lie algebra homomorphism since the connection is not flat. However, if $H\colon S \to \mathbb{R}$ is a Hamiltonian with zero integral, X_H its symplectic gradient, and $\widehat{X_H} = \overline{X_H} + H \circ p \cdot \partial/\partial\theta$, the map $H \mapsto \widehat{X_H}$ is a Lie algebra homomorphism from the Poisson algebra to the Lie algebra of vector fields on T^1S commuting with the SO(2) action. Integrating this homomorphism, we get a homomorphism $f \mapsto \hat{f}$ from $\mathrm{Ham}(S, \text{area})$ (which is simply connected) to the group of diffeomorphisms of T^1S commuting with SO(2). This construction is due to A. Banyaga [7].

Now, consider an element f in $\mathrm{Ham}(S, \text{area})$, written as time 1 of a Hamiltonian isotopy $(f_t)_{t\in[0,1]}$. For each point x in S, and each unit vector v tangent at x, one gets a curve $\hat{f}_t(v)$ in T^1S which can be lifted as a curve in the unit tangent bundle of the disk. As we did before, we can now project this curve to the boundary of the Poincaré disk, so that we get a curve in a circle, giving a certain number of full turns, as t goes from 0 to 1. Fixing f and x, this integer changes by at most 2 when one changes v, so that we can consider its minimum $A(f; x)$. As usually, we can define $\pi(f) = \int_S A(f; x)\, d\,\text{area}(x)$, and homogenize to produce a homogeneous quasi-morphism $\Pi\colon \mathrm{Ham}(S, \text{area}) \to \mathbb{R}$. When the support of f lies in a disk $D \subset S$, the invariant $\Pi(f)$ coincides with the value of Calabi's invariant $\mathcal{C}(f_{|D})$ of the restriction of f to D. In other words, Π *is indeed a Calabi quasi-morphism.*

The computation of this invariant is especially interesting for a diffeomorphism $H^{(1)}$ which is the time 1 of some autonomous Hamiltonian $H\colon S \to \mathbb{R}$ with zero integral. Denote by v the genus of S and assume for simplicity that H is a Morse function with only $2v+2$ critical points $x_1, x_2, \ldots, x_{2v+2}$, such that $H(x_1) < H(x_1) < \cdots < H(x_{2v+2})$. In this case, it turns out that

$$\Pi(H^{(1)}) = \sum_{i=3}^{2v} H(x_i).$$

(up to some irrelevant multiplicative constant). For a general Morse function H with distinct critical values, the invariant $\Pi(H^{(1)})$ is the sum of the values of H on the $2v-2$ saddle points x_i which are such that the fundamental group of the connected component of $H^{-1}(H(x_i))$ containing x_i embeds in the fundamental group of the surface.

2.8. The Entov–Polterovich quasi-morphism. We briefly sketch the construction by M. Entov and L. Polterovich of a *Calabi quasi-morphism on the sphere* (and on many other symplectic manifolds) using elaborate tools from symplectic topology [25]. We will restrict our description to the 2 dimensional case, and refer to [16], [25], [72] for higher dimensional examples.[3]

[3] *Note added in proof.* G. Ben Simon recently proposed a new approach to such Calabi quasimorphisms: The nonlinear Maslov index and the Calabi homomorphism, to appear in Commun. Contemp. Math.; arXiv:math. SG/0604190, 2006.

The free loop space of the 2-sphere is not simply connected. Let us denote by Λ its universal cover, that one can consider as the space of pairs (γ, w) where $\gamma : \mathbb{S}^1 \to \mathbb{S}^2$ is a loop and $w : \overline{\mathbb{D}} \to \mathbb{S}^2$ is a disk with boundary γ, where one identifies (γ, w) with (γ, w') if w and w' are homotopic relative to their boundary.

Fix some time dependent Hamiltonian $H : \mathbb{S}^2 \times \mathbb{S}^1 \to \mathbb{R}$, normalized in such a way that for each time $t \in \mathbb{S}^1$ the integral of $H(-, t)$ over the sphere is zero. Denote by $H^{(1)}$ the Hamiltonian diffeomorphism of the sphere which is the time 1 of the isotopy defined by H. The *action* is a functional defined on Λ by

$$\mathcal{A}_H : (\gamma, w) \in \Lambda \mapsto \int_0^1 H(\gamma(t), t)\, dt - \text{area}(w) \in \mathbb{R}.$$

The critical points of $\mathcal{A}_H$ correspond to the fixed points of $H^{(1)}$. The *Floer homology* is a tool to analyze these critical points. One considers a differential complex freely generated by critical points, whose differential is defined using connecting orbits for the gradient flow of the action functional, which can be interpreted as pseudo-holomorphic cylinders (see [73], [71], [70] for many more "details"). The main point is that the corresponding Floer homology $HF(\Lambda)$ is independent of the choice of the Hamiltonian H. In our case, $HF(\Lambda)$ is some simple quantum deformation of the homology of the sphere.

However, the chain complex used to compute the Floer homology *does* depend on the choice of the Hamiltonian. One defines a *spectral invariant* for a Hamiltonian H: the infimum of the set of $z \in \mathbb{R}$ such that the sub-level $\{\mathcal{A}_H < z\}$ contains a Floer cycle representing the fundamental class in $HF(\Lambda)$. It turns out that this infimum only depends on the Hamiltonian diffeomorphism $H^{(1)}$, and defines therefore a map $ep : \text{Ham}(\mathbb{S}^2) \to \mathbb{R}$. M. Entov and L. Polterovich prove that ep is a quasi-morphism and define their *Calabi quasi-morphism* $\mathcal{E}P$ by homogenization. They also prove that the restrictions of $\mathcal{E}P$ to the subgroups $\text{Diff}_c(D, \text{area})$, where D is a disk with area less than one half of the sphere, coincide with Calabi's homomorphisms. The key point is that such a disk D is *displaceable*, which means that there is a Hamiltonian diffeomorphism h such that $h(D)$ and D are disjoint.

The computation of the Entov–Polterovich Calabi quasi-morphism on time 1 maps of *autonomous* Hamiltonians is very interesting. Assume for simplicity that H is a Morse function on $\mathbb{S}^2$. It is not difficult to see that there is a unique "median" value $z_H \in \mathbb{R}$ such that the complement of one of connected component of $H^{-1}(z_H)$ is a disjoint union of open disks with areas less $1/2$. Then

$$\mathcal{E}P(H^{(1)}) = \int_{\mathbb{S}^2} H\, d\,\text{area} - H(z_H).$$

(The total area of the sphere is normalized to 1). Hence, Entov–Polterovich's invariant is the difference between the "average" and the "median" values of the Hamiltonian.

The uniqueness of such a Calabi quasi-morphism on $\text{Ham}(\mathbb{S}^2, \text{area})$ *is an open question.*

Remarkably, this Entov–Polterovich Calabi quasi-morphism provides a natural example of a *quasi-measure* on the sphere. A quasi-measure μ on a compact space K is a map $\mu\colon C(K) \to \mathbb{R}$ defined on the algebra of continuous functions, which is linear on subalgebras generated by one element, and monotonic ($f \leq g$ implies $\mu(f) \leq \mu(g)$). Such a quasi-measure does not need to be a measure, *i.e.* does not need to be linear (see [1], [24], [56], [81]). If H is a Morse function on $\mathbb{S}^2$, one may set

$$\mu(H) = H(z_H).$$

It is not difficult to check that μ extends to continuous functions on the sphere as a quasi-measure.

3. An example: geodesics on the modular surface

3.1. The unit tangent bundle. The following is well known:

The quotient $M = \mathrm{PSL}(2,\mathbb{R}) / \mathrm{PSL}(2,\mathbb{Z})$ *is homeomorphic to the complement of the trefoil knot in the* 3*-sphere.*

An explicit homeomorphism is given by classical modular functions. Observe that M can be identified with the space of lattices $\Lambda \subset \mathbb{C}$ such that the area of the quotient torus $\mathbb{C}/\Lambda$ is 1. For any lattice Λ, one defines

$$g_2(\Lambda) = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-4}; \quad g_3(\Lambda) = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-6}$$

(see for instance [2]). Conversely, a pair (g_2, g_3) of $\mathbb{C}^2$ such that $\Delta = g_2^3 - 27g_3^2 \neq 0$ determines a unique lattice Λ. Note that the unit sphere $\mathbb{S}^3 \subset \mathbb{C}^2$ intersects the algebraic curve $\{\Delta = 0\}$ along a trefoil knot $\ell \subset \mathbb{S}^3$. Given (g_2, g_3) in $\mathbb{S}^3 \setminus \ell$, the associated lattice is not necessarily of co-area 1, but has a unique "rescaling" of co-area 1. This provides a homeomorphism from the complement of the trefoil knot to the space M.

We have already mentioned that M is equipped with a flow ϕ^t which is given by left translations by diagonal matrices

$$\delta(t) = \begin{pmatrix} \exp(t) & 0 \\ 0 & \exp(-t) \end{pmatrix}.$$

If one thinks of M as a space of lattices in $\mathbb{C} \simeq \mathbb{R}^2$, the action of ϕ^t is simply induced by the action of δ^t on $\mathbb{R}^2$.

The space M can also be seen as the unit tangent bundle of the *modular orbifold* $\Sigma = \mathbb{D}/\mathrm{PSL}(2,\mathbb{Z})$. Indeed, the group of positive isometries of the Poincaré disk $\mathbb{D}$ is isomorphic to $\mathrm{PSL}(2,\mathbb{R})$ and acts freely and transitively on the unit tangent bundle of the disk. From this point of view, ϕ^t *appears as the geodesic flow of the modular orbifold* (rescaled by a factor of 2).

Periodic orbits of this geodesic flow ϕ^t have a long mathematical tradition. Note that an element $P \in \mathrm{PSL}(2,\mathbb{R})$ defines an element in $\mathrm{PSL}(2,\mathbb{R})/\mathrm{PSL}(2,\mathbb{Z})$ which is fixed by ϕ^t if $\delta(t)P = \pm PA$ for some A in $\mathrm{PSL}(2,\mathbb{Z})$, which means that PAP^{-1} is diagonal. One deduces that *there is a natural bijection between periodic orbits of ϕ^t and conjugacy classes of hyperbolic elements in* $\mathrm{PSL}(2,\mathbb{Z})$.

These periodic orbits are also related to indefinite integral quadratic forms in $\mathbb{Z}^2$, or to the structure of ideals in real quadratic fields (Gauss, see for instance [22]). Of course, one could also say that periodic orbits correspond to closed geodesics on $\Sigma = \mathbb{D}/\mathrm{PSL}(2,\mathbb{Z})$, or to free homotopy classes of closed curves in Σ (with the exception of parabolic and elliptic elements).

Summing up, *any hyperbolic matrix $A \in \mathrm{PSL}(2,\mathbb{Z})$ defines a periodic orbit of ϕ^t, hence a knot k_A in the complement of the trefoil knot.*

In this section, we describe the topology of these knots that we call *modular knots*.

3.2. The Rademacher function. Our first task will be to relate the linking number between k_A and the trefoil knot ℓ to a classical arithmetical invariant that we now recall.

The *Dedekind η function* defined for $\Im\tau > 0$ by

$$\eta(\tau) = \exp(i\pi\tau/12)\prod_1^\infty(1-\exp(2i\pi n\tau))$$

"is one of the most famous and well-studied in mathematics" [6]. Its 24th power is a modular form of weight 12, which means that

$$\eta^{24}\left(\frac{a\tau+b}{c\tau+d}\right) = \eta^{24}(\tau)(c\tau+d)^{12}$$

for every matrix $A = \pm\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ in $\mathrm{PSL}(2,\mathbb{Z})$ (see for instance [2]). Since η does not vanish, there is a holomorphic determination of $\log\eta$ defined on the upper half plane. Taking logarithms on both sides of the previous identity, we get

$$24(\log\eta)\left(\frac{a\tau+b}{c\tau+d}\right) = 24(\log\eta)(\tau) + 6\log(-(c\tau+d)^2) + 2i\pi\mathfrak{R}(A)$$

for some function $\mathfrak{R}\colon \mathrm{PSL}(2,\mathbb{Z}) \to \mathbb{Z}$ (the second log in the right hand side is chosen with imaginary part in $(-\pi,\pi)$). The numerical determination of $\mathfrak{R}(A)$ has been a challenge, and turned out to be related to many different topics, in particular number theory, topology, and combinatorics. The inspiring paper by M. Atiyah [6] contains an "omnibus theorem" proving that seven definitions of $\mathfrak{R}$ are equivalent! In [11], we proposed an approach to understand better these coincidences, based on the more or less obvious fact that $\mathfrak{R}$ is a quasi-morphism. It is difficult to choose a name for this "ubiquitous" function: Arnold, Atiyah, Brooks, Dedekind, Dupont, Euler, Guichardet, Hirzebruch, Kashiwara, Leray, Lion, Maslov, Meyer, Rademacher, Souriau, Vergne, Wigner? For simplicity, we will call it the *Rademacher function* [78].

3.3. Linking with the trefoil. We now state a result relating modular knots with the Rademacher function.

For every hyperbolic element A in $\mathrm{PSL}(2,\mathbb{Z})$*, the linking number between the knot k_A and the trefoil knot ℓ is equal to $\mathfrak{R}(A)$, where $\mathfrak{R}$ is the Rademacher function.*

We will give three proofs, connecting $\mathrm{link}(k_A,\ell)$ to three different aspects of this ubiquitous function $\mathfrak{R}$ (thus providing new proofs of the identifications of these various versions of $\mathfrak{R}$). The third proof will give an extra bonus, and will allow a precise description of the topology of modular knots.

Our *first proof* relies on the definition of $\mathfrak{R}$ based on the Dedekind η function. The trefoil knot is a fibered knot. The map $\Delta/|\Delta|\colon \mathbb{S}^3\setminus\ell\to\mathbb{S}^1\subset\mathbb{C}$ is a locally trivial fibration whose fibers are punctured tori. Given a closed oriented curve γ in the complement of the trefoil knot, the linking number $\mathrm{link}(\gamma,\ell)$ is the topological degree of the restriction of Δ to γ (en passant, this defines an orientation for ℓ). Jacobi established a connection between Δ and the Dedekind η function (see [2]). If we denote by $\Delta(\omega_1,\omega_2)$ the $\Delta\,(=g_2^3-27g_3^2)$ invariant of the lattice $\mathbb{Z}\cdot\omega_1+\mathbb{Z}\cdot\omega_2\subset\mathbb{C}$ (with $\Im(\omega_2/\omega_1)>0$), then

$$\Delta(\omega_1,\omega_2)=(2\pi)^{12}\omega_1^{-12}\eta\left(\frac{\omega_2}{\omega_1}\right)^{24}.$$

Consider the periodic orbit of period $T>0$ associated to a hyperbolic element $A=\pm\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ in $\mathrm{PSL}(2,\mathbb{Z})$. One can describe it as a closed curve of lattices $\mathbb{Z}\cdot\delta^t\omega_1+\mathbb{Z}\cdot\delta^t\omega_2$ ($t\in[0,T]$) such that

$$\delta^T(\omega_2)=a\omega_1+b\omega_2;\quad \delta^T(\omega_1)=c\omega_1+d\omega_2.$$

We wish to compute the variation $\mathrm{VarArg}\,\Delta$ of the argument of $\Delta(\delta^t\omega_1,\delta^t\omega_2)$ as t goes from 0 to T. To fix notation, given a curve $q(t)$ in $\mathbb{C}^\star$ ($t\in[0,T]$), written as $\exp(2i\pi\tau(t))$ for some continuous $\tau(t)$, the variation of the argument $\mathrm{VarArg}\,q$ is defined as $\Re(\tau(T)-\tau(0))$. By Jacobi's theorem, $\mathrm{VarArg}\,\Delta(\delta^t\omega_1,\delta^t\omega_2)$ is equal to:

$$-12\,\mathrm{VarArg}(\delta^t\omega_1)+24\frac{1}{2\pi}\Im\left((\log\eta)\left(\frac{\delta^T\omega_2}{\delta^T\omega_1}\right)-(\log\eta)\left(\frac{\omega_2}{\omega_1}\right)\right).$$

Note that $\delta^T\omega_2/\delta^T\omega_1=(a\frac{\omega_2}{\omega_1}+b)/(c\frac{\omega_2}{\omega_1}+d)$, so that we can use the definition of the Rademacher function using the logarithm of η. We get:

$$-12\,\mathrm{VarArg}(\delta^t\omega_1)+\frac{6}{2\pi}\Im\log\Big(-\Big(c\frac{\omega_2}{\omega_1}+d\Big)^2\Big)+\mathfrak{R}(A).$$

Observe that the curve $\delta^t\omega_1$ is contained in a quadrant, so that $\mathrm{VarArg}(\delta^t\omega_1)$ belongs to the interval $(-1/4,1/4)$ and is therefore equal to $\frac{1}{2}\frac{1}{2\pi}\Im\log\big(-\big(\frac{\delta^T\omega_1}{\omega_1}\big)^2\big)$. Recall that log denotes the determination with imaginary part in $(-\pi,+\pi)$. Hence two terms cancel, and we get that $\mathrm{link}(k_A,\ell)$ is indeed equal to $\mathfrak{R}(A)$, as claimed.

3.4. A topological approach. Let us sketch a purely topological computation of $\mathrm{link}(k_A, \ell)$, related to another approach to the Rademacher function.

Consider a compact oriented surface S with fundamental group Γ equipped with a hyperbolic metric. For each element γ in Γ, denote by $\overline{\gamma}$ the closed geodesic which is freely homotopic to γ. This defines a periodic orbit k_γ of the geodesic flow in the unit tangent bundle T^1S of S. If γ_1, γ_2 are in Γ, there is an obvious singular 2-chain $c(\gamma_1, \gamma_2)$ in S whose boundary is $\overline{\gamma_1\gamma_2} - \overline{\gamma_1} - \overline{\gamma_2}$. The obstruction to lift $c(\gamma_1, \gamma_2)$ to a 2-chain in T^1S with boundary $k_{\gamma_1\gamma_2} - k_{\gamma_1} - k_{\gamma_2}$ is an integer $\mathrm{eu}(\gamma_1, \gamma_2) \in \mathbb{Z}$. In other words, one can find a 2-chain in T^1S whose boundary is $k_{\gamma_1\gamma_2} - k_{\gamma_1} - k_{\gamma_2} + \mathrm{eu}(\gamma_1, \gamma_2)\mathbf{f}$ where $\mathbf{f}$ denotes one fiber of T^1S, and which projects on $c(\gamma_1, \gamma_2)$. This defines a 2-cocycle on Γ whose cohomology class is the Euler class of the circle bundle. This construction generalizes to the noncompact modular orbifold $\Sigma = \mathbb{D}/\mathrm{PSL}(2, \mathbb{Z})$ with a little care. One has to adapt the definition of k_A for elliptic and parabolic elements. Since the second rational cohomology of $\mathrm{PSL}(2, \mathbb{Z})$ is trivial, there is a map $\Phi\colon \mathrm{PSL}(2, \mathbb{Z}) \to \mathbb{Q}$ such that $\Phi(\gamma_1\gamma_2) - \Phi(\gamma_1) - \Phi(\gamma_2) = \mathrm{eu}(\gamma_1, \gamma_2)$. Note that this defines uniquely Φ since there is no nontrivial homomorphism from $\mathrm{PSL}(2, \mathbb{Z})$ to $\mathbb{Q}$. It turns out that 6Φ and $\mathfrak{R}$ agree on hyperbolic elements of $\mathrm{PSL}(2, \mathbb{Z})$ (see [6], [11]): this is the topological aspect of $\mathfrak{R}$.

Let us temporarily denote $\mathrm{link}(k_A, \ell)$ by $\lambda(A)$. In order to show that $\lambda(A) = 6\Phi(A)$, it is enough to show that $\lambda(AB) - \lambda(A) - \lambda(B) = 6\,\mathrm{eu}(A, B)$. Let D_A, D_B and D_{AB} be singular disks in $\mathbb{S}^3$ with boundaries k_A, k_B, k_{AB} respectively. By definition of the linking number, the intersection numbers of these disks with ℓ are $\lambda(A)$, $\lambda(B)$, $\lambda(AB)$. Choose a singular surface in $T^1\Sigma \simeq \mathbb{S}^3 \setminus \ell$ with boundary $k_{AB} - k_A - k_B + \mathrm{eu}(A, B)\mathbf{f}$. Glue this surface to D_A, D_B, D_{AB} along the boundaries and cap the result with a disk in $\mathbb{S}^3$ with boundary $\mathrm{eu}(A, B)\mathbf{f}$, with intersection number $6\,\mathrm{eu}(A, B)$ with ℓ. Note that the linking number between ℓ and $\mathbf{f}$ is 6. The resulting boundaryless (singular) surface in $\mathbb{S}^3$ has an intersection number 0 with ℓ since the homology of the sphere is trivial. Putting things together, we get

$$\lambda(AB) - \lambda(A) - \lambda(B) - 6\,\mathrm{eu}(A, B) = 0$$

as required.

3.5. Lorenz and modular knots. We now turn to a dynamical proof which will lead to a topological description of these modular knots.

Recall that a *Lorenz knot* is a knot isotopic to a periodic orbit of the Lorenz differential equation. We will establish a close connection between the Lorenz knots and the modular dynamics:

Isotopy classes of Lorenz knots and modular knots coincide.

We first deform the embedding of $\mathrm{PSL}(2, \mathbb{Z})$ in $\mathrm{PSL}(2, \mathbb{R})$ in order to produce a discrete subgroup of infinite covolume. Recall that $\mathrm{PSL}(2, \mathbb{Z})$ is isomorphic to a free product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ corresponding to the elements of order 2 and 3:

$$U = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad V = \pm\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Consider two points x, y in the Poincaré disk at distance $\rho \geq 0$. This defines a homomorphim $i_\rho\colon \mathrm{PSL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{R})$ sending U to the symmetry with respect to x, and V to the rotation of angle $2\pi/3$ around y. Note that, up to conjugacy, i_ρ only depends on ρ, and that the canonical embedding corresponds to some explicit value ρ_0 (the hyperbolic distance between $\sqrt{-1}$ and $(-1+\sqrt{-3})/2$ in Poincaré' s upper half plane). When $0 < \rho < \rho_0$, the image is a dense subgroup. When $\rho > \rho_0$, the image of i_ρ is a discrete subgroup with infinite covolume: "the cusp has been opened". The quotient Σ_ρ of $\mathbb{D}$ by $i_\rho\,\mathrm{PSL}(2,\mathbb{Z})$ is a noncompact orbifold with a "funnel".

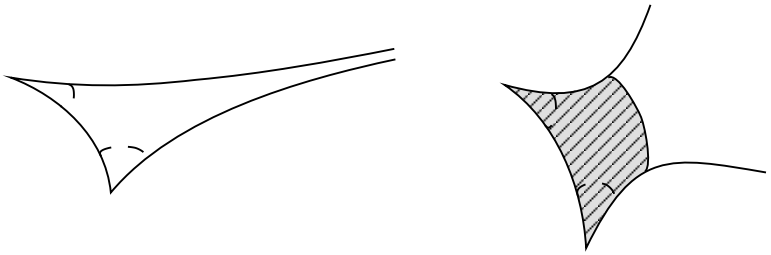


Figure 6. Deforming the modular surface.

Of course, for $\rho \geq \rho_0$, all the quotients $M_\rho = \mathrm{PSL}(2,\mathbb{R})\,/\,i_\rho\,\mathrm{PSL}(2,\mathbb{Z})$ are homeomorphic to the complement of the trefoil knot.

For $\rho > \rho_0$, there is also a flow ϕ_ρ^t on M_ρ given by left translations by diagonal matrices; this is the geodesic flow on the orbifold Σ_ρ of infinite area. The limit set $K_\rho \subset \partial\mathbb{D}$ of the Fuchsian group $i_\rho(\mathrm{PSL}(2,\mathbb{Z}))$ is a Cantor set. The action of $i_\rho(\mathrm{PSL}(2,\mathbb{Z}))$ on the convex hull $\widehat{K_\rho} \subset \mathbb{D}$ is cocompact: the quotient is a compact orbifold $\Sigma_\rho^{\mathrm{conv}} \subset \Sigma_\rho$ with one geodesic boundary component and two singular points. Geodesics in $\mathbb{D}$ whose two limit points are in K_ρ define a compact set Ω_ρ in $T^1\Sigma_\rho = \mathrm{PSL}(2,\mathbb{R})\,/\,i_\rho\,\mathrm{PSL}(2,\mathbb{Z})$ which is invariant under ϕ_ρ^t: this is the nonwandering set. Of course, this invariant set is hyperbolic in the sense of dynamical systems, and the now classical hyperbolic theory of Hadamard–Morse–Anosov–Smale implies that the restrictions of ϕ_ρ^t to Ω_ρ are all equivalent by some homeomorphisms (sending orbits to orbits, respecting their orientations, but of course not respecting time). Periodic orbits of ϕ_ρ^t are contained in Ω_ρ so that, in particular, all flows ϕ_ρ^t in $\mathbb{S}^3 \setminus \ell$ carry the same (isotopy classes of) links (as soon as $\rho > \rho_0$). Clearly, the original flow $\phi^t = \phi_{\rho_0}^t$ is *not* topologically conjugate to ϕ_ρ^t (for $\rho > \rho_0$) since most orbits of ϕ^t are dense, and this is not the case for ϕ_ρ^t ($\rho > \rho_0$). However, when ρ decreases to ρ_0, closed orbits of ϕ_ρ^t, which correspond to closed geodesics in $\Sigma_\rho^{\mathrm{conv}}$, converge to periodic orbits of ϕ^t, with the exception of (the multiples of) the geodesic boundary of $\Sigma_\rho^{\mathrm{conv}}$ which "escapes at infinity in the cusp".

In other words, with the exception of boundary geodesics, corresponding to parabolic elements in $\mathrm{PSL}(2,\mathbb{Z})$, the periodic knots associated to ϕ_ρ^t ($\rho > \rho_0$) are (isotopic to) the modular knots we want to describe. We are therefore led to give a description of the topology of periodic orbits of ϕ_ρ^t ($\rho > \rho_0$).

Look at Figure 7. Consider a geodesic $u\colon \mathbb{R} \to \mathbb{D}$ with endpoints $u(-\infty)$ in the interval I and $u(+\infty)$ in the interval J. It intersects the central hexagon on a compact arc, and the union of these arcs defines an embedding j of $I \times J \times [0,1]$ in $T^1\mathbb{D} \simeq \mathrm{PSL}(2,\mathbb{Z})$. Projecting this parallelepiped in $\mathrm{PSL}(2,\mathbb{R})/i_\rho\,\mathrm{PSL}(2,\mathbb{Z})$, one gets an embedding of $I \times J \times (0,1)$ in $T^1\Sigma_\rho$, but the top and the bottom faces do intersect in the projection. Figure 8 describes the projected parallelepiped $P \subset \mathrm{PSL}(2,\mathbb{R})/i_\rho\,\mathrm{PSL}(2,\mathbb{Z})$, which is a compact manifold with boundary and corners.

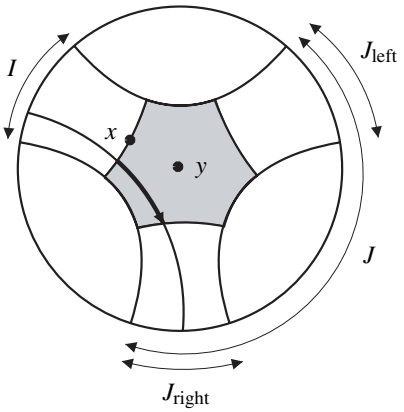


Figure 7. Universal cover of Σ_ρ.

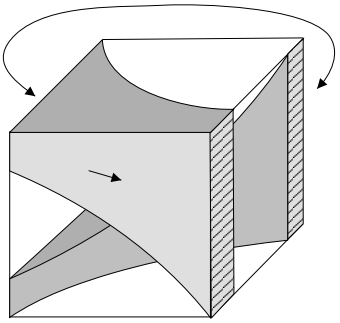


Figure 8. Parallelepiped.

The maximal ϕ_ρ^t invariant set contained in P is of course the nonwandering set Ω_ρ. The restriction of ϕ_ρ^t to Ω_ρ is therefore conjugate to the suspension of a full shift on two symbols {left, right}. A nonwandering geodesic travels in the convex hull $\widehat{K_\rho} \subset \mathbb{D}$, intersects successively $\mathrm{PSL}(2,\mathbb{Z})$-translates of the hexagon, and might exit by the right or left exit, as seen from the entrance side. Any bi-infinite sequence is possible and the sequence characterizes the geodesic.

We now use the main idea of Birman–Williams' template theory. In each of the rectangles $j(I \times J_{\mathrm{left}} \times [0,1])$, and $j(I \times J_{\mathrm{right}} \times [0,1])$, collapse the strong stable manifolds. This produces two rectangles forming a branched manifold which is embedded in $M_\rho \simeq \mathbb{S}^3 \setminus \ell$.

We still have to explain why it is embedded in the way described in Figure 9. Assuming this for a moment, we recognize the Lorenz template, which carries Lorenz knots and links. The process of collapsing the stable manifolds can be done in a smooth way, so that the periodic orbits move by some isotopy (note that a periodic orbit intersects a strong stable manifold in at most one point, so that the collapse does not introduce double points). In other words, the periodic links of ϕ_ρ^t are precisely the periodic links on the template, *i.e.* the Lorenz links.

We briefly explain why the template is indeed embedded as in the picture. We basically have to prove that the two Mickey Mouse ears represent a trivial two com-

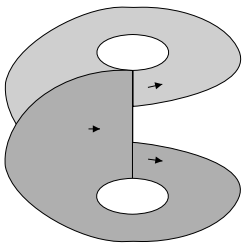


Figure 9. Modular template.

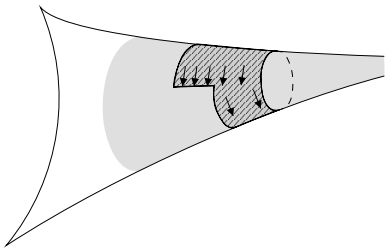


Figure 10. Cusp neighborhood.

ponent link, and that the ears are untwisted. The template consists of two rectangles (symmetric with respect to the involution $v \mapsto -v$ in $T^1\Sigma_\rho$). Each consists of the periodic orbit corresponding to (one orientation of) the boundary of $\Sigma_\rho^{\text{conv}}$ and a piece of the unstable manifold of this orbit. This rectangle projects in $\Sigma_\rho^{\text{conv}}$ as a neighborhood of the boundary curve. In the original modular surface, the rectangle projects as in Figure 10, that one can push as close as one wants towards the cusp.

From the lattice point of view, the first rectangle consists of (rescaled) lattices of the form $\mathbb{Z} + \mathbb{Z} \cdot \tau$ with $\Im\tau > 1$. The Weierstrass invariants (g_2, g_3) of such lattices are given by the classical formulas

$$g_2(q) = \frac{4\pi^4}{3}(1 + 240q + \cdots); \quad g_3(q) = \frac{8\pi^6}{27}(1 - 504q + \cdots)$$

where, as usual, $q = \exp(2i\pi\tau)$. This means that the rectangle sits inside (a rescaling of) the holomorphic disk $q \mapsto (g_2(q), g_3(q)) \in \mathbb{C}^2$ which is an embedding for $|q|$ small enough, and intersects transversally the curve $\{\Delta = 0\}$ since $\Delta(q) = (2\pi)^{12}(q - 24q^2 + \cdots)$ for small q. One concludes first of all that the periodic orbit corresponding to the boundary of the rectangle is unknotted in the sphere since it can be isotoped in this embedded disk. Second of all, it implies that the rectangle is untwisted, since it can also be pushed in an embedded disk. Finally, this implies that the linking number between the boundary curve and the trefoil knot is 1.

The second rectangle is the image of the first one by the symmetry $v \mapsto -v$ (which, from the lattice side, corresponds to one quarter turn). One has to consider now lattices of the form $i(\mathbb{Z} + \mathbb{Z} \cdot \tau)$ with $\Im\tau > 1$ for which the invariants are $g_2(q)$, $-g_3(q)$. The situation is exactly the same as before except that the boundary geodesic is now described with the other orientation, and has a linking number -1 with the trefoil. Moreover, we see that the two boundary periodic orbits define a trivial two component link (since they bound disjoint embedded disks). From this information, one can deduce that the template is indeed embedded as in Figure 9.

This finishes the sketch of proof that (isotopy classes of) Lorenz and modular knots coincide. To be precise, we should be careful with the two boundary trivial knots that we just discussed, which appear on the template, but not in the modular surface (since they were pushed to infinity). However, since some modular knots are

trivial knots, one can state that modular knots and Lorenz knots coincide. Of course, one does not have to restrict to knots, and we could also discuss links as well. The same proof shows that *all modular links are isotopic to Lorenz links and, conversely,* that *a Lorenz link with no exceptional component is isotopic to a modular link.*[4]

Figure 11 represents the simultaneous position of the template and the trefoil knot (easy to prove). *This picture provides a third computation* of $\mathrm{link}(k_A, \ell)$. Indeed, up to conjugacy, any hyperbolic element A in $\mathrm{PSL}(2, \mathbb{Z})$ can be written as a product

$$A = UV^{\varepsilon_1}UV^{\varepsilon_1}\dots UV^{\varepsilon_n}$$

where each ε_i is equal to ± 1. From the dynamical point of view, this means that the corresponding closed geodesic follows the template, turning left or right successively

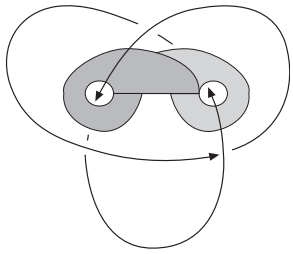


Figure 11. Trefoil wearing modular glasses.

according to the signs of the ε_i's. Since we know that the trefoil knot has linking number $+1$ with the first ear and -1 with the second, we obviously get:

$$\mathrm{link}(k_A, \ell) = \sum_1^n \varepsilon_i .$$

This is a third version of the Rademacher function [6], [11]! The reader will notice some analogy between this left-right count and the signature invariant that we discussed earlier. This is not surprising since it turns out that the spherical braid group $B_4(\mathbb{S}^2)$ is isomorphic to $\mathrm{SL}(2, \mathbb{Z})$, and that the signature is (a multiple of) the Rademacher function [39].

As a corollary of the description of modular knots and links, we get the following:

Modular links are fibered links and have nonnegative signature. Modular knots are prime. The knot k_A is trivial if and only if A is conjugate to a word of the form $(UV)^a(UV^{-1})^b$ $(a, b \geq 1)$.

Indeed, these properties hold for Lorenz knots [17], [91]!

It would be nice to understand those fibrations from the modular side: for instance, can one find some "arithmetical" description of the fibrations of the complements

[4] *Note added in proof.* The reader may look at the AMS feature Column by É. Ghys and J. Leys: Lorenz and modular knots, a visual introduction, AMS Feature Column, November 2006, http://www.ams.org/featurecolumn/archive/lorenz.html

of k_A? In [17], the authors suggest that there could be some "natural limit" to the fibrations of $\mathbb{S}^3 \setminus L$ as L describes all Lorenz links. Maybe the modular point of view will answer this question, and build a bridge between Riemann's ζ function and dynamical ζ functions (see for instance [89]).

Another question would be to give an arithmetical or combinatorial computation of the linking numbers of two knots k_A and k_B as a function of A, B in $\mathrm{PSL}(2,\mathbb{Z})$ (compare [54]). One could also try to understand more sophisticated link invariants for these modular links.

Final remorse. Many interesting questions should have been discussed in this survey, like energy bounds and asymptotic crossing numbers, Hofer metric, global geometry of groups of symplectic diffeomorphisms etc. This is a good excuse to suggest [35], [74], [75] as additional reading!

Acknowledgment. It is a pleasure to thank Jean-Marc Gambaudo for his friendly collaboration.

References

[1] Aarnes, J. F., Quasi-states and quasi-measures. *Adv. Math.* **86** (1) (1991), 41–67.

[2] Apostol, T. M., *Modular functions and Dirichlet series in number theory*. Grad. Texts in Math. 41, Springer-Verlag, New York 1976.

[3] Arnold, V., Sur la géométrie différentielle des groupes de Lie de dimension infinie et ses applications à l'hydrodynamique des fluides parfaits. *Ann. Inst. Fourier* (*Grenoble*) **16** (1) (1966), 319–361.

[4] Arnold, V., The asymptotic Hopf invariant and its applications. *Selecta Math. Soviet.* **5** (4) (1986), 327–345.

[5] Arnold, V. I., and Khesin, B. A., *Topological methods in hydrodynamics*. Appl. Math. Sci. 125, Springer-Verlag, New York 1998.

[6] Atiyah, M., The logarithm of the Dedekind η-function. *Math. Ann.* **278** (1–4) (1987), 335–380.

[7] Banyaga, A., The group of diffeomorphisms preserving a regular contact form. In *Topology and algebra* (Proc. Colloq., Eidgenöss. Techn. Hochsch., Zürich, 1977), Monograph. Enseign. Math. 26, Université Genève, Geneva 1978, 47–53.

[8] Banyaga, A., Sur la structure du groupe des difféomorphismes qui préservent une forme symplectique. *Comment. Math. Helv.* **53** (2) (1978), 174–227.

[9] Banyaga, A., *The structure of classical diffeomorphism groups*, Math. Appl. 400, Kluwer Academic Publishers Group, Dordrecht 1997.

[10] Barge, J., and Ghys, É., Surfaces et cohomologie bornée. *Invent. Math.* **92** (3) (1988), 509–526.

[11] Barge, J., and Ghys, É., Cocycles d'Euler et de Maslov. *Math. Ann.* **294** (2) (1992), 235–265.

[12] Bavard, C., Longueur stable des commutateurs. *Enseign. Math.* (2) **37** (1–2) (1991), 109–150.

[13] Berger, M. A., Third-order braid invariants. *J. Phys. A* **24** (17) (1991), 4027–4036.

[14] Berger, M. A., Hamiltonian dynamics generated by Vassiliev invariants. *J. Phys. A* **34** (7) (2001), 1363–1374.

[15] Berger, M. A., Topological quantities in magnetohydrodynamics. In *Advances in nonlinear dynamos*, Fluid Mech. Astrophys. Geophys. 9, Taylor & Francis, London 2003, 345–374.

[16] Biran, P., Entov, M., and Polterovich, L., Calabi quasimorphisms for the symplectic ball. *Commun. Contemp. Math.* **6** (5) (2004), 793–802.

[17] Birman, J. S., and Williams, R. F., Knotted periodic orbits in dynamical systems. I. Lorenz's equations. *Topology* **22** (1) (1983), 47–82.

[18] Burger, M., and Monod, N., Bounded cohomology of lattices in higher rank Lie groups. *J. Eur. Math. Soc.* (*JEMS*) **1** (2) (1999), 199–235; Erratum: ibid. **1** (3) (1999), 338.

[19] Calabi, E., On the group of automorphisms of a symplectic manifold. In *Problems in analysis*, Lectures at the Sympos. in honor of Salomon Bochner (Princeton University, Princeton, N.J., 1969), Princeton University Press, Princeton, N.J., 1970, 1–26.

[20] Cantat, S., Version kählérienne d'une conjecture de Robert J. Zimmer. *Ann. Sci. École Norm. Sup.* (4) **37** (5) (2004), 759–768.

[21] Chandrasekhar, S., and Woltjer, L., On force-free magnetic fields. *Proc. Nat. Acad. Sci. U.S.A.* **44** (1958), 285–289.

[22] Cohn, H., *Advanced number theory*. Dover Publications Inc., New York 1980; reprint of *A second course in number theory*, Dover Books on Advanced Mathematics, 1962.

[23] Contreras, G., and Iturriaga, R., Average linking numbers. *Ergodic Theory Dynam. Systems* **19** (6) (1999), 1425–1435.

[24] Entov, M., and Polterovich, L., Quasi-states and symplectic intersections. *Comment. Math. Helv*. **81** (2006), 75–99.

[25] Entov, M., and Polterovich, L., Calabi quasimorphism and quantum homology. *Internat. Math. Res. Notices* **2003** (30) (2003), 1635–1676.

[26] Epple, M., Topology, matter, and space. I. Topological notions in 19th-century natural philosophy. *Arch. Hist. Exact Sci.* **52** (4) (1998), 297–392.

[27] Epstein, D. B. A., and Fujiwara, K., The second bounded cohomology of word-hyperbolic groups. *Topology* **36** (6) (1997), 1275–1289.

[28] Etnyre, J., and Ghrist, R., Contact topology and hydrodynamics. III. Knotted orbits. *Trans. Amer. Math. Soc.* **352** (12) (2000), 5781–5794 (electronic).

[29] Farb, B., and Shalen, P., Real-analytic actions of lattices. *Invent. Math.* **135** (2) (1999), 273–296.

[30] Farb, B., and Shalen, P. B., Real-analytic, volume-preserving actions of lattices on 4-manifolds. *C. R. Math. Acad. Sci. Paris* **334** (11) (2002), 1011–1014.

[31] Feres, R., Actions of discrete linear groups and Zimmer's conjecture. *J. Differential Geom.* **42** (3) (1995), 554–576.

[32] Franks, J., and Handel, M., Distortion Elements in Group actions on surfaces. *Duke Math. J.* **131** (3) (2006), 441–468.

[33] Franks, J., and Handel, M., Area preserving group actions on surfaces. *Geom. Topol.* **7** (2003), 757–771 (electronic).

[34] Franks, J. M., Knots, links and symbolic dynamics. *Ann. of Math.* (2) **113** (3) (1981), 529–552.

[35] Gambaudo, J.-M., Knots, flows and fluids. In *Dynamique des difféomorphismes conservatifs des surfaces : un point de vue topologique*, Panoramas et Synthèses 21, Soc. Math. France, Paris 2006, 53–103.

[36] Gambaudo, J.-M., and Ghys, É., Enlacements asymptotiques. *Topology* **36** (6) (1997), 1355–1379.

[37] Gambaudo, J.-M., and Ghys, É., Signature asymptotique d'un champ de vecteurs en dimension 3. *Duke Math. J.* **106** (1) (2001), 41–79.

[38] Gambaudo, J.-M., and Ghys, É., Commutators and diffeomorphisms of surfaces. *Ergodic Theory Dynam. Systems* **24** (5) (2004), 1591–1617.

[39] Gambaudo, J.-M., and Ghys, É., Braids and signatures. *Bull. Soc. Math. France* **133** (4) (2005), 541–579.

[40] Gambaudo, J.-M., and Pécou, E. E., Dynamical cocycles with values in the Artin braid group. *Ergodic Theory Dynam. Systems* **19** (3) (1999), 627–641.

[41] Ghrist, R. W., Flows on S^3 supporting all links as orbits. *Electron. Res. Announc. Amer. Math. Soc.* **1** (2) (1995), 91–97 (electronic).

[42] Ghrist, R. W., Holmes, P. J., and Sullivan, M. C., *Knots and links in three-dimensional flows*. Lecture Notes in Math. 1654, Springer-Verlag, Berlin 1997.

[43] Ghys, É., Sur les groupes engendrés par des difféomorphismes proches de l'identité. *Bol. Soc. Brasil. Mat.* (*N.S.*) **24** (2) (1993), 137–178.

[44] Ghys, É., Construction de champs de vecteurs sans orbite périodique (d'après Krystyna Kuperberg). Séminaire Bourbaki 1993/94, Exposés 775-789; *Astérisque* **227** (785) (1995), 283–307.

[45] Ghys, É., Actions de réseaux sur le cercle. *Invent. Math.* **137** (1) (1999), 199–231.

[46] Ghys, É., Groups acting on the circle. *Enseign. Math.* (2) **47** (3–4) (2001), 329–407.

[47] Gromov, M., Volume and bounded cohomology. *Inst. Hautes Études Sci. Publ. Math.* **56** (1982), 5–99.

[48] Guckenheimer, J., and Williams, R. F., Structural stability of Lorenz attractors. *Inst. Hautes Études Sci. Publ. Math.* **50** (1979), 59–72.

[49] Haïssinsky, P., L'invariant de Calabi pour les homéomorphismes quasiconformes du disque. *C. R. Math. Acad. Sci. Paris* **334** (8) (2002), 635–638.

[50] Hofer, H., Pseudoholomorphic curves in symplectizations with applications to the Weinstein conjecture in dimension three. *Invent. Math.* **114** (3) (1993), 515–563.

[51] Hofer, H., Wysocki, K., and Zehnder, E., Unknotted periodic orbits for Reeb flows on the three-sphere. *Topol. Methods Nonlinear Anal.* **7** (2) (1996), 219–244.

[52] Holmes, P., and Williams, R. F., Knotted periodic orbits in suspensions of Smale's horseshoe: torus knots and bifurcation sequences. *Arch. Rational Mech. Anal.* **90** (2) (1985), 115–194.

[53] Kauffman, L. H., *On knots*. Ann. of Math. Stud. 115, Princeton University Press, Princeton, N.J., 1987.

[54] Kennedy, S. F., Algorithms for the linking numbers of Lorenz and horseshoe knots. *Houston J. Math.* **20** (4) (1994), 705–712.

[55] Khesin, B., Topological fluid dynamics. *Notices Amer. Math. Soc.* **52** (1) (2005), 9–19.

[56] Knudsen, F. F., New topological measures on the torus. *Fund. Math.* **185** (3) (2005), 287–293.

[57] Kotschick, D., What is... a quasi-morphism? *Notices Amer. Math. Soc.* **51** (2) (2004), 208–209.

[58] Kuperberg, G., A volume-preserving counterexample to the Seifert conjecture. *Comment. Math. Helv.* **71** (1) (1996), 70–97.

[59] Kuperberg, K., A smooth counterexample to the Seifert conjecture. *Ann. of Math.* (2) **140** (3) (1994), 723–732.

[60] Lifschitz, L., and Morris, D. W., Isotropic nonarchimedean S-arithmetic groups are not left orderable. *C. R. Math. Acad. Sci. Paris* **339** (6) (2004), 417–420.

[61] Marché, J., Comportement à l'infini du graphe gordien des nœuds. *C. R. Math. Acad. Sci. Paris* **340** (5) (2005), 363–368.

[62] Moffatt, H. K., Topological dynamics of fluids. In *XIth International Congress of Mathematical Physics* (Paris, 1994), International Press, Cambridge, MA, 1995, 465–473.

[63] Moffatt, H. K., Knots and fluid dynamics. In *Ideal knots*, Ser. Knots Everything 19, World Sci. Publishing, River Edge, N.J., 1998, 223–233.

[64] Moffatt, H. K., and Ricca, R. L., Helicity and the Călugăreanu invariant. *Proc. Roy. Soc. London Ser. A* **439** (1992), 411–429.

[65] Moffatt, H. K., and Tsinober, A. (eds.), *Topological fluid mechanics*. Proceedings of the IUTAM Symposium (Cambridge, 1989), Cambridge University Press, Cambridge 1990.

[66] Moffatt, H. K., Zaslavsky, G. M., Comte, P., and Tabor, M. (eds.), *Topological aspects of the dynamics of fluids and plasmas.* University of California at Santa Barbara, 1991, NATO Adv. Sci. Inst. Ser. E Appl. Sci. 218, Kluwer Academic Publishers Group, Dordrecht 1992.

[67] Moreau, J.-J., Constantes d'un îlot tourbillonnaire en fluide parfait barotrope. *C. R. Acad. Sci. Paris* **252** (1961), 2810–2812.

[68] Morris, D. W., *Ratner's theorems on unipotent flows*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2005.

[69] Navas, A., Actions de groupes de Kazhdan sur le cercle. *Ann. Sci. École Norm. Sup.* (4) **35** (5) (2002), 749–758.

[70] Oh, Y.-G., Lectures on Floer theory and spectral invariants of Hamiltonian flows. In *Morse theoretic methods in non-linear analysis and symplectic topology* (University of Montreal, 2004), Nato Sci. Ser. II 217, Springer-Verlag, Dordrecht 2006, 321–416.

[71] Oh, Y.-G., and Fukaya, K., Floer homology in symplectic geometry and mirror symmetry. In *Proceedings of the International Congress of Mathematicians* (Madrid, 2006), Volume II, EMS Publishing House, Zürich 2006, 879–905.

[72] Ostrover, Y., Calabi quasi-morphisms for some non-monotone symplectic manifolds. *Algebr. Geom. Topol.* **6** (2006), 405–434 (electronic).

[73] Piunikhin, S., Salamon, D., and Schwarz, M., Symplectic Floer-Donaldson theory and quantum cohomology. In *Contact and symplectic geometry* (Cambridge, 1994), Publ. Newton Inst. 8, Cambridge University Press, Cambridge 1996, 171–200.

[74] Polterovich, L., Floer homology, dynamics and groups. In *Morse theoretic methods in nonlinear analysis and symplectic topology* (University of Montreal, 2004), Nato Sci. Ser. II 217, Springer-Verlag, Dordrecht 2006, 417–438.

[75] Polterovich, L., *The geometry of the group of symplectic diffeomorphisms*. Lectures in Mathematics ETH Zürich, Birkhäuser, Basel 2001.

[76] Polterovich, L., Growth of maps, distortion in groups and symplectic geometry. *Invent. Math.* **150** (3) (2002), 655–686.

[77] Py, P., Quasi-morphismes et invariant de Calabi. *Ann. Sci. École Norm. Sup*. (4) **39** (2006), 177–195.

[78] Rademacher, H., and Grosswald, E., *Dedekind sums*. The Carus Mathematical Monographs 16, The Mathematical Association of America, Washington, D.C., 1972.

[79] Rebelo, J. C., On nilpotent groups of real analytic diffeomorphisms of the torus. *C. R. Acad. Sci. Paris Sér. I Math.* **331** (4) (2000), 317–322.

[80] Ruelle, D., Rotation numbers for diffeomorphisms and flows. *Ann. Inst. H. Poincaré Phys. Théor.* **42** (1) (1985), 109–115.

[81] Rustad, A. B., The median in multidimensional spaces. *Adv. in Appl. Math.* **33** (2) (2004), 366–396.

[82] Schwartzman, S., Asymptotic cycles. *Ann. of Math.* (2) **66** (1957), 270–284.

[83] Sparrow, C., *The Lorenz equations: bifurcations, chaos, and strange attractors*. Appl. Math. Sci. 41, Springer-Verlag, New York 1982.

[84] Starkov, A. N., *Dynamical systems on homogeneous spaces*. Transl. Math. Monogr. 190, Amer. Math. Soc., Providence, RI, 2000.

[85] Sullivan, D., Cycles for the dynamical study of foliated manifolds and complex manifolds. *Invent. Math.* **36** (1976), 225–255.

[86] Tucker, W., A rigorous ODE solver and Smale's 14th problem. *Found. Comput. Math.* **2** (1) (2002), 53–117.

[87] Verjovsky, A., and Vila Freyer, R. F., The Jones-Witten invariant for flows on a 3-dimensional manifold. *Comm. Math. Phys.* **163** (1) (1994), 73–88.

[88] Vogel, T., On the asymptotic linking number. *Proc. Amer. Math. Soc.* **131** (7) (2003), 2289–2297.

[89] Waddington, S., Asymptotic formulae for Lorenz and horseshoe knots. *Comm. Math. Phys.* **176** (2) (1996), 273–305.

[90] Williams, R. F., The structure of Lorenz attractors. *Inst. Hautes Études Sci. Publ. Math.* **50** (1979), 73–99.

[91] Williams, R. F., Lorenz knots are prime. *Ergodic Theory Dynam. Systems* **4** (1) (1984), 147–163.

[92] Witte, D., Arithmetic groups of higher **Q**-rank cannot act on 1-manifolds. *Proc. Amer. Math. Soc.* **122** (2) (1994), 333–340.

[93] Zimmer, R. J., Actions of semisimple groups and discrete subgroups. *Proceedings of the International Congress of Mathematicians* (Berkeley, Calif., 1986), Vol. 2, Amer. Math. Soc., Providence, R.I., 1987, 1247–1258.

École Normale Supérieure de Lyon, Unité de Mathématiques Pures et Appliquées,
UMR CNRS 5669, 46, Allée d'Italie 69360 Lyon, France
E-mail: etienne.ghys@umpa.ens-lyon.fr

Prime numbers and L-functions

Henryk Iwaniec*

Abstract. The classical memoir by Riemann on the zeta function was motivated by questions about the distribution of prime numbers. But there are important problems concerning prime numbers which cannot be addressed along these lines, for example the representation of primes by polynomials. In this talk I will show a panorama of techniques, which modern analytic number theorists use in the study of prime numbers. Among these are sieve methods. I will explain how the primes are captured by adopting new axioms for sieve theory. I shall also discuss recent progress in traditional questions about primes, such as small gaps, and fundamental ones such as equidistribution in arithmetic progressions. However, my primary objective is to indicate the current directions in Prime Number Theory.

Mathematics Subject Classification (2000). Primary L20; Secondary N05.

Keywords. Prime numbers, L-functions.

1. Introduction

Prime numbers fascinate every mathematician, regardless of her or his field of main interest. They also capture the attention of people in other professions. I recall my popular talk in May 2005 which I delivered to engineers in my native city Elblag in Poland; never before have I heard questions about primes being asked with greater passion. Since our modern daily life is driven by computers, the prime numbers are used to combat hackers. There are offers of huge monetary awards for finding large prime numbers (which are apparently useful in cryptography). Regardless of industrial applications the prime numbers will always play a fundamental role in number theory, because they are to arithmetic as the elementary particles are to matter in physics. Primes form the heart of analytic number theory. Therefore this is a serious subject in which I have been happily working most of my life (and fortunately being paid to do so). When presenting results in this talk I shall often express my views on methods and perspectives concerning prime numbers. The tools for studying primes (like the L-functions, character sums, bilinear forms, sieve methods, combinatorial identities) are as fascinating as the results themselves; thus I will spend considerable time analyzing the strength of these tools and their potential.

This is not a survey of all that is known about prime numbers. There are truly great results concerning prime numbers, which nevertheless do not seem to give insight into

*Supported by NSF grant DMS-03-01168.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

the nature of primes. One of these, in my opinion, is the recent spectacular result of B. Green and T. Tao concerning long arithmetic progressions (you will find a full in-depth account of their result in these Congress Proceedings). My goal here is to cover various areas of analytic number theory which are oriented towards the Theory of Prime Numbers in general. Among them are the very promising developments by D. A. Goldston, J. Pintz and C. Y. Yildirim [32] concerning small gaps between primes. For a recreational style article (nevertheless deep) I refer to E. Bombieri [5], which is also very valuable for many historical details.

2. Primes versus zeros

Traditionally primes are denoted by the letter p. The set of all primes $\mathcal{P} = \{p = 2, 3, 5, 7, 11, 13, 17, 19, \dots\}$ is infinite, and in fact relatively dense. Precisely, the Prime Number Theorem asserts that $\pi(x)$, the number of primes $p \le x$, satisfies the asymptotic formula

$$\pi(x) \sim x(\log x)^{-1}, \quad \text{as } x \to \infty.$$

Hence a novice may argue that basic questions concerning the distribution of primes in various regions or in various sequences of arithmetical interest could be answered with confidence by statistical considerations. Definitely the abundance of primes is useful to support many heuristic arguments. It is often quite easy to predict where the primes are, but rigorous proofs require advanced technology. The point is, we have not yet found any structural mechanism which controls the behavior of prime numbers.

Today, for example, we cannot even determine whether there are infinitely many twin primes, although we expect there are plenty; in particular Hardy and Littlewood conjectured that

$$\pi_2(x) = |\{p \le x : p + 2 \text{ prime}\}| \sim 2cx(\log x)^{-2}$$

where $c = .6601\dots$ is a constant given by a certain product over odd primes. Somewhat related to the twin prime problem is the old question of Goldbach that every even number $N > 2$ is the sum of two primes. We have reason to believe that the number of solutions to the equation $p_1 + p_2 = N$ is quite large (it should be asymptotically $c(N)N(\log N)^{-2}$, where $c(N)$ is a positive number depending on N mildly). Nevertheless we cannot rule out the possibility that sums of two primes may miss a few even numbers. J. Pintz [60] showed that the set of even numbers $N \le X$ which are not represented by sums of two primes is extremely small, its cardinality is bounded by $O(X^{2/3})$. Note that this estimate for the missing Goldbach numbers yields the classical result of I. M. Vinogradov, that every large odd number is a sum of three primes. The meaning of a large number is, of course, subjective. But in the case of sums of primes it has provoked serious investigations. If we are not allowed to use the Grand Riemann Hypothesis then it is still not possible by powerful contemporary

computers to check that the Vinogradov theorem holds for all odd numbers > 5. One needs pure mathematics to cover the middle range (I would call it a theory of midsize numbers). J.-M. Deshouillers and his collaborators [11], [12], [14], have undertaken the task with such goals in mind (also for the Waring problem), so today we are sure that every number > 5 is a sum of at most six primes (due to O. Ramaré [62]).

One may fairly ask the questions, "Why is the Goldbach problem important, or why is it so difficult?" For the first part the answer is; "It is not important per se, it simply arises from our curiosity". I am sure many people would be happy to crack the problem, although this would make no great impact on the foundation of mathematics. For the second part the answer is; "Because it appeals to the multiplicative properties within the additive structure of integers".

Incidentally, a close analog of the twin prime conjecture for Gaussian primes appears in some problems on elliptic curves with complex multiplication (see the short communication in this Congress by Jorge Jiménez Urroz [46]).

The additive group aspects of the integers are quite well understood by means of harmonic analysis. For example, consider the Poisson summation formula

$$\sum_{m\in\mathbb{Z}^r} f(m) = \sum_{n\in\mathbb{Z}^r} \hat{f}(n)$$

where the summations on both sides are over integer vectors of the same dimension. In a slightly more general version of Poisson's formula a sum over a lattice goes to another sum over a dual lattice while the test function changes by the Fourier transform. This can be interpreted as a trace formula for a torus. The very general case of the trace formula for homogeneous spaces when the relevant group action is not commutative may look differently, however it creates similar effects. The group elements no longer correspond to other group elements, but rather they are associated with eigenvalues of a differential operator. Each side of the trace formula serves as a tool to improve our knowledge about the other side. After having established along these lines basic properties of both spectra many applications follow. This is the scheme we practice in analytic number theory (the spectral theory of automorphic forms versus sums of Kloosterman sums being a great example in the modern theory, where non-commutative harmonic analysis rules the game).

The prime numbers resist obeying this treatment unconditionally. Their dual companions are the complex zeros of the zeta function. Historically speaking the zeta function was introduced by Euler as the Dirichlet series

$$\zeta(s) = \sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

so today we call it the Riemann zeta function. Rightly so, because Riemann realized better than anybody previously that the secret of primes is revealed by the zeta function in the whole complex domain $s = \sigma + it$. Besides the above Euler product over primes,

we have the Weierstrass type product over the complex zeros

$$s(1-s)\pi^{-\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)\zeta(s) = e^{-bs}\prod_{\rho}\Big(1-\frac{s}{\rho}\Big)e^{s/\rho}.$$

Combining the Euler product and the Weierstrass product one derives by complex variable integration the so called explicit formula

$$\sum_n \Lambda(n)f(n) = \int_1^\infty \Big(1-\frac{1}{(x-1)x(x+1)}\Big)f(x)dx - \sum_\rho F(\rho).$$

Here $\Lambda(n)$ denotes the von Mangoldt function; it is equal to $\log p$ if n is a power of p and zero elsewhere (actually it was P. Tchebyshev who first realized that counting primes p with the weight $\log p$ is more natural than with the weight one). On the right side F denotes the Mellin transform of f. This formula holds for a large class of test functions, for example, for any f which is smooth, compactly supported on $(1,\infty)$. There are also other variants of the explicit formula and for quite general L-functions.

The explicit formula (which is an involution) would be a natural analog of the trace formula for primes if only we could relate the zeros to eigenvalues of some self-adjoint operator. Hence the celebrated hypothesis of Riemann would follow (which says that all the complex zeros lie on the line $\mathrm{Re}(s)=\frac{1}{2}$, the critical line). However, in spite of many intelligent speculations (especially those inspired by Random Matrix Theory, cf. B. Conrey [9]), this vision remains a dream (Polya–Hilbert). I hope that my talk will show how much has been accomplished concerning prime numbers by roundabout methods. Yes, the RH would do a lot for primes, but, as a plain statement in the absence of intrinsic meaning of the zeros, the hypothesis does not reach far enough. Let me say with satisfaction that researchers in analytic number theory have developed tools which outperform the RH. I shall return to substantiate this claim on several occasions.

A lot is known about the complex zeros $\rho=\beta+i\gamma$ of $\zeta(s)$. There are plenty of them (all are in the critical strip $0<\mathrm{Re}(s)<1$, none on the line $\mathrm{Re}(s)=1$, which fact is equivalent with the PNT), namely

$$N(T) = |\{\rho=\beta+i\gamma;\ |\gamma|\le T\}| = \frac{T}{\pi}\log T + \mathrm{O}(T).$$

Today we know that over 40% of the zeros lay on the critical line (due to B. Conrey [8]), while relatively few are away from the critical line $\mathrm{Re}(s)=\frac{1}{2}$. Quantitative statements of such results are treasures of the zeta-function theory. For example, we have the following Density Theorem

$$\begin{aligned} N(\alpha,T) &= |\{\rho=\beta+i\gamma : \beta>\alpha, |\gamma|\le T\}| \\ &\ll T^{c(1-\alpha)}\log T \end{aligned} \tag{1}$$

for $\frac{1}{2}\le\alpha\le 1$ and $T\ge 2$, where c is an absolute constant.

What is special about this inequality? First it tells us that the chance to find zeros a fixed positive distance from the critical line diminishes rapidly with that distance. The Density Conjecture asserts that the density theorem holds with the exponent $c = 2$. Hence almost all the zeros are close to the critical line (this fact is known unconditionally). The DC is a lovely substitute for the RH in applications for estimating gaps between consecutive primes; it implies (among other things)

$$d_n = p_{n+1} - p_n \ll p_n^{\frac{1}{2}} (\log p_n)^2 \tag{2.1}$$

a result, which can be improved by the Riemann hypothesis only slightly. Therefore it is not surprising that the density theorems received a great attention (in various forms, slightly different than the above). Major developments were carried out from the late sixties to the late eighties. One of many original ideas that emerged from these investigations consists of reducing the counting of zeros to counting large values of special Dirichlet polynomials (naturally called the zero detectors). These values are larger than expected only at the hypothetical zeros off the critical line (they are not good for the zeros on the critical line!), so the phenomenon is rather superficial. In this context H. L. Montgomery [55] laid a foundation for the theory of Dirichlet polynomials. There are deep conjectures in his theory, which are interesting in their own right. Great progress was made by subsequent researchers, especially by M. Huxley [41], M. Jutila [49] and D. R. Heath-Brown [34]. In particular, Huxley succeeded in proving the density theorem with the exponent $c = 12/5$,which produces (after refinements by extra ingredients from sieve methods, see [36]), the asymptotic formula

$$\sum_{x-y<n\le x} \Lambda(n) \sim y, \quad y = x^{\frac{7}{12}}. \tag{2.2}$$

The density conjecture seems to be within reach of current technology, so it is extremely attractive, because it would fully eliminate the need for the Riemann hypothesis for important applications to the distribution of prime numbers (sorry, no prize of one million dollars for a proof of the density conjecture, unless you show that the sets whose cardinalities are being estimated in the density conjecture are all empty).

3. Gaps between primes

If we ask for slightly less than the asymptotic formula (2.2), say we are satisfied instead with a lower bound of the right order of magnitude, then the sieve method becomes a handy addition to the density theorems. Briefly speaking, the sieve offers a decomposition for sums over primes into terms, some of which are non-negative so they can be discarded at will. Of course, after dropping these inconvenient terms the asymptotic formula is lost, but one gains a greater flexibility when dealing with the remaining terms. To these one can apply the theory of Dirichlet polynomials more efficiently due to factorization properties, which are under control to some extent.

Consequently, one gets better bounds for gaps between consecutive primes. The best known unconditional result is

$$d_n = p_{n+1} - p_n \ll p_n^{0.525}$$

due to R. C. Baker, G. Harman and J. Pintz [2]. This is not yet what the RH yields, but it is very close. My point here is that the elementary arguments of combinatorial nature, like the exclusion-inclusion arguments of sieve methods, can be very powerful in conjunction with analytic tools (by exploring features of positivity before applying complex variable analysis).

Suppose the RH is true. Can one get a better bound for d_n if the zeros are regularly distributed on the critical line? Yes, but not very much better. The Pair Correlation Conjecture of Montgomery [56] offers some insight as to how the differences between zeros are distributed, but only with a limited precision in asymptotic formulas for the density function (up to a few main terms). Goldston, Heath-Brown and Julia Mueller explored these conjectures many times ending up with the following result:

$$d_n = \mathrm{o}(\sqrt{p_n}\log p_n).$$

Note that this estimate is just a bit too short to solve the old problem that prime numbers exist between every two consecutive squares. To this end one needs $d_n < 2\sqrt{p_n} + 5$.

Regardless of the zeta-function theory limitation, it is expected that d_n is much smaller. Some heuristic considerations of a probabilistic nature let Cramer [30] conjecture that $d_n \ll (\log n)^2$. While we believe this estimate could be true, one has to be cautious about Cramer's probabilistic model (it is too simplistic, it suffers from having no arithmetical elements). Indeed, Cramer's model suggests that the asymptotic formula (2.2) may hold for extremely short intervals, like $y = (\log x)^A$ with any constant $A > 2$. On the other hand H. Maier [54] showed that the asymptotic formula (2.2) fails even for some larger $y = y(x)$. His idea is quite simple, yet the consequences are very surprising (see more observations in the article by J. Friedlander [21]).

For probabilistic modeling of arithmetic quantities I would suggest to look for inspirations in the Random Matrix Theory. This wonderfully elaborated theory is capable of revealing hidden characteristics, which are impossible to find by naive straightforward thinking. Although the Random Matrix Theory is primarily analytic in essence, mysteriously enough every asymptotic formula predicted by the RMT so far seems to be correct, including the arithmetical factors. I do not completely comprehend why the two worlds of numbers, analytic and arithmetic in nature, manifest their co-existence here? Many interesting relations have been discovered and explained in this framework by B. Conrey, D. Farmer and others; see how some of these are articulated by B. Conrey [9].

Next question is; "How large can the gaps be between primes?" By the PNT it follows that $p_n \sim n\log n$, so d_n is about $\log n$ on average. More precisely we know that $d_n/\log n$ behaves like a random variable with Poisson distribution, this means

$$|\{n \le x;\, d_n > t\log n\}| \sim e^{-t}x \quad \text{for } t > 0, \text{ as } x \to \infty.$$

However, gaps larger than the average size do occur occasionally. Erdös and Rankin showed that infinitely often d_n can be as large as

$$c(\log n)(\log\log n)(\log\log\log\log n)(\log\log\log n)^{-2},$$

where c is a positive constant. (Once in a while D. Goldston asks, "What are the last words of a drowning analytic number theorist?" and he is still saying, "logloglog".)

Of course, for small gaps we expect to have $d_n = 2$ infinitely often (the twin prime conjecture). The problem of finding small gaps between primes sparked a great deal of interest (see Bombieri–Davenport [7], Huxley [42] and Maier [54]). Just a year ago the world was stunned by the following result:

$$\liminf_n \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

This is a magnificent achievement of D. A. Goldston, J. Pintz and C. Y. Yildirim [32] after over a decade of working on the problem by Goldston and Yildirim. They also showed that

$$\liminf_n \frac{p_{n+1} - p_n}{\sqrt{\log n}(\log\log n)^2} < \infty.$$

Their work represents a significant contribution to sieve methods. We shall return to this subject in Section 6.

4. Primes in arithmetic progressions

Primes in arithmetic progressions are building blocks for basic constructions in analytic number theory. Let $q > 1$ and $(a, q) = 1$. After Dirichlet we know that there are infinitely many primes $p \equiv a \pmod q$. His introduction of multiplicative characters $\chi \pmod q$ and L-functions

$$L(s, \chi) = \sum_n \chi(n) n^{-s} \tag{2}$$

$$= \prod_p (1 - \chi(p) p^{-s})^{-1} \tag{3}$$

are commonly considered as the beginning of analytic number theory (should Euler be the father?). The historical memoir of Riemann on the zeta-function has been naturally extended to the family of Dirichlet L-functions including the Riemann hypothesis. The so-called Grand Riemann Hypothesis asserts that all the zeros of $L(s, \chi)$ in the critical strip $0 < \mathrm{Re}(s) < 1$ are on the critical line $\mathrm{Re}(s) = \frac{1}{2}$; it is equivalent to the

asymptotic formula

$$\psi(x; q, a) = \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \Lambda(n)$$
$$= \frac{x}{\phi(q)} + \mathrm{O}(\sqrt{x}(\log x)^2)$$

where the implied constant is absolute. Note that the above formula is meaningful (i.e. its main term exceeds the error term) for relatively large modulus q in terms of x, namely, it holds uniformly in $q \ll \sqrt{x}(\log x)^{-3}$.

In analytic number theory, the uniformity of asymptotic formulas, or inequalities, with respect to the involved parameters, is the key issue, because these parameters constitute structural components for connecting distinct sets of numbers. We shall see this machine in action when producing primes in special sparse sequences by sieve methods. In this regard the Grand Riemann Hypothesis would be most useful. The great virtue of GRH for all natural L-functions (like L-functions on ideals in number fields, L-functions of Galois representations, L-functions of elliptic curves, and ultimately the automorphic L-functions of any degree) is its ability to yield strong and neat estimates of great uniformity with respect to the relevant invariants. For industrial applications we should use GRH without hesitation. But for a critical researcher the prospect of obtaining extra strong results might deter him from attacking the GRH. My point is that current ideas (in analytic number theory) are not capable, in fact not even aimed to penetrate the subject so deeply. By design many methods are successful in breaking only through the surface of the problem, which is critical for its solution. For example one does not need the full strength of the Lindelöf hypothesis for L-functions in terms of the conductor (another consequence of the GRH), but a small improvement in the convexity bound is just sufficient for proving major results. H. Weyl and D. Burgess get credit for establishing the first subconvexity bounds for the Riemann zeta function in the s-aspect, and for the Dirichlet L-functions in the conductor aspect, respectively. Do not expect that a small improvement of a convexity bound is possible by squeezing the functional equation arguments; in every case it is the state-of-the-art technique which crashes the barrier. I refer to the full in-depth presentation by P. Michel in the Number Theory Section of this Congress for other examples and for many original ideas with surprising applications.

We now return to primes in arithmetic progressions. It is known that $L(s, \chi)$, for any character χ of conductor q, does not vanish in the region

$$\sigma > 1 - \frac{c}{\log q(|t| + 1)}, \quad s = \sigma + it \tag{4.1}$$

where c is a positive absolute constant, with at most one exception. The exceptional character is real and the exceptional zero is also real and simple (due to E. Landau [52]). The problems of the exceptional character are fascinating, so we shall speak more about these issues in a separate section. By the above zero-free region one

derives the unconditional formula

$$\psi(x;q,a) = \frac{x}{\phi(q)} - \frac{\chi(a)}{\phi(q)}\frac{x^{\beta}}{\beta} + \mathrm{O}(x\,\exp(-b\sqrt{\log x})) \tag{4.2}$$

where χ is the exceptional character, β is the exceptional zero, so

$$1 - \frac{c}{\log q} < \beta < 1, \tag{4.3}$$

and b is a positive absolute constant. Here on the right-hand side, the second term disappears if the exceptional character does not exist. However, if the exceptional character does exist with the exceptional zero very close to one, then it distorts the asymptotic for $\psi(x;q,a)$ dramatically. Depending on the value $\chi(a) = -1, 1$, we find that the asymptotic number of prime $p \equiv a \pmod q$, either doubles or reduces to nothing, respectively. Of course, we do not believe in this phenomenon, yet we cannot rule it out. In fact there are many situations where the existence of the exceptional character would be welcome.

Even if the GRH is true the primes are not very uniformly distributed among various residue classes. In 1853 P. Tchebyshev noticed that the class 3 (mod 4) has a tendency of representing more primes than the class 1 (mod 4). Of course, the bias must not be large, because of the uniformity guaranteed by the GRH. A hundred years later S. Knapowski and P. Turan [51] succeeded in justifying this observation rigorously creating the so called Comparative Prime Number Theory, which is based on another great invention, the Turan Power Sum Method. Their results stimulated further investigations by several authors, who discovered other phenomena. M. Rubinstein and P. Sarnak [63] gave a quite precise characterization of those moduli and the residue classes for which the Tchebyshev bias is present. They also provided the measures which describe quite precisely the distribution of the error terms

$$E(x;q,a) = \psi(x;q,a) - \frac{x}{\phi(q)}$$

simultaneously with respect to specific collections of the classes $a \pmod q$. Better yet, their work illuminates the interface where primes and zeros communicate with each other.

While we may have to wait a long time for a proof of the GRH, its main consequence is already established in practical terms, that is to say, the error term $E(x;q,a)$ is showed to be relatively small on average with respect to the modulus q over the same range which the GRH covers. Indeed we know that

$$\sum_{\substack{q\le Q\\(q,a)=1}} \lambda(q,a)E(x;q,q) \ll x(\log x)^{-A} \tag{4.4}$$

where $\lambda(q,a)$ are arbitrary real numbers absolutely bounded, A is any positive number and $Q = \sqrt{x}(\log x)^{-B}$, with B depending only on A. Here the quality of the

bound is not impressive, we save only a factor $(\log x)^A$ relative to the trivial bound, which nevertheless is sufficient for most applications. More important is that we have here useful estimates for quite large moduli. Because the coefficients $\lambda(q,a)$ are arbitrary we can sum the error terms $E(x;q,a)$ with absolute values, so no cancellation occurs. In this format the above estimate was established in 1965 independently by E. Bombieri [3] and A. I. Vinogradov [67] (actually the original statement of Bombieri was slightly more refined). This was a great triumph of the then new technology, the large sieve. The Bombieri–Vinogradov theorem turned out to be particularly useful in applications of combinatorial sieve methods, having the effect of replacing the GRH.

Yet, neither the GRH nor the Bombieri–Vinogradov theorems are the last words about primes in arithmetic progressions. We expect that (4.4) holds with $Q = x^{1-\varepsilon}$, or even better that each error term satisfy

$$E(x;q,a) \ll x^{\varepsilon}(x/q)^{\frac{1}{2}}, \quad \text{if } 1 \le q \le x.$$

If one attempts to prove the latter estimate by an appeal to the explicit formula, then the task boils down to having extremely regular distribution of zeros of L-functions on the critical line (mostly the zeros near the central point $s = \frac{1}{2}$ play a role). However, nothing like that is known, and nobody so far has had the courage to formulate the required distribution. Let me say that the analysis based on the n-level correlation theory (cf. Z. Rudnick and P. Sarnak [64]) does seem to hint for the problem in question, however not enough. Nevertheless, an important progress was made in the eighties by working directly with primes. We know today (see Bombieri–Friedlander–Iwaniec [6] and Fouvry [16]) that (4.4) holds with $Q = x^{\frac{4}{7}-\varepsilon}$, provided a is fixed and the coefficients $\lambda(q) = \lambda(q,a)$ are well factorable (this means that for any factorization $Q_1Q_2 = Q$ with $Q_1 > 1$, $Q_2 > 1$ one can represent the coefficients $\lambda(q)$ as a convolution of two new coefficients supported on numbers less than Q_1 and Q_2, respectively). These coefficients are almost as good as any other in applications, especially in conjunction with sieve methods.

When the modulus q is close to x there are not sufficiently many primes $p \le x$, to warrant the equidistribution among the residue classes $a(\mathrm{mod}q)$. J. Friedlander and A. Granville [22], building upon an idea of H. Maier, have shown that for every B the asymptotic formula $\psi(x;q,a) \sim x/\phi(q)$ cannot hold uniformly in the range $q \le x(\log x)^{-B}$. Even if we consider averaging over the moduli the situation does not improve, for they have shown that the Bombieri–Vinogradov estimate (4.4) cannot hold for $Q = x(\log x)^{-B}$, where A, B are arbitrary positive constants.

Primes in arithmetic progressions appear in various contexts, and not just as tools for shaping other things. For example the arithmetic in a number field (a finite algebraic extension of the field of rational numbers) requires a good knowledge of prime ideals in the ring of algebraic integers of that field. One can find all of them by factoring the rational primes p. If the extension is abelian the kind of factorization depends almost exclusively on the residue class of p modulo the conductor of the field. Clearly, a good question is; "What is the first prime ideal in a number field

(precisely the non-rational prime ideal of the lowest norm), that is to say the smallest "elementary particle" of the field?"

In particular we have the question; "What is the least prime number in an arithmetic progression?", say $p_{\min}(q, a) \equiv a \pmod q$. The best known asymptotic formula (the Siegel–Walfisz theorem)

$$\psi(x; q, a) = \frac{x}{\phi(q)} + \mathrm{O}(x(\log x)^{-A}) \tag{4.5}$$

provides a poor estimate, while the GRH would tell us that $p_{\min}(q, a) \ll q^{2+\varepsilon}$. One of the deepest results in the Prime Number Theory is the estimation of Yu. V. Linnik

$$p_{\min}(q, a) \ll q^L,$$

where L and the implied constant are absolute, effectively computable. The original arguments of Linnik, and later refinements by several authors (cf. [39]), are gems of the theory. Among many strong ingredients one finds the repulsion property of the exceptional real zero of a real character L-function. It is a fascinating subject to which we give more attention in Section 6. Recently J. Friedlander and H. Iwaniec (see [45]) developed a different approach to the Linnik theorem avoiding many of these ingredients; our method does not essentially appeal to the zeros of L-functions but instead it applies a lot of sieve arguments. The best known Linnik constant $L = 5.5$ is due to D. R. Heath-Brown [37], while it is expected that $L = 1 + \varepsilon$ should be fine. Note that the statement $p_{\min}(q, a) = \mathrm{o}(q \log q)$ would be false! For more delicate results and fine speculations we refer to A. Granville [29].

Because the uniformity in estimates for $\pi(x; q, a)$ with respect to q is vital in practice, there are many interesting results which are not perfect, but non-trivial for very large moduli. In this regard the sieve methods have an advantage over the analytic methods. First, using the elementary Brun sieve, Titchmarsh showed that $\pi(x; q, a) < cx/\phi(q) \log(x/q)$ for all $q < x$, where the constant c is absolute. This is a problem of the one-dimensional sieve (often called the linear sieve). The very elegant method of Selberg, which is optimal in this case, leads to the Brun–Titchmarsh estimate with $c = 2$. The same neat estimate can be also achieved by a large sieve type argument (a Hilbert inequality due to H. L. Montgomery and R. C. Vaughan [57], [58]). It is intrinsic to the linear sieve that we miss the correct estimate by factor of two (the parity problem, see E. Bombieri [4]). Therefore it was surprising when Y. Motohashi [59] improved this estimate in some ranges by incorporating analytic arguments with the sieve theory. His work inspired further developments of the linear sieve theory (see [43]). The key new feature is the bilinear form structure of the remainder term which can be better estimated by methods of exponential sums over a finite field. Recently J. Friedlander and H. Iwaniec [25] employed estimates for extremely short exponential sums of Kloosterman type (based on the original ideas of Karatsuba, and reminiscent of the Vinogradov exponential sums method) getting an improvement essentially in the whole range,

$$\pi(x; q, a) \leq (2 - \delta)x/\phi(q) \log(x/q)$$

for $x^\alpha < q < x^\beta$ with any fixed $0 < \alpha < \beta < 1$ and some $\delta > 0$ depending only on α, β (we assume that x is large in terms of α, β). This estimate does not break the parity barrier of sieve theory; it would do so if we had $\log(x/q)$ replaced by $\log x$. However we are skeptical that one can go that far with the sieve arguments, because the consequences would be fantastic, namely the non-existence of the exceptional zero (apply the formula (4.2)).

5. Problems of exceptional character

Perhaps there is nothing more exciting in analytic number theory than debates about the exceptional character. I have written a long survey on the subject [45], and I now repeat some of my observations here. For brevity let me restrict the story to the odd real characters; although many remarks are valid for the even characters as well. Such a character $\chi_D(n) = \left(\frac{-D}{n}\right)$ is the Kronecker symbol, whose values $+1, -1, 0$ characterize factorization of rational primes into ideals in the imaginary quadratic field $K = Q(\sqrt{-D})$. Here $-D$ is the discriminant of the field K and $D > 0$ is the conductor of the character χ_D.

Let me begin with an intriguing observation by L. Euler, that the polynomial $x^2 - x + 41$ takes prime values for all $0 \le x \le 40$. No, do not hope for many such amusing examples! We know today that the reason for seeing so many first prime values of the Euler polynomial is that its splitting field $K = Q(\sqrt{-163})$ has the class number one, that is to say, every integral ideal of K is principal. G. Rabinowitsch [61] made it clear with his criterion for all the discriminants $-D$ with $K = Q(\sqrt{-D})$ having class number one. Long ago C. F. Gauss conjectured that there are exactly nine such fields, and hence our saga began. After the early 1930s (Deuring, Heilbronn, Linfoot), we knew that the Gauss list is complete except possibly for one missing discriminant, so the problem was to show that the tenth discriminant did not exist! Numerical computations were useless until we got an effective bound for the class number $h(-D)$ in terms of D.

By the Dirichlet class number formula

$$L(1, \chi_D) = \frac{\pi h(-D)}{\sqrt{D}}, \quad \text{if } D > 4 \tag{5.1}$$

and by the estimates $(\log\log D)^{-1} \ll L(1, \chi_D) \ll \log\log D$, which follow from the Riemann Hypothesis for $L(s, \chi_D)$, we infer a pretty good location for the class number

$$\sqrt{D}(\log\log D)^{-1} \ll h(-D) \ll \sqrt{D}\log\log D.$$

Of course, this would end the saga for someone who takes the Riemann hypothesis for granted, but we are not willing to do so. Therefore, we are looking for an unconditional lower bound for $L(1, \chi_D)$. If there is no exceptional zero of $L(s, \chi_D)$ in the region (4.1), then $L(1, \chi_D) \gg 1/\log D$, and consequently $h(-D) \gg \sqrt{D}/\log D$, where

the implied constant is effectively computable. This lower bound would be more than sufficient to determine all the imaginary quadratic fields $K = Q(\sqrt{-D})$ with any fixed class number $h(-D) = 1, 2, 3, \ldots$. Ironically the original idea of Dirichlet for estimating $L(1, \chi_D)$ (which was needed for the existence of primes in arithmetic progressions) uses the trivial bound $h(-D) \geq 1$ in the formula (5.1), offering nothing useful for the class number problem itself. E. Landau [53] gave the first non-trivial bound $h(-D) \gg D^{1/8}$ (shortly after C. L. Siegel [66] improved it), which is quite impressive, but still useless for solving the Gauss problem. Landau's estimate is defective (so is Siegel's), because the implied constant is ineffective. This translates into saying that the exceptional zero of $L(s, \chi_D)$ is not too close to one. Specifically Siegel proved that for every $\varepsilon > 0$ there exists a constant $c(\varepsilon) > 0$ such that

$$\beta \leq 1 - c(\varepsilon) q^{-\varepsilon}. \tag{5.2}$$

The constant $c(\varepsilon)$ cannot be computed. This deficiency doesn't matter for many applications, but one must be aware that certain statements with ineffective constants have no content. For example, consider the following grotesque theorem: There is a constant $T > 0$, such that if every complex zero of ζ(s) with height $< T$ is on the critical line then the RH is true. However Siegel's result is serious, it is indispensable for the Bombieri–Vinogradov theorem.

One of many intriguing characteristics of the exceptional character is its repelling property. Roughly speaking if the exceptional zero of $L(s, \chi_D)$ is closer to the point $s = 1$, then the other zeros are farther away from $s = 1$, not only the real zeros of $L(s, \chi_D)$, but also all the zeros of any other natural L-function. This effect seems to be pretty universal. Here is how the mystery can be explained in a few steps:

- Suppose a real zero of $L(s, \chi_D)$ is close to $s = 1$.
- Then $L(1, \chi_D)$ is very small.
- Consequently, by the class number formula $h(-D)$ is small.
- Therefore, the prime numbers which split in $K = Q(\sqrt{-D})$ are rare.
- Hence the character χ_D takes value -1 at almost all primes.
- This says that χ_D pretends to be the Möbius function on squarefree numbers, because both are multiplicative.
- While also being periodic the character χ_D works nicely with any natural L-function by twisting.
- The natural L-function after twisting is still entire and in the same time it pretends to be the inverse.
- In conclusion the natural L-function, whatever it is, cannot vanish in vast regions.

This colorful scenario is a dream which we wish were true. For one reason the exceptional character could help prove beautiful theorems about primes without recourse to the Grand Riemann Hypothesis. In fact, we shall see that the existence of the exceptional character can permit us to do better than what we can do with the GRH.

Before indulging ourselves in this illusory situation, let me come back to reality with some historical points. To derive effective results, in principle, there is no reason to abandon the repelling property of a real zero; provided this special zero is really real, that is it has a numerical value. Fine, but how can one produce this repellant if we believe in the GRH? The only hope along such ideas is to find an L-function which vanishes at the central point $\beta = \frac{1}{2}$. A quick examination of Siegel's arguments reveals that any zero $\beta > \frac{1}{2}$ has some power of repelling, which is not as strong as that of the zero near the point $s = 1$, yet sufficiently strong for showing effectively that

$$h(-d) \gg D^{\beta-\frac{1}{2}}(\log D)^{-1}.$$

In view of this property the first question that arises is; "Does the central zero have an effect on the class number?" In the remarkable paper by J. Friedlander [20] we find the answer; "Yes it does and the impact depends on the order of the central zero!" The second question is; "How does one find L-functions which do vanish at the central point with sufficient multiplicity?" Definitely the Dirichlet L-functions do not qualify (by a folk conjecture $L\left(\frac{1}{2}, \chi\right) > 0$ for any real character χ). Obviously, if $L(s, f)$ is self-dual and has the root number -1 in its functional equation, then $L\left(\frac{1}{2}, f\right) = 0$. Alas, not a single such case was known until J. V. Armitage [1] gave an example of an L-function of a number field.

A lot more possibilities are offered by elliptic curves. Indeed, according to the Birch and Swinnerton-Dyer conjecture the Hasse–Weil L-function of an elliptic curve E/Q vanishes at the central point to the order equal to the rank of the group of rational points. D. Goldfeld [31] first took this route successfully assuming he was given an L-function which vanishes at the central point to order three (a double zero at the central point is not repelling). It is easy to point out the candidate as it is easy to construct an elliptic curve of rank $g = 3$ (by forcing three points to lay on a curve), but proving that it is modular with the corresponding L-function vanishing to the correct order at the central point is much harder a problem. Ten years after Goldfeld's work such an L-function was provided by B. Gross and D. Zagier [33], concluding with the lower bound

$$h(-D) \gg \prod_{p|D}(1 - \frac{2\sqrt{p}}{p+1}) \log D.$$

This bound is effective, so today one can determine (time permitting) all the imaginary quadratic fields $K = Q(\sqrt{-D})$ which have a given class number.

Some renowned researchers contemplated that the GRH could hold for any natural L-function except possibly for some real zeros very close to the point $s = 1$. But

recently P. Sarnak and A. Zaharescu [65] proved that such a zero would ruin the GRH very badly. Briefly speaking, the L-functions for certain cusp forms would have complex zeros off the critical line.

Let us assume the Grand Riemann Hypothesis. A simple or double zero at the center has no visible effect on the class number. But what about the other zeros on the critical line, which we know appear in abundance? Rather than asking for high multiplicity, more hopefully, one should ask if some clustering of the complex zeros do the job. Yes indeed, to wipe out the exceptional zeros of real Dirichlet L-functions one only needs to appeal to the zeros of the Riemann zeta function. B. Conrey and H. Iwaniec [10] showed that if the gaps between zeros of $\zeta(s)$ are smaller than half of the average value sufficiently often, then the exceptional zeros do not exist (see the original paper for more precise statements). Of course, one must question whether the required small gaps do occur in reality. We cannot yet prove it, but we have strong evidence deduced from the Pair Correlation Theory of H. L. Montgomery [56].

We used to think that the zeros of distinct L-functions do not see each other, that they are governed by independent distribution laws (read the Katz–Sarnak philosophy [50]). This is not so clear today by the results of [10] (the Riemann zeta function conspires against the Dirichlet L-functions?).

The L-functions co-exist and interact strongly in families. Analytic number theorists are very successful in exploring families associated with objects, which are in some sense orthogonal and complete in an appropriate ambient space (like the Hilbert space of modular forms). For example, let H_k be the basis of the linear space of cusp forms of weight k which are simultaneous eigenfunctions of all the Hecke operators on the modular group $\mathrm{SL}(2, \mathbb{Z})$. Let $H(K)$ be the union of H_k for $k \leq K$, $k \equiv 0(\bmod 4)$, so $H(K)$ has about K^2 forms. Let $L(s, f)$ be the Hecke L-function associated with f in $H(K)$. Note that the root number (the sign of the functional equation) is $+1$ (we normalize the Hecke operators so that the central point of any $L(s, f)$ is at $s = \frac{1}{2}$). Motivated by questions of the exceptional character H. Iwaniec and P. Sarnak [48] proved that at least 50% of the L-functions in the set $H(K)$ do not vanish at the central point. Actually we gave fairly good positive lower bounds. We believe that 100% of these central values are strictly positive (and relatively large). So what is special about the 50%? If we got just a bit more, then we could say good-bye to the exceptional zero. Keep in mind that here we took a somewhat opposite direction for attacking the exceptional zero, that is to say, we do not explore zeros of L-functions as repellants, but instead we utilize a lot of positive central values.

So far we have tried vigorously to eliminate the exceptional zero, because it is a pest in many areas of analytic number theory. However, as we have said previously, in some applications the exceptional character and its exceptional zero are very welcome. In particular the exceptional character helps to deal with prime numbers in exotic sequences where the Riemann hypothesis is not applicable. Recall that the real character χ_D is said to be exceptional if the corresponding L-function has a real zero $\beta > 1 - c/\log D$, for some fixed sufficiently small positive constant c. Assuming that this happens for arbitrarily large modulus D one can show the existence of

primes in many sparse sequences. I call these "the illusory primes", because today nobody believes that the exceptional zeros exist in reality. First D. R. Heath-Brown [35] showed under the above condition that there are infinitely many twin primes. J. Friedlander and H. Iwaniec [26], [27], [28] found illusory primes in other sets. For example we showed under similar conditions (see [28]) that the polynomial $x^2 + y^6$ represents infinitely many primes.

Having enjoyed the assistance of the exceptional zeros for the Dirichlet L-functions in the quest for prime numbers we can only dream of extending this illusory world to other kind of L-functions. But we already know that the L-functions of cusp forms are not exceptional; nor are the associated symmetric square L-functions (due to Goldfeld, Hoffstein, Lockhart, Lieman, Ramakrishnan). In view of these results and related intense investigations, the real character appears to be the hardest stubborn case!

6. Capturing primes by sieve methods

The sieve methods were created with great expectation for finding the twin primes and for proving the Goldbach conjecture. The first ideas of Viggo Brun of 1915–1924 followed the exclusion-inclusion procedure as in the ancient Eratosthenes sieve. Over fifty years many ramifications of this approach have been developed, notably the combinatorial sieve, the Selberg upper bound sieve and the Bombieri asymptotic sieve (see my article [44] in the Proceedings of the ICM in Helsinki). Although the principal ideas are elementary, it was necessary to incorporate analytic arguments for the finest estimates. In the most important cases, like the linear sieve, we know the optimal results. Unfortunately they are too weak to give prime numbers in general sequences for which the methods apply. Not because we overlooked something, but rather because of an intrinsic barrier, which is called the *parity phenomenon*. The parity phenomenon is best explained in the context of Bombieri's asymptotic sieve [4]. This says that within the classical conditions for the sieve one cannot sift out all numbers having the same parity of the number of their prime divisors. Never mind producing primes; we cannot even produce numbers having either one, three, five or seven prime divisors. However under the best circumstances we can obtain numbers having either 2006 or 2007 prime divisors. Similarly we can also obtain numbers having either one or two prime divisors, but we are not able to determine which of these numbers are there, probably both.

Therefore, in order to distinguish primes from numbers having two prime divisors it is necessary to extend the system of sieve conditions by adding a new condition. We shall explain the new idea by modifying the asymptotic sieve of Bombieri.

Suppose $\mathcal{A} = (a_n)$ is a sequence of real, non-negative numbers. We are after the sum

$$S(x) = \sum_{n \le x} a_n \Lambda(n). \tag{6.1}$$

Recall that $\Lambda(n)$ denotes the von Mangoldt function which is supported on powers of prime numbers (in practice it is easy to ignore the high powers). Assume we are given natural approximations to the sums

$$A_d(x) = \sum_{\substack{n \le x \\ n \equiv 0 (\bmod d)}} a_n,$$

specifically we have

$$A_d(x) = g(d)A(x) + r_d(x)$$

where $g(d)$ is a multiplicative functions with $0 \le g(p) < 1$ for all p and $r_d(x)$ is considered to be an error term, which is relatively small. Here $g(d)$ represents the density of the subsequence of elements a_n with n being divisible by d. Naturally we assume that $g(d)$ is multiplicative, because we believe that the divisibility by distinct primes are independent events (this is not exactly true in stronger models of the sieve). Writing $\Lambda(n)$ as a convolution of the Möbius function and the logarithm, or more conveniently writing

$$\Lambda(n) = \sum_{d|n} \mu(d) \log d,$$

we arrange $S(x) = H(x)A(x) + R(x)$, where

$$H(x) = -\sum_{d \le x} \mu(d)(\log d)g(d),$$

$$R(x) = -\sum_{d \le x} \mu(d)(\log d)r_d(x).$$

The density function $g(d)$ usually satisfies natural regularity conditions, which imply that $H(x)$ has a limit

$$H(x) \sim H = \prod_p (1 - g(p)) \left(1 - \frac{1}{p}\right)^{-1}. \tag{6.2}$$

Ignoring the remainder term $R(x)$ one is led to the following asymptotic formula

$$S(x) \sim HA(x), \quad \text{as } x \to \infty. \tag{6.3}$$

Although one cannot ignore the remainder terms arbitrarily, the above asymptotic formula is conjectured to hold for every natural sequences $\mathcal{A} = (a_n)$. This agrees with formulas derived by various heuristic arguments, for instance by the circle method.

Why do we expect that the remainder term $R(x)$ is insignificant? There are primarily two reasons. First if the moduli d are relatively small, say $d < D$ with some $D = D(x) \le x$, then the individual error terms $r_d(x)$ are small. But for d

large, closer to x, the error terms $r_d(x)$ are comparable in size with the main terms $g(d)A(x)$. Hence their contribution is insignificant not because they are relatively small, but because of a cancellation in $R(x)$, which is due to the sign change of the Möbius function $\mu(d)$. The first part with $d < D$ belongs to the classical system of sieve conditions while the remaining part is critical for breaking the parity barrier. Looking behind the scene is the randomness of the Möbius function, which we loosely articulate as the following principle:

Randomness of the Möbius function. *The Möbius function $\mu(d)$ changes sign with unbiased fashion towards any natural sequence $c(d)$, thus producing a considerable cancellation in sums of the twisted terms $\mu(d)c(d)$.*

It is hard to imagine that a natural sequence conspires with the Möbius function, so it is frequently save to accept the heuristic formula (6.3). Then why do we face the parity barrier of sieve methods which prevents us from capturing prime numbers? Because the combinatorial sieve constructions make use of a truncated Möbius function which is obviously biased to the pure Möbius function! The Selberg sieve is somewhat different, but not much in this regard.

Estimating sums of terms twisted by the Möbius function is usually as difficult as that of the von Mangoldt function, so we are not yet done. In the next step of the sieve for primes we convert the twisted sums to bilinear forms. The latter can be estimated using a variety of tools of operator theory with the most successful being the duality principle and the large sieve inequality (not a sieve method, please). Here the structure of a bilinear form plays a vital role. It works for quite general coefficients so one can escape from the vicious circle created by the Möbius function. Let me give a simple but quite general result which is derived along the above lines.

Proposition (sieve for primes). *Suppose a sequence of non-negative numbers $\mathcal{A} = (a_n)$ has the density function $g(d)$ which is multiplicative with $0 \le g(p) < 1$ and*

$$\sum_{p\le y} g(p)\log p = \log y + c_g + O(1/\log y), \tag{6.4}$$

for any $y \ge 2$, with c_g a constant. Suppose

$$\sum_{d\le D} |r_d(x)| \le A(x)(\log x)^{-2}, \tag{6.5}$$

$$\sum_{\ell} \Big| \sum_{\substack{\ell m\le x\\ z<m\le z^2}} \mu(m)a_{\ell m}\Big| \le A(x)(\log x)^{-2}, \tag{6.6}$$

where $z = x^\delta$, $D = x^{1-\delta}$ with some small $\delta > 0$. Then we have

$$\sum_{n\le x} a_n\Lambda(n) \sim HA(x), \quad \text{as } x \to \infty. \tag{6.7}$$

The first condition (6.5) is classical in sieve theory, and sometimes it can be established for $D = x^{1-\delta}$ with δ arbitrarily small. In this case the first condition alone suffices to derive an asymptotic formula (due to Bombieri)

$$\sum_{n\le x} a_n \Lambda_k(n) \sim kHA(x)(\log x)^{k-1}$$

for any $k \ge 2$, where $\Lambda_k(n)$ is the von Mangoldt function of order k which is supported on numbers having at most k distinct prime divisors. As we mentioned before this asymptotic formula must fail for $k = 1$, because of the parity barrier. Our second condition (6.6) takes care of this barrier. This bilinear form estimate is much harder to establish, yet it is in the realm of modern technology.

Example (Fouvry–Iwaniec). The sequence $\mathcal{A} = (a_n)$ with

$$a_n = \sum_{\ell^2+m^2=n} \Lambda(\ell)$$

satisfies (6.5) and (6.6). Therefore we have

$$\sum_{\ell^2+m^2\le x} \Lambda(\ell)\Lambda(\ell^2+m^2) \sim Hx$$

where H is a positive constant. Hence there are infinitely many primes of type $p = \ell^2 + m^2$ where ℓ is also prime.

Presently there are various variants of sieve axioms which are capable of producing primes (see Friedlander and Iwaniec [23]), Heath-Brown [37]). In the above proposition the axioms are realistic only if the sequence $\mathcal{A} = (a_n)$ is relatively dense, while the other versions can handle quite sparse sequences. Of course the verification of these axioms for sparse sequences is even harder, but the results are more impressive.

Example (Friedlander–Iwaniec). We have

$$\sum_{a^2+b^4\le x} \Lambda(a^2+b^4) \sim Hx^{\frac{3}{4}}.$$

Example (Heath-Brown). He has

$$\sum_{a^3+2b^3\le x} \Lambda(a^3+2b^3) \sim Hx^{\frac{2}{3}}.$$

Let me point out that in every case considered so far the prime producing sieve does not actually produce primes. At best what it does is allow the search for primes in a target sequence to be augmented by using primes in another sequence which has a simpler structure so we know it contains primes by standard analytic arguments, usually like the zeta function methods. Yes, it is a steal, but not easy. Usually these

transformations are far more advanced than a proof of the PNT in the comparative sequence.

The same can be said about the prime producing sieve in the work of Goldston–Pintz–Yildirim [32], although their approach is very different. They start with a collection of some distinct positive integers $h_1, \dots, h_r$, to which they associate the arithmetic function

$$W(m) = \sum_{1 \le i \le r} \Lambda^\flat(m - h_i) - \log m$$

where $\Lambda^\flat(n) = \log n$ if n is prime, and zero otherwise. Assume that the Bombieri–Vinogradov theorem holds with moduli $q \le Q = x^\theta$, for some $\theta > \frac{1}{2}$, and that the number of shifts r is sufficiently large in terms of θ. Summing $W(m)$ over $m \le x$ with certain non-negative weights (Selberg's sieve weights of various dimensions) they managed to show that $W(m)$ is positive for many $m \le x$. For these m's at least two of the shifted numbers $m - h_1, \dots, m - h_r$ are primes (these primes are not produced by sieve weights, they are borrowed from the Bombieri–Vinogradov theorem, which extracts them from the Siegel–Walfish theorem). Consequently the gap between these primes is bounded by $H = \max |h_i - h_j|$. Note that the result requires the level of distribution of primes in arithmetic progressions to be x^θ with $\theta > \frac{1}{2}$, which the GRH does not reach. Nevertheless, as we said in Section 4 we believe this should hold with any $\theta < 1$. Assuming this conjecture (the Elliott–Halberstam conjecture) the arguments of Goldston–Pintz–Yildirim lead to a conclusion that there are infinitely many gaps between distinct primes which do not exceed 16. Wow!

7. Bilinear forms technique for sums over primes

The core of Prime Number Theory consists of the distribution of primes in short segments, in arithmetic progressions, in homogeneous polynomials and in other similar sparse sequences. This territory expands to number fields, where the prime ideals play the role of primes. Here new challenging aspects emerge, particularly important being the uniformity of estimates with respect to the field invariants. For example, the distribution of prime ideals in the Galois conjugacy classes (the Tchebotarev theorem) is considered as a non-abelian analog of the distribution of primes in arithmetic progressions. Then one goes further into the territory of automorphic forms, where for example one may study the Hecke eigenvalues at primes. Why at primes? Because these eigenvalues admit a geometric interpretation (consider the group of points of an elliptic curve over a finite field). One may view this section of the theory of primes as a natural continuation of the celebrated memoir of Riemann on the zeta function. Here analytic arguments come to fruition through the zeros of L-functions. H. Davenport named this territory "multiplicative number theory".

Now I would like to go through a different territory of sums over primes which can hardly be treated by L-function methods. They are distinguished by the idea of

bilinear forms. Consider the sum

$$S_f(x) = \sum_{p \le x} f(p)$$

where f is an arithmetic function defined on primes, but not necessarily on all positive integers. Of course, one can always extend f to all integers arbitrarily, however a natural extension may not suggest itself easily. Very often, neither the associated Dirichlet series

$$\sum_n f(n) n^{-s},$$

nor the Fourier series

$$\sum_n f(n) e(nz)$$

has any beneficial properties (these series are logical creatures if f is multiplicative or additive respectively).

The bilinear forms technique rearranges the sum $S_f(x)$ into a number of other sums (as in sieve methods), the key one being of type

$$S_f(M, N) = \sum_{m \le M} \sum_{n \le N} \alpha_m \beta_n f(m, n)$$

with some specific coefficients α_m, β_n. Because of the complexity of these coefficients one cannot expect to treat them in any other way than as general complex numbers. For this reason the sum $S_f(M, N)$ is almost a genuine bilinear form. A non-trivial estimate is still possible; provided f does not resemble a multiplicative function, and f has a considerable sign variation. Paraphrasing, we are looking for a non-trivial estimate of the norm of the corresponding operator, which in this case is the largest eigenvalue of the corresponding matrix. While there are lots of possibilities here, it turns out that an application of Cauchy's inequality is most popular, because it is very flexible. I do not mean a straightforward application, in many situations it precedes with elaborate preparation of the bilinear form by exploiting its characteristics. For example it is wise to perform some kind of linearization before applying Cauchy's inequality to avoid the increase of the dimension of the resulting lattice point problem (see how in [17] we landed in the domain of complex integers when counting the rational primes of type $p = \ell^2 + m^2$ with ℓ prime).

Let me state one of many results about general sums over primes which exhibit the bilinear form technique.

Theorem (Duke–Friedlander–Iwaniec). *Let $f(n)$ be any sequence of complex numbers with $|f(n)| \le \tau(n)$. Suppose*

$$\sum_{d \le y} \Big| \sum_{dm \le x} f(dm) \Big| \le x (\log x)^{-2},$$

$$\sum_m \Big| \sum_{\substack{pm\le x\\ w<p<v}} p^{it} f(pm)\Big| \le x(\log x)^{-4}$$

for $x \ge e^{1/\varepsilon}$ with $0 < \varepsilon \le \frac{1}{12}$, where t is any real number and the parameters y, v, w are given by $y = x^{\frac12-\varepsilon}$, $v = x^{\frac13-\varepsilon}$, $w = x^{\varepsilon/10\log\log x}$. Then we have

$$\sum_{p\le x} f(p) \ll \varepsilon x(\log x)^{-1},$$

where the implied constant is absolute.

Remark. The inner sum coefficients in the first double sum are constant and in the second double sum they are p^{it}, so virtually they are general because t is not fixed.

This theorem was crafted for a specific sequence in mind, namely

$$f(n) = \sum_{\nu^2+1\equiv 0\,(n)} e\Big(\frac{\nu h}{n}\Big)$$

where $h \ne 0$ is a fixed integer. That this sequence satisfies the above condition is itself a great problem which we solved using the spectral theory of automorphic forms. Hence we obtain

$$\frac{1}{\pi(x)} \sum_{p\le x} \sum_{\nu^2+1\equiv 0(p)} e\Big(\frac{\nu h}{p}\Big) \to 0, \quad \text{as } x \to \infty.$$

In other words, using Weyl's criteria from equidistribution theory we proved that the roots of the polynomial $P(X) = X^2 + 1$ in the finite field of p elements are uniformly distributed when p runs over primes (for every $p \equiv 1 \pmod 4$ there are two roots, and none if $p \equiv 3 \pmod 4$). Similar results are established for other quadratic polynomials irreducible over $\mathbb{Z}$. The problem for higher degree irreducible polynomials is out of reach by current technology. Probably the uniform distribution of roots holds no matter what is the Galois group of the polynomial.

According to a theorem of Fermat every prime $p \equiv 1 \pmod 4$ is a sum of two squares, $p = a^2 + b^2$. This representation is unique if we require a, b to be positive and b odd. We call the Jacobi symbol $s_p = \big(\frac{a}{b}\big)$ the spin of the corresponding Gaussian prime $\pi = a + bi$. As a by-product of the work on primes represented by the polynomials $X^2 + Y^4$ we have shown that the spin changes quite regularly, in fact we got (see [24])

$$\sum_{\substack{p\le x\\ p\equiv 1(4)}} s_p \ll x^{\frac{76}{77}}.$$

8. Sums over primes related to modular forms

A great variety of interesting arithmetic functions appear in modular forms, for example the Fourier coefficients of cusp forms. For an obvious reason the bilinear form technique does not work for sums over primes of a multiplicative function. In particular this would fail for the Hecke eigenvalues of any classical cusp form (holomorphic of integral weight). However it works nicely for the Fourier coefficients $\rho(n)$ of any metaplectic cusp form (a modular form on a congruence group of half-integral weight with respect to the theta multiplier). Indeed W. Duke and H. Iwaniec [15] established the following estimate

$$\sum_{p\leq x}\rho(p) \ll x^{\frac{156}{157}}.$$

D. R. Heath-Brown and S. Patterson got an estimate of similar nature for cubic Gauss sums. When investigating the low lying zeros of classical cusp forms in [47] we encountered sums of type

$$S_f(x) = \sum_{p\leq x}\lambda(p)e(2\sqrt{p})$$

where $\lambda(p)$ are the eigenvalues of the Hecke operators T_p acting on a classical cusp form on the full modular group. We normalize these so that the Ramanujan conjecture (proved by P. Deligne) becomes $|\lambda(p)| \leq 2$. Due to the twist by the exponential factor the function $f(n) = \lambda(n)e(2\sqrt{n})$ is not multiplicative, so it is possible to show by bilinear form techniques that

$$S_f(x) \ll x^{\frac{5}{6}}.$$

In the theory of exponential sums and character sums there is a reasonable expectation that cancellation should be of the order of the square root of the number of terms, unless there is a natural reason to prevent this from happening, in which case one gets a larger main term. Clearly this philosophy is consistent with the Grand Riemann Hypothesis. Indeed we can show that the sum of $f(n)$ over all integers $n \leq x$ is bounded by $O(x^{\frac{1}{2}+\varepsilon})$. Should this bound be also true for the sum restricted by primes? One would think so according to the above philosophy, but our findings suggest different things! To be convinced we applied the Möbius Function Randomness Principle which led us to the surprising asymptotic formula

$$S_f(x) \sim cx^{\frac{3}{4}}(\log x)^{-1}$$

where $c \neq 0$ is a constant (c is the value of the associated symmetric square L-function at $s = 1$, up to some elementary factors). On the other hand for the sums over primes with no twists the GRH implies

$$\sum_{p\leq x}\lambda_f(p) \ll x^{\frac{1}{2}+\varepsilon}, \tag{4}$$

$$\sum_{p\le x} e(2\sqrt{p}) \ll x^{\frac{1}{2}+\varepsilon}. \tag{5}$$

Comparing the above three estimates one may conclude that the Hecke eigenvalues $\lambda(p)$ are somewhat biased towards the exponential function $e(2\sqrt{p})$. Why does it happen at primes but not at all integers? It would be interesting to understand this behavior within the structure of modular forms.

Some important arithmetic functions at primes do not obey the law of equidistribution with respect to the natural (Lebesgue) measure. For example the angles of the Hecke eigenvalues $\lambda(p) = 2\cos(\theta_p)$ for a given cusp form on the full modular group (so it is not of complex multiplication type) are conjectured to be equidistributed with respect to the Sato–Tate measure $2\pi^{-1}(\sin\theta)^2 d\theta$ on $[0, \pi]$. This would follow (as part of Langlands' program) from the conjecture that all the symmetric power L-functions associated with the given cusp form are holomorphic in the half-plane $\mathrm{Re}(s) \ge 1$ and do not vanish on the line $\mathrm{Re}(s) = 1$.

The angles of the classical Kloosterman sums

$$K(a, b; p) = \sum_{xy\equiv 1\,(p)} e\left(\frac{ax+by}{p}\right) = 2\sqrt{p}\cos\theta_p$$

with $ab \ne 0$ are also conjectured to have the Sato–Tate measure of equidistribution. Sadly enough we do not even know whether they change sign infinitely often. However E. Fouvry and P. Michel [18], [19] showed that the Kloosterman sums to moduli, which are the product of at most twenty-three distinct primes, do change sign very often. This is a very deep work. Besides creating innovations in sieve methods they gave original transformations which reduce the problem to the Riemann hypothesis for varieties over a finite field (proved by P. Deligne).

The Kloosterman sums twisted by the real character

$$S(a, b; p) = \sum_{xy\equiv 1\,(p)} \left(\frac{x}{p}\right) e\left(\frac{ax+by}{p}\right) = 2\sqrt{p}\cos\theta_p$$

(named Salie sums), behave differently. Their angles are known to be equidistributed with respect to the natural (Lebesgue) measure. This fact was proved by W. Duke, J. Friedlander and H. Iwaniec [13] using the bilinear forms technique and the spectral theory of automorphic forms.

9. Closing remarks

Analytic number theory is fortunate to have one of the most famous unsolved problems, the Riemann hypothesis. Not so fortunately, this puts us in a defensive position, because outsiders who are unfamiliar with the depth of the problem, in their pursuit for the ultimate truth, tend to judge our abilities rather harshly. In concluding this

talk I wish to emphasize my advocacy for analytic number theory by saying again that the theory flourishes with or without the Riemann hypothesis. Actually, many brilliant ideas have evolved while one was trying to avoid the Riemann hypothesis, and results were found which cannot be derived from the Riemann hypothesis. So, do not cry, there is a healthy life without the Riemann hypothesis. I can imagine a clever person who proves the Riemann hypothesis, only to be disappointed not to find new important applications. Well, an award of one million dollars should dry the tears; no applications are required!

References

[1] Armitage, J. V., Zeta functions with a zero at $s = \frac{1}{2}$. *Invent. Math.* **15** (1972), 199–205.

[2] Baker, R. C., Harman, G., Pintz, J., The difference between consecutive primes, II. *Proc. London Math. Soc.* (3) **83** (3) (2001), 532–562.

[3] Bombieri, E., On the large sieve. *Mathematika* **12** (1965), 201–225.

[4] Bombieri, E., The asymptotic sieve. *Rend. Accad. Naz. XL* (5) **1/2** (1975/76), 243–269.

[5] Bombieri, E., Prime numbers from recreational mathematics to practical applications. Preprint of IAS.

[6] Bombieri, E., Friedlander, J. B., Iwaniec, H., Primes in arithmetic progressions to large moduli. *Acta Math.* **156** (3–4) (1986), 203–251.

[7] Bombieri, E., Davenport, H., Small differences between prime numbers. *Proc. Roy. Soc. Ser. A* **293** (1966), 1–18.

[8] Conrey, J. B., More than two fifths of the zeros of the Riemann zeta function are on the critical line. *J. Reine Angew. Math.* **399** (1989), 1–26.

[9] Conrey, J. B., L-functions and random matrices. In *Mathematics Unlimited—2001 and beyond*, Springer-Verlag, Berlin 2001, 331–352.

[10] Conrey, B., Iwaniec, H., Spacing of zeros of Hecke L-functions and the class number problem. *Acta Arith.* **103** (3) (2002), 259–312.

[11] Deshouillers, J.-M., te Riele, H., On the probabilistic complexity of numerically checking the binary Goldbach conjecture in certain intervals. In *Number Theory and its Applications* (Kyoto, 1997), Dev. Math. 2, Kluwer Acadademic Publishers, Dordrecht 1999, 89–99.

[12] Deshouillers, J.-M., Effinger, G., te Riele, H., Zinoviev, D., A complete Vinogradov 3-primes theorem under the Riemann hypothesis. *Electron. Res. Announc. Amer. Math. Soc.* **3** (1997), 99–104 (electronic).

[13] Duke, W., Friedlander, J. B., Iwaniec, H., Equidistribution of roots of a quadratic congruence to prime moduli. *Ann. of Math.* (2) **141** (2) (1995), 423–441.

[14] Deshouillers, J.-M., Hennecart, F., Landreau, B., Waring's problem for sixteen biquadrates—numerical results. *Colloque International de Théorie des Nombres* (Talence, 1999); *J. Théor. Nombres Bordeaux* **12** (2) (2000), 411–422.

[15] Duke, W., Iwaniec, H., Bilinear forms in the Fourier coefficients of half-integral weight cusp forms and sums over primes. *Math. Ann.* **286** (4) (1990), 783–802.

[16] Fouvry, É., Autour du théoréme de Bombieri-Vinogradov. *Acta Math.* **152** (3–4) (1984), 219–244.

[17] Fouvry, E., Iwaniec, H., Gaussian primes. *Acta Arith.* **79** (3) (1997), 249–287.

[18] Fouvry, E., Michel, P., Crible asymptotique et sommes de Kloosterman. In *Proceedings of the Session in Analytic Number Theory and Diophantine Equations*, Bonner Math. Schriften 360, Universität Bonn, Bonn 2003.

[19] Fouvry, E., Michel, P., Sur le changement de signe des sommes de Kloosterman. *Ann. of Math.*, to appear.

[20] Friedlander, J. B. On the class numbers of certain quadratic extensions. *Acta Arith.* **28** (4) (1975/76), 391–393.

[21] Friedlander, J. B., Irregularities in the distribution of primes. In *Advances in Number Theory* (Kingston, ON, 1991), Oxford Sci. Publ., Oxford University Press, New York 1993, 17–30.

[22] Friedlander, J. B., Granville, A., Limitations to the equi-distribution of primes. I. *Ann. of Math.* (2) **129** (2) (1989), 363–382.

[23] Friedlander, J. B., Iwaniec, H., Using a parity-sensitive sieve to count prime values of a polynomial. *Proc. Nat. Acad. Sci. U.S.A.* **94** (4) (1997), 1054–1058.

[24] Friedlander, J. B., Iwaniec, H., The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math.* (2) **148** (3) (1998), 945–1040.

[25] Friedlander, J. B., Iwaniec, H., The Brun-Titchmarsh theorem. In *Analytic Number Theory* (Kyoto, 1996), London Math. Soc. Lecture Note Ser. 247, Cambridge University Press, Cambridge 1997, 85–93.

[26] Friedlander, J. B., Iwaniec, H., Exceptional characters and prime numbers in arithmetic progressions. *Internat. Math. Res. Notices* **2003** (37) (2003), 2033–2050.

[27] Friedlander, J. B., Iwaniec, H., Exceptional characters and prime numbers in short intervals. *Selecta Math.* (*N.S.*) **10** (1) (2004), 61–69.

[28] Friedlander, J. B., Iwaniec, H., The illusory sieve. *Int. J. Number Theory* **1** (4) (2005), 459–494.

[29] Granville, A., Least primes in arithmetic progressions. In *Théorie des Nombres* (Quebec, PQ, 1987), Walter de Gruyter, Berlin 1989, 306–321.

[30] Granville, A., Harald Cramér and the distribution of prime numbers. *Harald Cramér Symposium* (Stockholm, 1993); *Scand. Actuar. J.* **1995** (1) (1995), 12–28.

[31] Goldfeld, D. M., The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **3** (4) (1976), 624–663.

[32] Goldston, D. A., Pintz, J., Yildirim, C. Y., Small gaps between primes. Preprint, May 26, 2005.

[33] Gross, B. H., Zagier, D. B., Heegner points and derivatives of L-series. *Invent. Math.* **84** (2) (1986), 225–320.

[34] Heath-Brown, D. R., Zero density estimates for the Riemann zeta-function and Dirichlet L-functions. *J. London Math. Soc.* (2) **19** (2) (1979), 221–232.

[35] Heath-Brown, D. R., Prime twins and Siegel zeros. *Proc. London Math. Soc.* (3) **47** (2) (1983), 193–224.

[36] Heath-Brown, D. R., The number of primes in a short interval. *J. Reine Angew. Math.* **389** (1988), 22–63.

[37] Heath-Brown, D. R., Primes represented by $x^3 + 2y^3$. *Acta Math.* **186** (1) (2001), 1–84.

[38] Heath-Brown, D. R., Prime number theory and the Riemann zeta-function. In *Recent Perspectives in Random Matrix Theory and Number Theory*, London Math. Soc. Lecture Note Ser. 322, Cambridge University Press, Cambridge 2005, 1–30.

[39] Heath-Brown, D. R., Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc.* (3) **64** (2) (1992), 265–338.

[40] Hildebrand, A., Maier, H., Irregularities in the distribution of primes in short intervals. *J. Reine Angew. Math.* **397** (1989), 162–193.

[41] Huxley, M. N., On the difference between consecutive primes. *Invent. Math.* **15** (1972), 164–170.

[42] Huxley, M. N., Small differences between consecutive primes. *Mathematika* **20** (1973), 229–232.

[43] Iwaniec, H., A new form of the error term in the linear sieve. *Acta Arith.* **37** (1980), 307–320.

[44] Iwaniec, H., Sieve methods. In *Proceedings of the International Congress of Mathematicians* (Helsinki, 1978), Acad. Sci. Fennica, Helsinki 1980, 357–364.

[45] Iwaniec, H., Conversations on the exceptional character. In *Analytic Number Theory*, Lecture Notes in Math. 1891, Springer-Verlag, Berlin 2006, 97–132.

[46] Iwaniec, H., Jiménez, U. J., Almost prime orders of CM elliptic curves modulo primes. *International Congress of Mathematicians* (Madrid, 2006), Short Communication.

[47] Iwaniec, H., Luo, W., Sarnak, P., Low lying zeros of families of L-functions. *Inst. Hautes Études Sci. Publ. Math.* **91** (2000), 55–131.

[48] Iwaniec, H., Sarnak, P., The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros. *Israel J. Math.* **120** (Part A) (2000), 155–177.

[49] Jutila, M., Zero-density estimates for L-functions. *Acta Arith.* **32** (1) (1977), 55–62.

[50] Katz, N. M., Sarnak, P., Zeroes of zeta functions and symmetry. *Bull. Amer. Math. Soc.* (*N.S.*) **36** (1) (1999), 1–26.

[51] Knapowski, S., Turán, P., On prime numbers $\equiv$ 1 resp. 3 mod 4. In *Number theory and algebra*, Academic Press, New York 1977, 157–165.

[52] Landau, E., Über die Nullstellen der Dirichletschen Reihen und der Riemannschen ζ-Funktion. *Arkiv für Mat. Astr. och Fysik* **16** (1921).

[53] Landau, E., Bemerkungen zum Heilbronnschen Satz. *Acta Arithmetica* **1** (1936), 1–18.

[54] Maier, H., Small differences between prime numbers. *Michigan Math. J.* **35** (3) (1988), 323–344.

[55] Montgomery, H. L., *Topics in multiplicative number theory*. Lecture Notes in Math. 227, Springer-Verlag, Berlin 1971.

[56] Montgomery, H. L., The pair correlation of zeros of the zeta function. In *Analytic Number Theory* (St. Louis Univ., St. Louis, Mo., 1972), Proc. Sympos. Pure Math. XXIV, Amer. Math. Soc., Providence, R.I., 1973, 181–193.

[57] Montgomery, H. L., Vaughan, R.C., The large sieve. *Mathematika* **20** (1973), 119–134.

[58] Montgomery, H. L., Vaughan, R.C., Hilbert's inequality. *J. London Math. Soc.* (2) **8** (1974), 73–82.

[59] Motohashi, Y., On some improvements of the Brun-Titchmarsh theorem. *J. Math. Soc. Japan* **26** (1974), 306–323.

[60] Pintz, J., Recent results on the Goldbach conjecture. In *Elementare und Analytische Zahlentheorie* (ed. by W. Schwarz and J. Steuding), Franz Steiner Verlag, Stuttgart 2006, 220–254.

[61] Rabinowitsch, G., Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. In *Proceedings of the Fifth International Congress of Mathematicians* (Cambridge, 1912), Vol. 1, Cambridge University Press, Cambridge 1913, 418–421.

[62] Ramaré, O., On Šnirelman's constant. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **22** (4) (1995), 645–706.

[63] Rubinstein, M., Sarnak, P., Chebyshev's bias. *Experiment. Math.* **3** (3) (1994), 173–197.

[64] Rudnick, Z., Sarnak, P., The n-level correlations of zeros of the zeta function. *C. R. Acad. Sci. Paris Sér. I Math* **319** (10) (1994), 1027–1032.

[65] Sarnak, P., Zaharescu, A., Some remarks on Landau-Siegel zeros. *Duke Math. J.* **111** (3) (2002), 495–507.

[66] Siegel, C. L., Über die Classenzahl quadratischer Zahlkörper. *Acta Arithmetica* **1** (1936), 83–86.

[67] Vinogradov, A. I., The density hypothesis for Dirichet L-series. *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 903–934 (in Russian).

Department of Mathematics, Rutgers, The State University of New Jersey, 110 Frelinghuysen Road, Hill Center-Busch Campus, Piscataway, NJ 08854-8019, U.S.A.

E-mail: iwaniec@math.rutgers.edu

High dimensional statistical inference and random matrices

Iain M. Johnstone*

Abstract. Multivariate statistical analysis is concerned with observations on several variables which are thought to possess some degree of inter-dependence. Driven by problems in genetics and the social sciences, it first flowered in the earlier half of the last century. Subsequently, random matrix theory (RMT) developed, initially within physics, and more recently widely in mathematics. While some of the central objects of study in RMT are identical to those of multivariate statistics, statistical theory was slow to exploit the connection. However, with vast data collection ever more common, data sets now often have as many or more variables than the number of individuals observed. In such contexts, the techniques and results of RMT have much to offer multivariate statistics. The paper reviews some of the progress to date.

Mathematics Subject Classification (2000). Primary 62H10, 62H25, 62H20; Secondary 15A52.

Keywords. Canonical correlations, eigenvector estimation, largest eigenvalue, principal components analysis, random matrix theory, Wishart distribution, Tracy–Widom distribution.

1. Introduction

Much current research in statistics, both in statistical theory, and in many areas of application, such as genomics, climatology or astronomy, focuses on the problems and opportunities posed by availability of large amounts of data. (More detail may be found, for example, in the paper by Fan and Li [40] in these proceedings.) There might be many variables and/or many observations on each variable. Loosely one can think of each variable as an additional dimension, and so many variables corresponds to data sitting in a high dimensional space. Among several mathematical themes one could follow – Banach space theory, convex geometry, even topology – this paper focuses on random matrix theory, and some of its interactions with important areas of what in statistics is called "multivariate analysis."

Multivariate analysis deals with observations on more than one variable when there is or may be some dependence between the variables. The most basic phenomenon is that of correlation – the tendency of quantities to vary together: tall parents tend to

*The author is grateful to Persi Diaconis, Noureddine El Karoui, Peter Forrester, Matthew Harding, Plamen Koev, Debashis Paul, Donald Richards and Craig Tracy for advice and comments during the writing of this paper, to the Australian National University for hospitality, and to NSF DMS 0505303 and NIH R01 EB001988 for financial support.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

have tall children. From the beginning, there has also been a focus on summarizing and interpreting data by reducing dimension, for example by methods such as principal components analysis (PCA). While there are many methods and corresponding problems of mathematical interest, this paper concentrates largely on PCA as a leading example, together with a few remarks on related problems. Other overviews with substantial statistical content include [5], [30] and [36].

In an effort to define terms and give an example, the earlier sections cover introductory material, to set the stage. The more recent work, in the later sections, concentrates on results and phenomena which appear in an asymptotic regime in which p, the number of variables increases to infinity, in proportion to sample size n.

2. Background

2.1. Principal components analysis. Principal components analysis (PCA) is a standard technique of multivariate statistics, going back to Karl Pearson in 1901 [75] and Harold Hotelling in 1933 [51]. There is a huge literature [63] and interesting modern variants continue to appear [87], [80]. A brief description of the classical method, an example and references are included here for convenience.

PCA is usually described first for abstract random variables, and then later as an algorithm for observed data. So first suppose we have p variables $\mathsf{X}_1, \ldots, \mathsf{X}_p$. We think of these as random variables though, initially, little more is assumed than the existence of a *covariance matrix* $\Sigma = (\sigma_{kk'})$, composed of the mean-corrected second moments

$$\sigma_{kk'} = \mathrm{Cov}(\mathsf{X}_k, \mathsf{X}_{k'}) = E(\mathsf{X}_k - \mu_k)(\mathsf{X}_{k'} - \mu_{k'}).$$

The goal is to reduce dimensionality by constructing a smaller number of "derived" variables $W = \sum_k v_k \mathsf{X}_k$, having variance

$$\mathrm{Var}(W) = \sum_{k,k'} v_k \sigma_{kk'} v_{k'} = \boldsymbol{v}^T \Sigma \boldsymbol{v}.$$

To concentrate the variation in as few derived variables as possible, one looks for vectors that maximize $\mathrm{Var}(W)$. Successive linear combinations are sought that are orthogonal to those previously chosen. The *principal component eigenvalues* ℓ_j and *principal component eigenvectors* $\boldsymbol{v}_j$ are thus obtained from

$$\ell_j = \max \left\{ \boldsymbol{v}^T \Sigma \boldsymbol{v} : \boldsymbol{v}^T \boldsymbol{v}_{j'} = 0;\ j' < j,\ |\boldsymbol{v}| = 1 \right\}. \tag{1}$$

In statistics, it is common to assume a stochastic model in terms of random variables whose distributions contain unknown parameters, which in the present case would be the covariance matrix and its resulting principal components. To *estimate* the unknown parameters of this model we have observed data, assumed to be n observations on each of the p variables. The observed data on variable X_k is viewed as

a vector $\boldsymbol{x}_k \in \mathbb{R}^n$. The vectors of observations on each variable are collected as rows into a $p \times n$ data matrix

$$X = (x_{ki}) = [\boldsymbol{x}_1 \dots \boldsymbol{x}_p]^T.$$

A standard pre-processing step is to center each variable by subtracting the sample mean $\bar{x}_k = n^{-1} \sum_i x_{ki}$, so that $x_{ki} \leftarrow x_{ki} - \bar{x}_k$. After this centering, define the $p \times p$ *sample covariance matrix* $S = (s_{kk'})$ by

$$S = (s_{kk'}) = n^{-1} X X^T, \quad s_{kk'} = n^{-1} \sum_i x_{ki} x_{k'i}.$$

The derived variables in the sample, $\boldsymbol{w} = X\boldsymbol{v} = \sum_k v_k \boldsymbol{x}_k$, have sample variance $\widehat{\mathrm{Var}}(\boldsymbol{w}) = \boldsymbol{v}^T S \boldsymbol{v}$. Maximising this quadratic form leads to successive sample principal components $\hat{\ell}_j$ and $\hat{\boldsymbol{v}}_j$ from the sample analog of (1):

$$\hat{\ell}_j = \max \left\{ \boldsymbol{v}^T S \boldsymbol{v} : \boldsymbol{v}^T \hat{\boldsymbol{v}}_{j'} = 0,\ j' < j,\ |\boldsymbol{v}| = 1 \right\}$$

Equivalently, we obtain for $j = 1, \dots, p$,

$$S\hat{\boldsymbol{v}}_j = \hat{\ell}_j \hat{\boldsymbol{v}}_j, \quad \hat{w}_j = X\hat{\boldsymbol{v}}_j.$$

Note the statistical convention: estimators derived from samples are shown with hats. Figure 1 shows a conventional picture illustrating PCA.

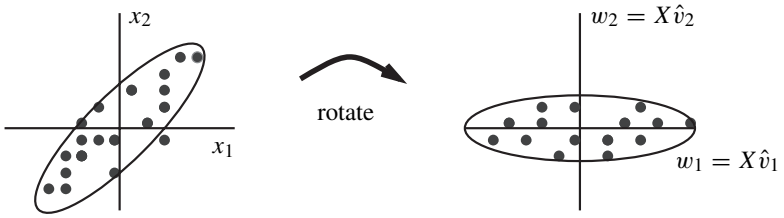


Figure 1. The n data observations are viewed as n points in p dimensional space, the p dimensions corresponding to the variables. The sample PC eigenvectors $\hat{\boldsymbol{v}}_j$ create a rotation of the variables into the new derived variables, with most of the variation on the low dimension numbers. In this two dimensional picture, we might keep the first dimension and discard the second.

Observed data are typically noisy, variable, and limited in quantity, so we are interested in the estimation errors

$$\hat{\ell}_j(X) - \ell_j, \quad \hat{\boldsymbol{v}}_j(X) - \boldsymbol{v}_j.$$

An additional key question in practice is: how many dimensions are "significant", or should be retained? One standard approach is to look at the percent of total variance explained by each of the principal components:

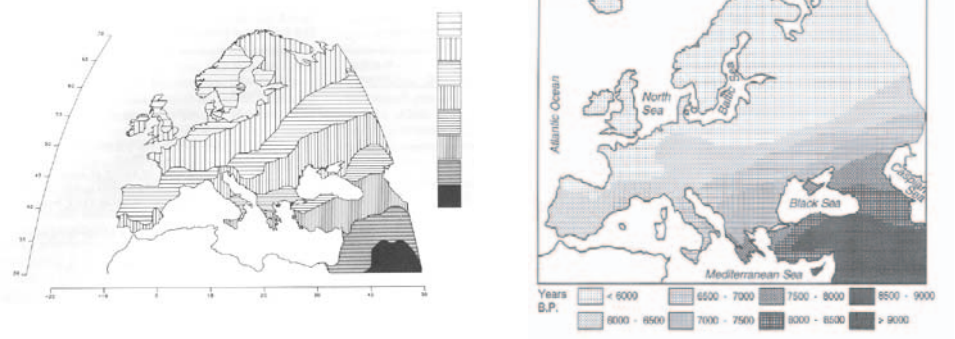
$$p_j = \hat{\ell}_j / \sum \hat{\ell}_{j'} = \hat{\ell}_j / \operatorname{tr} S.$$

An example. Menozzi, Piazza, and Cavalli-Sforza [70] is a celebrated example of the use of PCA in human genetics and anthropology. It was known from archaeological excavations that farming spread gradually from Near East across Europe 9000–5000 yrs ago (map below right). A motivating question was whether this represented spreading of the farmers themselves (and hence their genes) or transfer of technology to pre-existing populations (without a transfer of genes).

Menozzi et al. [70] brought genetic data to bear on the issue. Simplifying considerably, the data matrix X consisted of observations on the frequencies of alleles of $p = 38$ genes in human populations at $n = 400$ locations in Europe. The authors sought to combine information from the 38 genes to arrive at a low dimensional summary.

A special feature of the genetics data is that the observations i have associated locations loc$[i]$, so that it is possible to create a map from each of the principal components w_j, by making a contour plot of the values of the derived variable $w_j[i]$ at each of the sampling locations loc$[i]$. For example the first principal component (map below left) shows a clear trend from south-east to north-west, from Asia Minor to Britain and Scandinavia. The remarkable similarity of the PC map, derived from the gene frequencies, with the farming map, derived from archaeology, has been taken as strong support for the spread of the farmers themselves.

For the genetics data, the first component (out of 38) explains $p_1 = 27\%$ of the variance, the second $p_2 = 18\%$, and the third $p_3 = 11\%$. Thus, and this is typical, more than half the variation is captured in the first three PCs. The second and third, and even subsequent PCs also show patterns with important linguistic and migratory interpretations. For more detail, we refer to books of Cavalli-Sforza [23], [22], from which the maps below are reproduced with the kind permission of the author.



2.2. Gaussian and Wishart distributions. For quantitative analysis, we need more specific assumptions about the process generating the data. The simplest and most conventional model assumes that the p random variables $\mathsf{X}_1, \ldots, \mathsf{X}_p$ follow a p-variate Gaussian distribution $N_p(\mu, \Sigma)$, with mean μ and covariance matrix Σ, and

with probability density function for $\mathsf{X} = (\mathsf{X}_1, \ldots, \mathsf{X}_p)$ given by

$$f(\mathsf{X}) = \left|\sqrt{2\pi}\,\Sigma\right|^{-1/2} \exp\big\{ -\tfrac{1}{2}(\mathsf{X}-\mu)^T \Sigma^{-1}(\mathsf{X}-\mu)\big\}.$$

The observed sample is assumed to consist of n independent draws $X_1, \ldots, X_n$ from $\mathsf{X} \sim N_p(\mu, \Sigma)$, collected into a $p \times n$ data matrix $X = [X_1 \ldots X_n]$. When focusing on covariances, it is a slight simplification to assume that $\mu = 0$, as we shall here. In practice, this idealized model of independent draws from a Gaussian is generally at best approximately true – but we may find some reassurance in the dictum "All models are wrong, some are useful." [16]

The (un-normalized) cross product matrix $A = XX^T$ is said to have a p-variate *Wishart* distribution on n degrees of freedom. The distribution is named for John Wishart who in 1928 [97] derived the density function

$$f(A) = c_{n,p}|\Sigma|^{-n/2}|A|^{(n-p-1)/2} \exp\big\{ -\tfrac{1}{2}\operatorname{tr}(\Sigma^{-1}A)\big\},$$

which is supported on the cone of non-negative definite matrices. Here $c_{n,p}$ is a normalizing constant, and it is assumed that Σ is positive definite and that $n \geq p$.

The eigendecomposition of the Wishart matrix connects directly with principal components analysis. Start with a Gaussian data matrix, form the covariance S, yielding a Wishart density for $A = nS$. The eigenvalues and vectors of A, given by

$$Au_i = l_i u_i, \quad l_1 \geq \cdots \geq l_p \geq 0, \tag{2}$$

are related to the principal component eigenvalues and vectors *via*

$$l_i = n\hat{\ell}_i, \quad u_i = \hat{\boldsymbol{v}}_i.$$

Canonical correlations. We digress briefly from the PCA theme to mention one additional multivariate technique, also due to Hotelling [52], since it will help indicate the scope of the results. Given two sets of variables $\mathsf{X} = (\mathsf{X}_1, \ldots, \mathsf{X}_p)$ and $\mathsf{Y} = (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$, with a joint $p+q$-variate Gaussian distribution, we may ask for that linear combination of X that is most correlated with some linear combination of Y, seeking the canonical correlations

$$r_i^2 = \max_{u_i, v_i} \operatorname{Corr}(u_i^T \mathsf{X}, v_i^T \mathsf{Y}),$$

and the maximization is subject to $|u_i| = |v_i| = 1$.

To take an example from climatology [8]: the X variables might be sea surface temperatures at various ocean locations, and the Y variables might be land temperatures at various North American sites. The goal may be to find the combination of sea temperatures that is most tightly correlated with some combination of land temperatures. For a recent example in functional magnetic resonance imaging, see [44].

If we have n draws (X_i, Y_i), $i = 1, \ldots, n$ from the joint distribution, the sample version of this problem may be written as a generalized eigenequation that involves

two independent matrices A and B, each following p-variate Wishart distributions – on q and $n-q$ degrees of freedom respectively:

$$Av_j = r_j^2(A+B)v_j, \quad r_1^2 \geq \cdots \geq r_p^2.$$

The parameters of the Wishart distribution depend on those of the parent Gaussian distribution of the data – if X and Y are independent, then they both reduce to Wishart matrices with identity covariance matrix: $A \sim W_p(q, I)$ and $B \sim W_p(n-q, I)$.

The double Wishart setting. Suppose we have two independent Wishart matrices $A \sim W_p(n_1, I)$ and $B \sim W_p(n_2, I)$, with the degrees of freedom parameters $n_1, n_2 \geq p$. We call this the double Wishart setting. Two remarks: By writing Wishart distributions with *identity* matrices, we emphasize, for now, the "null hypothesis" situation in which there is no assumed structure (compare Section 4). Second, by taking a limit with $n_2 \to \infty$, one recovers the single Wishart setting.

Of central interest are the roots $x_i, i = 1, \ldots, p$ of the generalized eigenproblem constructed from A and B:

$$\det[x(A+B) - A] = 0. \tag{3}$$

The canonical correlations problem is a leading example. In addition, essentially all of the classical multivariate techniques involve an eigendecomposition that reduces to some form of this equation. Indeed, we may collect almost all the chapter titles in any classical multivariate statistics textbook (e.g. [3], [72], [68], [58]) into a table:

Double Wishart	Single Wishart
Canonical correlation analysis	Principal component analysis
Multivariate analysis of variance	Factor analysis
Multivariate regression analysis	Multidimensional scaling
Discriminant analysis	
Tests of equality of covariance matrices	

This table emphasizes the importance of finding the distribution of the roots of (3), which are basic to the use of these methods in applications.

Joint density of the eigenvalues. The joint null hypothesis distribution of the eigenvalues for canonical correlations and principal components was found in 1939. The results were more or less simultaneously obtained by five distinguished statisticians in three continents [41], [45], [54], [71], [81]:

$$f(x_1, \ldots, x_p) = c \prod_i w^{1/2}(x_i) \prod_{i<j} (x_i - x_j), \quad x_1 \geq \cdots \geq x_p, \tag{4}$$

with

$$w(x) = \begin{cases} x^{n-p-1}e^{-x} & \text{single Wishart,} \\ x^{n_1-p-1}(1-x)^{n_2-p-1} & \text{double Wishart.} \end{cases}$$

The normalizing constant c is given, using the multivariate Gamma function $\Gamma_p(a) = \pi^{p(p-1)/4} \prod_{i=1}^{p} \Gamma(a - (i-1)/2)$, by

$$c = \begin{cases} \frac{2^{-pn/2} \pi^{p^2/2}}{\Gamma_p(p/2)\Gamma_p(n/2)} & \text{single Wishart,} \\ \frac{\pi^{p^2/2}\Gamma_p((n_1+n_2)/2)}{\Gamma_p(p/2)\Gamma_p(n_1/2)\Gamma_p(n_2/2)} & \text{double Wishart.} \end{cases}$$

Thus, the density has a product term involving each of the roots one at a time, through a weight function w which one recognizes as the weight function for two of the classical families of orthogonal polynomials, Laguerre and Jacobi respectively.

The second product is the so-called "Jacobian" term, which arises in the change of variables to eigenvalue and eigenvector co-ordinates. It is this pairwise interaction term, also recognizable as a Vandermonde determinant (see (13) below), that causes difficulty in the distribution theory.

This result was the beginning of a rich era of multivariate distribution theory in India, Britain, the U.S., and Australia, summarized, for example, in [3], [72], [68]. While some of this theory became so complicated that it lost much influence on statistical practice, with new computational tools and theoretical perspectives the situation may change.

2.3. Random matrices. We detour around this theory and digress a moment to introduce the role of random matrix theory. Beginning in the 1950s, physicists began to use random matrix models to study quantum phenomena. In quantum mechanics the energy levels of a system, such as the nucleus of a complex atom, are described by the eigenvalues of a Hermitian operator H, the Hamiltonian: $H\psi_i = E_i\psi_i$, with $E_0 \leq E_1 \leq \cdots$. The low-lying energy levels can be understood by theoretical work, but at higher energy levels, for example in the millions, the analysis becomes too complicated.

Wigner proposed taking the opposite approach, and sought a purely statistical description of an "ensemble" of energy levels – that could yield properties such as their empirical distribution and the distribution of spacings. He further made the hypothesis that the local statistical behavior of energy levels (or eigenvalues) is well modeled by that of the eigenvalues of a random matrix. Thus the approximation is to replace the Hermitian operator H by a large finite *random* $N \times N$ matrix H_N.

One example of a statistical description that we will return to later is the celebrated SemiCircle Law [95], [96]. This refers to the eigenvalues of a so-called Wigner matrix H_N, with independent and identically distributed entries of mean 0 and a finite variance σ^2. With no further conditions on the distribution of the matrix entries, the empirical distribution $F_N(t) = \#\{i : x_i \leq t\}/N$ of the eigenvalues converges to a limit with density given by a semicircle:

$$dF_N(x\sigma\sqrt{N}) \to \frac{1}{4\pi}\sqrt{4 - x^2}dx.$$

Ensembles and orthogonal polynomials. Quite early on, there was interest in eigenvalue distributions whose densities could be described by more general families of weight functions than the Gaussian. For example, Fox and Kahn [43] used weight functions from the families of classical orthogonal polynomials. Analogies with statistical mechanics made it natural to introduce an additional (inverse temperature) parameter β, so that the eigenvalue density takes the form

$$f(x_1, \ldots, x_N) = c \prod_1^N w(x_i)^{\beta/2} \prod_{i<j} |x_i - x_j|^\beta. \tag{5}$$

At this time, it was only partially realized that in the case $\beta = 1$, these densities were already known in statistics. But the table shows that in fact, the three classical orthogonal polynomial weight functions correspond to the three most basic null eigenvalue distributions in multivariate statistics:

Table 1. The orthogonal polynomials are taken in the standard forms given in Szegö [86].

$w(x) =$				
	$e^{-x^2/2}$	Hermite	H_k	*Gaussian*
	$x^a e^{-x}$	Laguerre	L_k^a	*Wishart*
	$(1-x)^a(1+x)^b$	Jacobi	$P_k^{a,b}$	*Double Wishart*

Dyson [34] showed that physically reasonable symmetry assumptions restricted β to one of three values:

	Symmetry type	Matrix entries
$\beta = 1$	orthogonal	real
$\beta = 2$	unitary	complex
$\beta = 4$	symplectic	quaternion

Mathematically, the complex-valued case is always the easiest to deal with, but of course it is the real case that is of primary statistical (and physical) interest; though cases with complex data do occur in applications, notably in communications.

To summarize, the classical "null hypothesis" distributions in multivariate statistics correspond to the *italicized* eigenvalue densities in the

$$\left\{\begin{matrix}\text{Gaussian}\\ \textit{Laguerre}\\ \textit{Jacobi}\end{matrix}\right\} \left\{\begin{matrix}\textit{orthogonal}\\ \textit{unitary}\\ \text{symplectic}\end{matrix}\right\} \text{ ensemble.}$$

These are often abbreviated to LOE, JUE, etc. We have not italicized the Symplectic case for lack (so far) of motivating statistical applications (though see [4]).

Some uses of RMT in statistics. This table organizes some of the classical topics within RMT, and some of their uses in statistics and allied fields. This paper will

focus selectively (topics in italics), and in particular on largest eigenvalue results and their use for an important class of hypothesis tests, where RMT brings something quite new in the approximations.

Bulk	Graphical methods [92], [93] [finance [15], [77], communications [91]]
Linear Statistics	Hypothesis tests, distribution theory
Extremes	*Hypothesis tests, distribution theory,* role in proofs [21], [33]
Spacings	[[10], otherwise few so far]
General	Computational tools [65], role in proofs

Types of asymptotics. The coincidence of ensembles between RMT and statistical theory is striking, but what can it be *used* for? The complexity of finite sample size distributions makes the use of asymptotic approximations appealing, and here an interesting dichotomy emerges. Traditional statistical approximations kept the number of variables p fixed while letting the sample size $n \to \infty$. This was in keeping with the needs of the times when the number of variables was usually small to moderate.

On the other hand, the nuclear physics models were developed precisely for settings of high energy levels, and so the number of variables in the matrix models were large, as seen in the Wigner semi-circle limit. Interestingly, the many-variables limit of RMT is just what is needed for modern statistical theories with many variables.

	Stat: $\mathbb{C}$Wishart	RMT: Laguerre UE
Density	$\prod_{j=1}^{p} x_j^{n-p} e^{-x_j} \Delta(x)$	$\prod_{j=1}^{N} x_j^{\alpha} e^{-x_j} \Delta(x)$
# variables:	p	N
Sample size:	$n - p$	α

Comparison of the parameters in the statistics and RMT versions of the Wishart density in the table above leads to an additional important remark: in statistics, there is no necessary relationship between sample size n and number of variables p. We will consider below limits in which $p/n \to \gamma \in (0, \infty)$, so that γ could take any positive value. In contrast, the most natural asymptotics in the RMT model would take N large and α fixed. Thus, from the perspective of orthogonal polynomial theory, the statistics models lead to somewhat less usual Plancherel–Rotach asymptotics in which both parameters N *and* α of the Laguerre polynomials are large.

Spreading of sample eigenvalues. To make matters more concrete, we first describe this phenomenon by example. Consider $n = 10$ observations on a $p = 10$ variable Gaussian distribution with identity covariance. The sample covariance matrix follows a Wishart density with $n = p = 10$, and the *population* eigenvalues $\ell_j(I)$ are all equal to 1.

Nevertheless, there is an extreme spread in the *sample* eigenvalues $\hat{\ell}_j = \hat{\ell}_j(S)$, indeed in a typical sample

$$(\hat{\ell}_j) = (.\mathbf{003}, .036, .095, .16, .30, .51, .78, 1.12, 1.40, \mathbf{3.07})$$

and the variation is over three orders of magnitude! Without some supporting theory, one might be tempted to (erroneously) conclude from the sample that the population eigenvalues are quite different from one another.

This spread of sample eigenvalues has long been known, indeed it is an example of the repulsion of eigenvalues induced by the Vandermonde term in (4). It also complicates the estimation of population covariance matrices – also a long standing problem, discussed for example in [85], [47], [98], [27], [66].

The quarter circle law. Marčenko and Pastur [69] gave a systematic description of the spreading phenomenon: it is the version of the semi-circle law that applies to sample covariance matrices. We consider only the special case in which $A \sim W_p(n, I)$. The *empirical distribution function* (or empirical *spectrum*) counts how many sample eigenvalues fall below a given value t:

$$G_p(t) = p^{-1}\#\{\hat{\ell}_j \le t\}.$$

The empirical distribution has a limiting density g^{MP} if sample size n and number of variables p grow together: $p/n \to \gamma$:

$$g^{\mathrm{MP}}(t) = \frac{\sqrt{(b_+ - t)(t - b_-)}}{2\pi\gamma t}, \quad b_\pm = (1 \pm \sqrt{\gamma})^2.$$

The larger p is relative to n, the more spread out is the limiting density. In particular, with $p = n/4$, one gets the curve supported in $\left[\frac{1}{4}, \frac{9}{4}\right]$. For $p = n$, the extreme situation discussed above, the curve covers the full range from 0 to 4, which corresponds to the huge condition numbers seen in the sample.

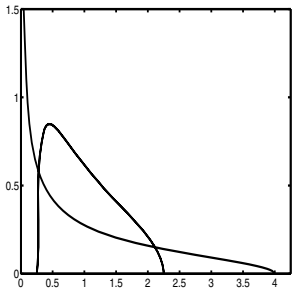


Figure 2. Marčenko–Pastur limit density for $\gamma = \frac{1}{4}$ and $\gamma = 1$.

3. Largest eigenvalue laws

Hypothesis test for largest eigenvalue. Suppose that in a sample of $n = 10$ observations from a $p = 10$ variate Gaussian distribution $N_{10}(0, \Sigma)$, we see a largest sample eigenvalue of 4.25. Is the observed value consistent with an identity covariance matrix (with all population eigenvalues = 1), even though 4.25 lies outside the support interval [0, 4] in the quarter-circle law?

In statistical terms, we are testing a *null hypothesis* of identity covariance matrix, $H_0 : \Sigma = I$ against an *alternative hypothesis* $H_A : \Sigma \neq I$ that Σ has some more general value. Normally, of course, one prefers the simpler model as a description of the data, unless forced by evidence to conclude otherwise.

One might compare 4.25 to random samples of the largest eigenvalue from the null hypothesis distribution (three examples yielding 2.91, 3.40 and 3.50); but what is actually needed is an approximation to the null hypothesis distribution of the largest sample eigenvalue:

$$P\{\hat{\ell}_1 > t : H_0 = W_p(n, I)\}.$$

Tracy–Widom limits. Random matrix theory leads to the approximate distribution we need. In the single Wishart case, assume that $A \sim W_p(n, I)$, either real or complex, that $p/n \to \gamma \in (0, \infty)$ and that $\hat{\ell}_1$ is the largest eigenvalue in equation (2). For the double Wishart case, assume that $A \sim W_p(n_1, I)$ is independent of $B \sim W_p(n_2, I)$, either real or complex together, and that $(p/n_1, p/n_2) \to (\gamma_1, \gamma_2) \in (0, 1)^2$, and that $\hat{\ell}_1$ is the largest generalized eigenvalue in equation (3). With appropriate centering μ_{np} and scaling σ_{np} detailed below, the distribution of the largest eigenvalue approaches one of the Tracy–Widom F_β laws:

$$P\{n\hat{\ell}_1 \leq \mu_{np} + \sigma_{np} s | H_0\} \to F_\beta(s). \tag{6}$$

These laws were first found by Craig Tracy and Harold Widom [88], [89] in the setting of the Gaussian unitary and orthogonal ensembles, *i.e.* (Hermitian) symmetric Gaussian matrices with i.i.d. entries. There are elegant formulas for the distribution functions

$$F_2(s) = \exp\left(-\int_s^\infty (x - s)^2 q(x)\, dx\right), \quad F_1(s)^2 = F_2(s) \exp\left(-\int_s^\infty q(x)\, dx\right).$$

in terms of the solution q to classical (Painlevé II) non-linear second-order differential equation

$$q'' = sq + 2q^3, \quad q(s) \sim \mathrm{Ai}(s) \text{ as } s \to \infty.$$

While q and F_β are somewhat tricky to compute numerically[1], from the point of view of applied data analysis with a software package, it is a special function just like the normal curve.

[1] At time of writing, for available software in MATLAB see http://math.arizona.edu/ momar/research.htm and [31] in S-PLUS see http://www.vitrum.md/andrew/MScWrwck/codes.txt and [9]. Both are based on ideas of [76] [see also [35]]

As will be seen from the explicit formulas (8)- (12) below, the scale of fluctuation σ_{np}/μ_{np} of the largest eigenvalue is $O(n^{-2/3})$ rather than the $O(n^{-1/2})$ seen in the Gaussian domain of attraction. This reflects the constraining effect of eigenvalue repulsion due to the Vandermonde term in (4).

The fact that the same limit arises in the single and double Wishart settings (Laguerre, Jacobi ensembles) is an instance of the universality discussed in P. Deift's paper [29] in this volume. In a different direction, one can modify the assumption that the i.i.d. entries in the $p \times n$ data matrix X are Gaussian. Soshnikov [82] shows that if $n - p = O(p^{1/3})$ and the matrix entries X_{ij} have sufficiently light (subGaussian) tails, then the largest eigenvalue continues to have a limiting Tracy–Widom distribution. The behavior of the largest eigenvalues changes radically with heavy tailed X_{ij} – for Cauchy distributed entries, after scaling by n^2p^2, [83], [84] shows a weak form of convergence to a Poisson process. If the density of the matrix entries behaves like $|x|^{-\mu}$, then [13] give physical arguments to support a phase transition from Tracy–Widom to Poisson at $\mu = 4$.

Second-order accuracy. To demonstrate the relevance of this limiting result for statistical application, it is important to investigate its accuracy when the parameters p and n are not so large. The generic rate of convergence of the left side of (6) to $F_\beta(s)$ is $O(p^{-1/3})$. However, small modifications in the centering and scaling constants μ and σ, detailed in the four specific cases below, lead to $O(p^{-2/3})$ errors, which one might call "second-order accuracy". With this improvement, (6) takes the form

$$\left|P\{n\hat{\ell}_1 \le \mu_{np} + \sigma_{np}s|H_0\} - F_\beta(s)\right| \le Ce^{-cs}p^{-2/3}. \tag{7}$$

This higher-order accuracy is reminiscent of that of the central limit, or normal, approximation to the t-test of elementary statistics for the testing of hypotheses about means, which occurs when the underlying data has a Gaussian distribution.

Single Wishart, complex data. Convergence in the form (6) was first established by Johansson [57] as a byproduct of a remarkable analysis of a random growth model, with

$$\mu^o_{np} = (\sqrt{n} + \sqrt{p})^2, \quad \sigma^o_{np} = (\sqrt{n} + \sqrt{p})\left(\frac{1}{\sqrt{n}} + \frac{1}{\sqrt{p}}\right)^{1/3}. \tag{8}$$

The second-order result (7) is due to El Karoui [38], If μ'_{np} and σ'_{np} denote the quantities in (8) with n and p replaced by $n + 1/2$ and $p + 1/2$, then the centering μ_{np} is a weighted combination of $\mu'_{n-1,p}$ and $\mu'_{n,p-1}$ and the scaling σ_{np} a similar combination of $\sigma'_{n-1,p}$ and $\sigma'_{n,p-1}$.

Single Wishart, real data. Convergence without rates in the form (6) to $F_1(s)$ with centering and scaling as in (8) is given in [60]. The assumption that $p/n \to \gamma \in (0, \infty)$ can be weakened to $\min\{n, p\} \to \infty$, as shown by El Karoui [37] – this extension is of considerable statistical importance since in many settings $p \gg n$ (see for example [40] in these proceedings).

Analysis along the lines of [61] suggests that the second order result (7) will hold with

$$\mu_{np} = \left(\sqrt{n-\tfrac{1}{2}} + \sqrt{p-\tfrac{1}{2}}\right)^2, \tag{9}$$

$$\sigma_{np} = \left(\sqrt{n-\tfrac{1}{2}} + \sqrt{p-\tfrac{1}{2}}\right)\left(\frac{1}{\sqrt{n-\tfrac{1}{2}}} + \frac{1}{\sqrt{p-\tfrac{1}{2}}}\right)^{1/3}. \tag{10}$$

Double Wishart, complex data. Set $\kappa = n_1 + n_2 + 1$ and define

$$\sin^2\left(\frac{\phi}{2}\right) = \frac{n_1 + \frac{1}{2}}{\kappa}, \quad \sin^2\left(\frac{\gamma}{2}\right) = \frac{p + \frac{1}{2}}{\kappa}. \tag{11}$$

Then

$$\mu_p^o = \sin^2\left(\frac{\phi+\gamma}{2}\right), \quad (\sigma_p^o)^3 = \frac{\sin^4(\phi+\gamma)}{4\kappa^2 \sin\phi \sin\gamma}. \tag{12}$$

The second-order result (7) (currently without the exponential bound, i.e., with $c = 0$) is established in [61] with μ_{np} a weighted combination of μ_p^o and μ_{p-1}^o and the scaling σ_{np} a similar combination of σ_p^o and σ_{p-1}^o.

Double Wishart, real data. Bound (7) is shown in [61] (again still for $c = 0$) with μ_{np} and σ_{np} given by (12) with $\kappa = n_1 + n_2 - 1$.

Approximation vs. tables for $p = 5$. With second-order correction, Tracy–Widom approximation turns out to be surprisingly accurate. William Chen [24], [25], [26] has computed tables of the exact distribution in the double Wishart, real data, case that cover a wide range of the three parameters p, n_1 and n_2, and allow a comparison with the asymptotic approximation. Even for $p = 5$ variables, the TW approximation is quite good, Figure 3, across the entire range of n_1 and n_2.

A different domain of attraction. The Tracy–Widom laws are quite different from other distributions in the standard statistical library. A full probabilistic understanding of their origin is still awaited (but see [78] for a recent characterization in terms of the low lying eigenvalues of a random operator of stochastic diffusion type). Instead, we offer some incomplete remarks as prelude to the original papers [88], [89].

Since one is looking at the largest of many eigenvalues, one might be reminded of extreme value theory, which studies the behavior of the largest of a collection of variables, which in the simplest case are independent. However, extreme value theory exploits the independence to study the maximum via products: $\{\max_{1\le i\le p} l_i \le t\} = \prod_{i=1}^p I\{l_i \le t\}$ For eigenvalues, however, the Jacobian term, or Vandermonde determinant,

$$V(l) = \prod_{i<j}(l_j - l_i) = \det[l_i^{k-1}]_{1\le i,k\le p}, \tag{13}$$

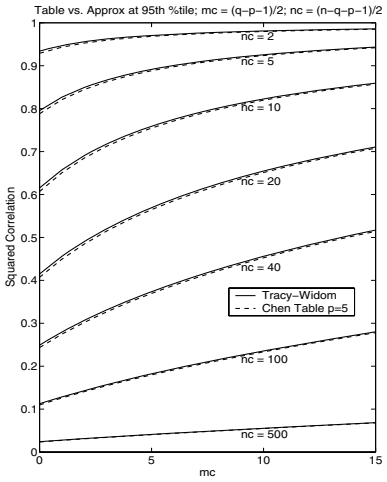


Figure 3. A comparison of the 95th percentile, relevant for hypothesis tests, from Chen's table (dashed line) and the Tracy–Widom approximation (solid line). Chen's parameters m_c, n_c are related to our double Wishart parameters n_1, n_2 by $m_c = (n_1 - p - 1)/2, n_c = (n_2 - p - 1)/2$.

changes everything. The theory uses the inclusion-exclusion relation:

$$\prod_{i=1}^{p} I\{l_i \le t\} = \sum_{k=0}^{p} (-1)^k \binom{p}{k} \prod_{i=1}^{k} I\{l_i > t\}.$$

The product structure of the left side, central to extreme value theory, is discarded in favor of the right side, which leads to an expression for $P\{\max_{1\le i\le p} l_i \le t\}$ in terms of so-called Fredholm determinants.

For example, it is shown by Tracy and Widom [90] that for complex data

$$P\{\max l_i \le t\} = \det(I - K_p \chi_{(t,\infty)}),$$

where χ_I is the indicator function for interval I, and $K_p \colon L_2 \to L_2$ is an operator whose kernel is the two-point correlation function

$$K_p(x, y) = \sum_{k=1}^{p} \phi_k(x)\phi_k(y),$$

written in terms of weighted orthonormal polynomials $\phi_k = h_k^{-1/2} w^{1/2} p_k$, where the polynomials p_k and weight functions w are given in Table 1 for the Gaussian, Wishart and double Wishart settings respectively.

For real data, Tracy and Widom [90] show that

$$P\{\max l_i \le t\} = \sqrt{\det(I - \mathcal{K}_p \chi_{(t,\infty)})},$$

where $\mathcal{K}_p$ is now a 2×2 matrix-valued operator on $L_2 \otimes L_2$. The corresponding kernel has form

$$\mathcal{K}_p(x, y) = \begin{pmatrix} \tilde{K}_p & -D_2\tilde{K}_p \\ \varepsilon_1\tilde{K}_p & \tilde{K}_p^T \end{pmatrix},$$

where $\tilde{K}_p = K_p + r_1$ and r_1 is a rank one kernel described in the three cases in more detail in [1], [42], [61]. Here D_2 and ε_1 denote partial differentiation and integration with respect to second and first variables respectively.

The expressions are thus somewhat more complicated in the real data case of primary interest in statistics. However they are amenable to analysis and approximation using orthogonal polynomial asymptotics near the largest zero, and to analysis based on the error terms to get the higher order approximation.

Back to the example. We asked if an observed largest eigenvalue of 4.25 was consistent with $H_0 : \Sigma = I$ when $n = p = 10$. The Tracy–Widom approximation using moments (9)–(10) yields a 6% chance of seeing a value more extreme than 4.25 even if "no structure" is present. Against the traditional 5% benchmark, this would not be strong enough evidence to discount the null hypothesis.

This immediately raises a question about the *power* of the largest root test, namely evaluation of

$$P\{\hat{\ell}_1 > t : W_p(n, \Sigma)\}$$

when $\Sigma \neq I$. How different from 1 does $\lambda_{\max}(\Sigma)$ need to be before H_0 is likely to be rejected? To this we now turn.

4. Beyond the null hypothesis

From the perspective of multivariate distribution theory, we have, in a sense, barely scratched the surface with the classical RMT ensembles, since they correspond to symmetric situations with no structure in the population eigenvalues or covariance matrix. Basic statistical quantities like power of tests and confidence intervals, as well as common applications in signal processing, genetics or finance, call for distributions under structured, asymmetric values for the covariance matrix Σ.

Statistical theory (pioneered by Alan James [56, e.g.], and summarized in the classic book by Robb Muirhead [72]) gives expressions for the classical multivariate eigenvalue distributions in more general settings, typically in terms of hypergeometric functions of matrix argument. For example, if $L = \operatorname{diag}(l_i)$ are the eigenvalues of $A \sim W_p(n, \Sigma)$, then the joint eigenvalue density

$$\frac{f_\Sigma(l_1, \ldots, l_p)}{f_I(l_1, \ldots, l_p)} = |\Sigma|^{-n/2} \exp\left\{\tfrac{1}{2} \operatorname{tr} L\right\} {}_0F_0\big(-\tfrac{1}{2}\Sigma^{-1}, L\big),$$

with

$$ {}_0F_0(S,T) = \int_{O(p)} \exp\{\mathrm{tr}(SUTU^T)\}\, dU, \tag{14} $$

and dU normalized Haar measure, but many other versions occur in the general theory. Despite recent major advances in computation by Alan Edelman and Plamen Koev [65], [64], and considerable work on the use of Laplace approximations (see e.g. [19], [20]), statistical theory would benefit from further serviceable approximations to these typically rather intractable objects.

Persistence of the Tracy–Widom limit. One basic question asks, in the setting of principal components analysis, for what conditions on the covariance Σ does the Tracy–Widom approximation continue to hold,

$$ P\{\hat{\ell}_1 \le \mu_{np}(\Sigma) + \sigma_{np}(\Sigma)s\} \to F_\beta(s), \tag{15} $$

perhaps with modified values for centering and scaling to reflect the value of Σ?

Fascinating answers are beginning to emerge. For example, El Karoui [39] establishes that (15) holds, along with explicit formulas for $\mu_{np}(\Sigma)$ and $\sigma_{np}(\Sigma)$, if enough eigenvalues accumulate near the largest eigenvalue, or if a small number of eigenvalues are not too isolated, as we describe below in a specific setting below.

Some of the results are currently restricted to complex data, because they build in a crucial way on the determinantal representation of the unitary matrix integral (the complex analog of (14))

$$ \int_{U(p)} \exp\{\mathrm{tr}\,\Sigma^{-1}ULU^*\}\, dU = c\, \frac{\det(e^{\pi_j l_k})}{V(\pi)V(l)} \tag{16} $$

known as the Harish-Chandra–Itzykson–Zuber formula [50], [55], see also [46]. Here the eigenvalues of Σ^{-1} are given by $\mathrm{diag}(\pi_j)$ and $V(l)$ is the Vandermonde determinant (13). While it is thought unlikely that there are direct analogs of (16), we very much need extensions of the distributional results to real data: there are some results in the physics literature [17], but any statistical consequences are still unclear.

Finite rank perturbations. We focus on a simple concrete model, and describe a phase transition phenomenon. Assume that

$$ \Sigma = \mathrm{diag}(\ell_1, \ldots, \ell_M, \sigma_e^2, \ldots, \sigma_e^2), \tag{17} $$

so that a fixed number M of population eigenvalues are greater than the base level σ_e^2, while both dimensions p and n increase in constant ratio $p/n \to \gamma \in (0, \infty)$.

First some heuristics: if all population eigenvalues are equal, then the largest sample eigenvalue $\hat{\ell}_1$ has $n^{-2/3}$ fluctuations around the upper limit of the support of the Marčenko–Pastur quarter circle law, the fluctuations being described by the Tracy–Widom law. For simplicity, consider $M = 1$ and $\sigma_e^2 = 1$. If ℓ_1 is large

and so very clearly separated from the bulk distribution, then one expects Gaussian fluctuations of order $n^{-1/2}$, and this is confirmed by standard perturbation analysis.

Baik et al. [7] describe, for *complex* data, a 'phase transition' that occurs between these two extremes. If $\ell_1 \le 1 + \sqrt{\gamma}$, then

$$n^{2/3}(\hat{\ell}_1 - \mu)/\sigma \Rightarrow \begin{cases} F_2 & \ell_1 < 1 + \sqrt{\gamma}, \\ \tilde{F}_2 & \ell_1 = 1 + \sqrt{\gamma} \end{cases}$$

where, from (8), we may set

$$\mu = (1 + \sqrt{\gamma})^2, \quad \sigma = (1 + \sqrt{\gamma})\left(1 + \sqrt{\gamma^{-1}}\right)^{1/3},$$

and $\tilde{F}_2$ is related to F_2 as described in Baik et al. [7]. On the other hand, if $\ell_1 > 1+\sqrt{\gamma}$,

$$n^{1/2}(\hat{\ell}_1 - \mu(\ell_1))/\sigma(\ell_1) \Rightarrow N(0, 1),$$

with

$$\mu(\ell_1) = \ell_1\left(1 + \frac{\gamma}{\ell_1 - 1}\right), \quad \sigma^2(\ell_1) = \ell_1^2\left(1 - \frac{\gamma}{(\ell_1 - 1)^2}\right). \tag{18}$$

Thus, below the phase transition the distribution of $\hat{\ell}_1$ is unchanged, Tracy–Widom, regardless of the value of ℓ_1. As ℓ_1 increases through $1 + \sqrt{\gamma}$, the law of $\hat{\ell}_1$ jumps to Gaussian and the mean increases with ℓ_1, but is biased low, $\mu(\ell_1) < \ell_1$, while the variance $\sigma^2(\ell_1)$ is lower than its value, ℓ_1^2, in the limit with p fixed.

A key feature is that the phase transition point $1 + \sqrt{\gamma}$, located at the zero of $\sigma(\ell_1)$, is buried deep inside the bulk, whose upper limit is $(1 + \sqrt{\gamma})^2$. A good heuristic explanation for this location is still lacking, though see El Karoui [39].

Further results on almost sure and Gaussian limits for both real and complex data, and under weaker distributional assumptions have been obtained by Paul [74] and Baik and Silverstein [6].

A recent example. Harding [49] illustrates simply this phase transition phenomenon in a setting from economics and finance. In a way this is a negative example for PCA; but statistical theory is as concerned with describing the limits of techniques as their successes.

Factor analysis models, of recently renewed interest in economics, attempt to "explain" the prices or returns of a portfolio of securities in terms of a small number of common "factors" combined with security-specific noise terms. It has been further postulated that one could estimate the number and sizes of these factors using PCA. In a 1989 paper that is widely cited and taught in economics and finance, Brown [18] gave a realistic simulation example that challenged this view, in a way that remained incompletely understood until recently.

Brown's example postulated four independent factors, with the parameters of the model calibrated to historical data from the New York Stock Exchange. The return in period t of security k is assumed to be given by

$$R_{kt} = \Sigma_{\nu=1}^{4} b_{k\nu} f_{\nu t} + e_{kt}, \quad k = 1, \ldots, p, \ t = 1, \ldots, T, \tag{19}$$

where it is assumed that $b_{k\nu} \sim N(\beta, \sigma_b^2)$, $f_{\nu t} \sim N(0, \sigma_f^2)$ and $e_{\nu t} \sim N(0, \sigma_e^2)$, all independently of one another. The population covariance matrix has the form (17) with $M = 4$ and

$$\ell_j = p\sigma_f^2(\sigma_b^2 + 4\beta\delta_{j1}) + \sigma_e^2, \quad j = 1, \ldots, 4. \tag{20}$$

Here δ_{j1} is the Kronecker delta, equal to 1 for $j = 1$ and 0 otherwise. Figure 4 (a) plots the population eigenvalues ℓ_1 (the dominant 'market' factor), the common value $\ell_2 = \ell_3 = \ell_4$ and the base value $\ell_5 = \sigma_e^2$ against p, the number of securities in the portfolio. One might expect to be able to recover an estimate of ℓ_2 from empirical data, but this turns out to be impossible for $p \in [50, 200]$ when $T = 80$ as shown in Figure 4 (b). First, the range of observed values of the top or market eigenvalue is biased upward from the true top eigenvalue. In addition, there are many sample eigenvalues above the anticipated value for ℓ_2.

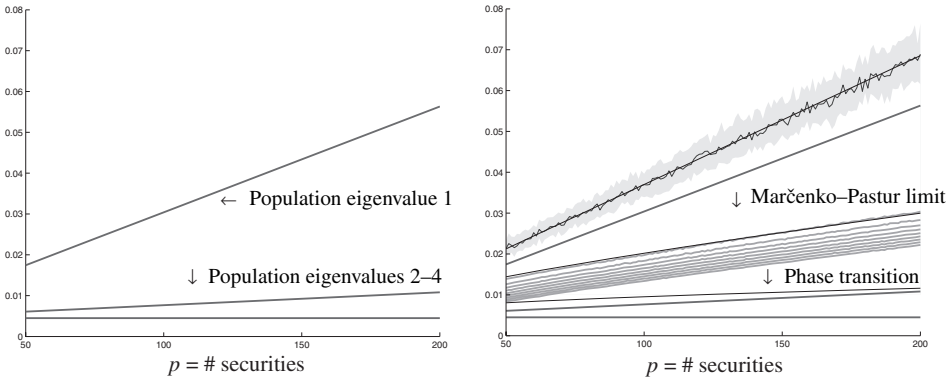


Figure 4. Population and sample eigenvalues for a four factor model (19) with $\beta = 0.6, \sigma_b = .4, \sigma_f = .01257, \sigma_e = .0671$. [Brown and Harding use $\beta = 1, \sigma_b = .1$; the values are modified here for legibility of the plot.] (a) Left panel: Population eigenvalues according to (20) (b) Right panel: The top sample eigenvalue in replications spreads about a sample average line which tracks the solid line given by (18), in particular overestimating the population value ℓ_1. The next nine sample eigenvalues fall at or below the Marčenko–Pastur upper limit, swamping the next three population eigenvalues.

Harding shows that one can directly apply the (real version) of the phase transition results previously discussed to fully explain Brown's results. Indeed, the inability to identify factors is because they fall on the wrong side of the phase transition $\sigma_e^2(1 + \sqrt{p/T})$, and so we can not expect the observed eigenvalue estimates to

exceed the Marčenko–Pastur upper bound $\sigma_e^2(1+\sqrt{p/T})^2$. Finally, the bias between the observed and true values of the top eigenvalue is also accurately predicted by the random matrix formulas (18).

5. Estimating eigenvectors

Most of the literature at the intersection of random matrix theory and statistics is focused on eigenvalues. We close with a few remarks on the estimation of eigen*vectors*. Of course, the question is only meaningful in non-symmetric settings when the covariance matrix Σ is not proportional to I. We again assume that $S \sim W_p(n, \Sigma)$ and now focus attention on covariance models which are a finite-rank perturbation of the identity[2]:

$$\Sigma = \sigma^2 I + \sum_{\nu=1}^{M} \lambda_\nu \theta_\nu \theta_\nu^T, \tag{21}$$

with $\lambda_1 \geq \cdots \geq \lambda_M > 0$ and $\{\theta_\nu\}$ orthonormal. We ask how well can the population eigenvectors θ_ν be estimated when both p and n are large.

First some remarks on how model (21) can arise from an *orthogonal factor* or *variance components* model for the data. Assume that the p-dimensional observations $X_i, i = 1, \ldots, n$ have the form

$$X_i = \mu + \sum_{\nu=1}^{M} \sqrt{\lambda_\nu} v_{\nu i} \theta_\nu + \sigma Z_i,$$

where $\{v_{\nu i} : 1 \leq \nu \leq M\}$ are i.i.d. $N(0,1)$, independently of $Z_i \sim N_p(0, I_p)$, for all i. If we further assume, for convenience, that $\mu = 0$, then with the sample covariance S defined as in Section 2, then $S \sim W_p(n, \Sigma)$. If we express X_i, θ_ν and Z_i in (22) in terms of co-ordinates in a suitable basis $\{e_k, k = 1, \ldots, p\}$ and write $f_{\nu i} = \sqrt{\lambda_\nu} v_{\nu i}$ we obtain

$$X_{ki} = \sum_{\nu=1}^{M} \theta_{k\nu} f_{\nu i} + \sigma Z_{ki},$$

in which $\theta_{k\nu}$ is viewed as the factor loading of the kth variable on the νth factor, and $f_{\nu i}$ is the factor score of the νth factor for the ith individual. As we have seen in (19) in the previous section, in economics X_{ki} may represent the return on the kth security in time period i.

[2]The situation is different in *functional* principal components analysis, where smoothness of the observed data (functions) leads to covariance matrices with smoothly decaying eigenvalues. For entries into this literature, see for example [28], [14], [48].

Assume that $\lambda_1 > \cdots > \lambda_M > 0$. Let $\hat{\theta}_\nu$ denote the normalized sample eigenvectors of S (denoted $\hat{\boldsymbol{v}}_\nu$ in Section 2.1) associated with the M largest sample eigenvalues. In classical asymptotics, with n large and p fixed, there is a well understood Gaussian limit theory:

$$\sqrt{n}(\hat{\theta}_\nu - \theta_\nu) \to N_p(0, \Gamma_\nu) \tag{22}$$

where Γ_ν is given, for example, in [2], [3].

The situation is radically different when $p/n \to \gamma > 0$ – indeed, ordinary PCA is necessarily inconsistent:

$$\langle \hat{\theta}_\nu, \theta_\nu \rangle \to \begin{cases} 0 & \lambda_\nu \in [0, \sqrt{\gamma}], \\ \frac{1-\gamma/\lambda_\nu^2}{1+\gamma/\lambda_\nu} & \lambda_\nu > \sqrt{\gamma}. \end{cases}$$

For signal strengths λ below the phase transition just discussed, nothing can be estimated – the estimate is asymptotically orthogonal to the truth. The angle decreases as λ_ν grows, but is never exactly consistent.

This result has emerged in several literatures, starting in the learning theory/statistical physics community, with non-rigorous arguments based on the replica method [79], [53], where this phenomenon has been termed "retarded learning" [11], [94]. More recently, rigorous results have been obtained [62], [74], [73].

To obtain consistent estimates, further assumptions are needed. One plausible situation is that in which there exists a basis $\{e_k\}_{k=1:p}$ in which it is believed that the vectors θ_ν have a sparse representation. In microarray genetics, for example X_{ki} might be the expression of gene k in the ith patient, and it may be believed that (in the standard basis) each factor ν is related to only a small number of genes [67]. In EEG studies of the heart, the beat-to-beat cycle might be expressed in a wavelet basis, in which the components of variation θ_ν may well be sparsely represented [62].

We briefly describe results in the sparse setting of work in progress by D. Paul, and by Paul and the author. For simplicity only, we specialize to $M = 1$. The error of estimation, or loss, of $\hat{\theta}$ is measured on unit vectors by

$$L(\hat{\theta}, \theta) = \|\hat{\theta} - \mathrm{sign}(\langle \hat{\theta}, \theta \rangle)\theta\|^2 = 4 \sin^2 \tfrac{1}{2} \angle(\hat{\theta}, \theta).$$

If $\hat{\theta}$ is now the ordinary PCA estimate of θ, and if $p/n \to \gamma > 0$, then to first order,

$$EL(\hat{\theta}, \theta) = \frac{p}{nh(\lambda)}(1 + o(1)), \quad h(\lambda) = \frac{\lambda^2}{1+\lambda},$$

from which it is natural to define the "per-variable" noise level $\tau_n = 1/\sqrt{nh(\lambda)}$.

As is common in non-parametric estimation theory, we use ℓ_q norm, $q < 2$, as a measure of sparsity: with $\|\theta\|_q^q = \sum_k |\theta_k|^2$, define $\Theta_q(C) = \{\theta \in S^{p-1} : \|\theta\|_q \le C\}$. Paul proposes a two-step procedure for selecting a reduced subset of variables on which to perform PCA, resulting in an estimator $\hat{\theta}^P$ for which

$$\sup_{\theta \in \Theta_q(C)} EL(\hat{\theta}^P, \theta) \le K(C) \log p \cdot m_n \tau_n^2. \tag{23}$$

Here m_n is an effective dimension parameter, equal to $(C^2/(\tau^2 \log p))^{q/2}$ in the "sparse" case when this is smaller than $c_1 p$, and equal to p in the contrary "dense" case. Lower bounds are obtained that show that this estimation error is optimal, in a minimax sense, up to factors that are at most logarithmic in p.

Bounds such as (23) are reminiscent of those for estimation of sparse *mean* sequences in white Gaussian noise [32], [12], [59]. An observation due to Paul provides a link between eigenvector estimation and the estimation of means. Again with $M = 1$ for simplicity, let $\hat{\theta}$ be the ordinary PCA estimate of θ. Write $\hat{C} = \langle \hat{\theta}, \theta \rangle$ and $\hat{\theta}^\perp = \hat{\theta} - C\theta$. Then, with $\hat{S}^2 = 1 - \hat{C}^2$, in the decomposition

$$\hat{\theta} = \hat{C}\theta + \hat{S}U, \quad U = \hat{\theta}^\perp / \|\hat{\theta}^\perp\|$$

it happens that U is uniformly distributed on a copy of S^{p-2}, independently of $\hat{S}$.

It is a classical remark that a high-dimensional isotropic Gaussian vector is essentially concentrated uniformly on a sphere. We may reverse this remark by starting with a uniform distribution on a sphere, and introducing an ultimately inconsequential randomization with $R^2 \sim \chi^2_{p-1}/p$ and $z_1 \sim N(0, 1/p)$ with the result that $z = RU + z_1\theta$ has an $N_p(0, I)$ distribution. This leads to a signal-in-Gaussian-noise representation

$$Y = \hat{C}\theta + \tau^2 z, \quad \tau^2 = 1/(2nh(\hat{\lambda})),$$

Work is in progress to use this connection to improve the extant estimation results for eigenvectors.

6. Coda

One may expect a continuing fruitful influence of developments in random matrix theory on high dimensional statistical theory, and perhaps even some flow of ideas in the opposite direction. A snapshot of current trends may be obtained from http://www.samsi.info/workshops/2006ranmat-opening200609.shtml, being the presentations from the opening workshop of a semester devoted to high dimensional inference and random matrices at the NSF Statistics and Applied Mathematics Institute in Fall 2006.

References

[1] Adler, M., Forrester, P. J., Nagao, T., and van Moerbeke, P., Classical skew orthogonal polynomials and random matrices. *J. Statist. Physics* **99** (1–2) (2000), 141–170.

[2] Anderson, T. W., Asymptotic theory for principal component analysis. *Ann. Math. Statist.* **34** (1963), 122–148.

[3] Anderson, T. W., *An Introduction to Multivariate Statistical Analysis*. 2nd ed., Wiley Ser. Probab. Math. Statist. Probab. Math. Statist., John Wiley & Sons, Inc., New York 1984.

[4] Andersson, S. A., Brøns, H. K., and Jensen, S. T., Distribution of eigenvalues in multivariate statistical analysis. *Ann. Statist.* **11** (2) (1983), 392–415.

[5] Bai, Z. D., Methodologies in spectral analysis of large dimensional random matrices, a review. *Statist. Sinica* **9** (1999), 611–677.

[6] Baik, J., and Silverstein, J. W., Eigenvalues of large sample covariance matrices of spiked population models. *J. Multivariate Anal.* **97** (2006), 1382–1408.

[7] Baik, J., Ben Arous, G., and Péché, S., Phase transition of the largest eigenvalue for nonnull complex sample covariance matrices. *Ann. Probab.* **33** (5) (2005), 1643–1697.

[8] Barnett, T. P., and Preisendorfer, R., Origins and levels of monthly and seasonal forecast skill for United States surface air temperatures determined by canonical correlation analysis. *Monthly Weather Review* **115** (1987), 1825–1850.

[9] Bejan, A., Largest eigenvalues and sample covariance matrices. Tracy-Widom and Painlevé II: computational aspects and realization in S-Plus with applications. http://www.vitrum.md/andrew/TWinSplus.pdf, 2005.

[10] Ben Arous, G., and Péché, S., Universality of local eigenvalue statistics for some sample covariance matrices. *Comm. Pure Appl. Math.* **58** (10) (2005), 1316–1357.

[11] Biehl, M., and Mietzner, A., Statistical mechanics of unsupervised structure recognition. *J. Phys. A* **27** (6) (1994), 1885–1897.

[12] Birgé. L., and Massart, P., Gaussian model selection. *J. Eur. Math. Soc.* (*JEMS*) **3** (2001), 203–268.

[13] Biroli, G., Bouchaud, J.-P., and Potters, M., On the top eigenvalue of heavy-tailed random matrices. Preprint, 2006; arXiv:cond-mat/0609070.

[14] Bosq, D., *Linear processes in function spaces*. Lecture Notes in Statist. 149, Springer-Verlag, New York 2000.

[15] Bouchaud, J.-P., and Potters, M., *Theory of Financial Risk and Derivative Pricing: From Statistical Physics to Risk Management*. Cambridge University Press, Cambridge 2003.

[16] Box, G. E. P., Robustness in the strategy of scientific model building. In R. L. Launer and G. N. Wilkinson, editors, *Robustness in Statistics* (R. L. Launer and G. N. Wilkinson, eds.), Academic Press, New York 1979, 201–236.

[17] Brézin, E., and Hikami, S., New correlation functions for random matrices and integrals over supergroups. *J. Phys. A* **36** (3) (2003), 711–751.

[18] Brown, S. J., The number of factors in security returns. *J. Finance* **XLIV** (5) (1989), 1247–1261.

[19] Butler, R. W., and Wood, A. T. A., Laplace approximations for hypergeometric functions with matrix argument. *Ann. Statist.* **30** (4) (2002), 1155–1177.

[20] Butler, R. W., and Wood, A. T. A., Laplace approximations to hypergeometric functions of two matrix arguments. *J. Multivariate Anal.* **94** (1) (2005), 1–18.

[21] Candès, E., and Tao, T., Near Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? *IEEE Trans. Inform. Theory* **52** (12) (2006), 5406–5425.

[22] Cavalli-Sforza, L. L., *Genes, peoples, and languages*. North Point Press, New York 2000.

[23] Cavalli-Sforza, L. L., Menozzi, P., and Piazza, A., *The history and geography of human genes*. Princeton University Press, Princeton, N.J., 1994.

[24] Chen, W. R., Some new tables of the largest root of a matrix in multivariate analysis: A computer approach from 2 to 6, 2002. Presented at the 2002 American Statistical Association.

[25] Chen, W. R., Table for upper percentage points of the largest root of a determinantal equation with five roots. *InterStat* (5), February 2003. http://interstat.statjournals.net/YEAR/2003/abstracts/0302005.php.

[26] Chen, W. R., The new table for upper percentage points of the largest root of a determinantal equation with seven roots. *InterStat* (1), September 2004. http://interstat.statjournals.net/YEAR/2004/abstracts/0409001.php.

[27] Daniels, M. J., and Kass, R. E., Shrinkage estimators for covariance matrices. *Biometrics* **57** (4) (2001), 1173–1184.

[28] Dauxois, J., Pousse, A., and Romain, Y., Asymptotic theory for the principal component analysis of a vector random function: some applications to statistical inference. *J. Multivariate Anal.* **12** (1) (1982), 136–154.

[29] Deift, P., Universality for mathematical and physical systems. *Proceedings of the International Congress of Mathematicians* (Madrid, 2006), Volume I, EMS Publishing House, Zürich 2007, 125–152.

[30] Diaconis, P., Patterns in eigenvalues: the 70th Josiah Willard Gibbs lecture. *Bull. Amer. Math. Soc.* (N.S.) **40** (2) (2003), 155–178.

[31] Dieng, M., Distribution Functions for Edge Eigenvalues in Orthogonal and Symplectic Ensembles: Painlevé Representations II. arXiv:math.PR/0506586.

[32] Donoho, D. L., and Johnstone, I. M., Ideal spatial adaptation via wavelet shrinkage. *Biometrika* **81** (1994), 425–455.

[33] DDonoho, D. L., For most large underdetermined systems of linear equations the minimal l_1-norm solution is also the sparsest solution. *Comm. Pure Appl. Math.* **59** (6) (2006), 797–829.

[34] Dyson, F. J., The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics. *J. Math. Phys.* **3** (6) (1962), 1199–1215.

[35] Edelman, A., and Persson, P.-O., Numerical Methods for Eigenvalue Distributions of Random Matrices. Preprint, 2005; arXiv:math-ph/0501068.

[36] Edelman, A., and Rao, N. R., Random matrix theory. *Acta Numer.* **14** (2005), 233–297.

[37] El Karoui, N., On the largest eigenvalue of Wishart matrices with identity covariance when n, p and p/n tend to infinity. Preprint, 2003; arXiv:math. ST/0309355.

[38] El Karoui, N., A rate of convergence result for the largest eigenvalue of complex white Wishart Matrices. *Ann. Probab.* **34** (2006), 2077–2117.

[39] El Karoui, N., Tracy-Widom limit for the largest eigenvalue of a large class of complex Wishart matrices. *Ann. Probab.* **35** (2007).

[40] Fan J., and Li, R., Statistical challenges with high dimensionality: feature selection in knowledge discovery. *Proceedings of the International Congress of Mathematicians* (Madrid, 2006), Volume III, EMS Publishing House, Zürich 2006, 595–622.

[41] Fisher, R. A., The sampling distribution of some statistics obtained from non-linear equations. *Ann. Eugenics* **9** (1939), 238–249.

[42] Forrester, P. J., Log-gases and Random matrices. http://www.ms.unimelb. edu.au/~matpjf/matpjf.html. Book manuscript, 2004.

[43] Fox, D., and Kahn, P. B., Higher order spacing distributions for a class of unitary ensembles. *Phys. Rev.* **134** (5B) (1964), B1151–B1155.

[44] Friman, O., Cedefamn, J., Lundberg, P., Borga, M., and H. Knutsson, H., Detection of neural activity in functional MRI using canonical correlation analysis. *Magnetic Resonance in Medicine* **45** (2001), 323–330.

[45] Girshick, M. A., On the sampling theory of roots of determinantal equations. *Ann. Math. Statist.* **10** (1939), 203–224.

[46] Gross, K. I., and Richards, D. St. P., Total positivity, spherical series, and hypergeometric functions of matrix argument. *J. Approx. Theory* **59** (2) (1989), 224–246.

[47] Haff, L. R., The variational form of certain Bayes estimators. *Ann. Statist.* **19** (1991), 1163–1190.

[48] Hall, P., Müller, H.-G., and Wang, J.-L., Properties of principal component methods for functional and longitudinal data analysis. *Ann. Statist.* **34** (3) (2006), 1493–1517.

[49] Harding, M. C., Explaining the single factor bias of arbitrage pricing models in finite samples. Dept. of Economics, MIT, 2006; http://www.mit.edu/~mharding/.

[50] Harish-Chandra, Differential operators on a semisimple Lie algebra. *Amer. J. Math.* **79** (1) (1957), 87–120.

[51] Hotelling, H., Analysis of a complex of statistical variables into principal components. *J. Educational Psychology* **24** (1933), 417–441, 498–520.

[52] Hotelling, H., Relations between two sets of variates. *Biometrika* **28** (1936), 321–377.

[53] Hoyle, D. C., and Rattray, M., Principal-component-analysis eigenvalue spectra from data with symmetry breaking structure. *Phys. Rev. E* **69** (2004), (026124).

[54] Hsu, P. L., On the distribution of roots of certain determinantal equations. *Ann. Eugenics* **9** (1939), 250–258.

[55] Itzykson, C., and Zuber, J.-B., The planar approximation. II. *J. Math. Phys.* **21** (3) (1980), 411–421.

[56] James, A. T., Distributions of matrix variates and latent roots derived from normal samples. *Ann. Math. Statist.* **35** (1964), 475–501.

[57] Johansson, K., Shape fluctuations and random matrices. *Commun. Math. Phys.* **209** (2000), 437–476.

[58] Johnson, R. A., and Wichern, D. W., *Applied Multivariate Statistical Analysis*. 5th ed., Prentice Hall, Englewood Cliffs, NJ, 2002.

[59] Johnstone, I. M., and Silverman, B. W., Needles and straw in haystacks: Empirical Bayes estimates of possibly sparse sequences. *Ann. Statist.* **32** (2004), 1594–1649.

[60] Johnstone, I. M., On the distribution of the largest eigenvalue in principal components analysis. *Ann. Statist.* **29** (2001), 295–327.

[61] Johnstone, I. M., Canonical correlation analysis and Jacobi ensembles: Tracy-Widom limits and rates of convergence. Manuscript, 50pp, August 2006.

[62] Johnstone, I. M., and Lu, A. Y., Sparse principal components analysis. Technical report, Stanford University, Dept. of Statistics, 2004; tentatively accepted, *J. Appl. Statist. Sci.*

[63] Jolliffe, I. T., *Principal Component Analysis*. Springer Ser. Statist., Springer, 2nd edition, New York 2002.

[64] Koev, P., Software `mhg`, `mhgi` for hypergeometric function of a matrix argument. 2006; http://www-math.mit.edu/~plamen/.

[65] Koev, P., and Edelman, A., The efficient evaluation of the hypergeometric function of a matrix argument. *Math. Comp.* **75** (254) (2006), 833–846.

[66] Ledoit, O., and Wolf, M., A well-conditioned estimator for large-dimensional covariance matrices. *J. Multivariate Analysis* **88** (2004), 365–411.

[67] Lucas, J., Carvalho, C., Wang, Q., Bild, A., Nevins, J., and West, M., Sparse statistical modelling in gene expression genomics. In *Bayesian Inference for Gene Expression and Proteomics* (K. A. Do, P. Mueller, and M. Vannucci, eds.), Cambridge University Press, Cambridge 2006, 155–176.

[68] Mardia, K. V., Kent, J. T., and Bibby, J. M., *Multivariate Analysis*. Academic Press, London, New York, Toronto, Ont., 1979.

[69] Marčenko, V. A., and Pastur, L. A., Distributions of eigenvalues of some sets of random matrices. *Math. USSR-Sb.* **1** (1967), 507–536.

[70] Menozzi, P., Piazza, A., and Cavalli-Sforza, L., Synthetic maps of human gene frequencies in Europeans. *Science* **201** (4358) (1978), 786–792.

[71] Mood, A. M., On the distribution of the characteristic roots of normal second-moment matrices. *Ann. Math. Statist.* **22** (1951), 266–273.

[72] Muirhead, R. J., *Aspects of Multivariate Statistical Theory*. Wiley Ser. Probab. Math. Statist. Probab. Math. Statist., John Wiley & Sons, Inc., New York 1982.

[73] Onatski, A., Asymptotic distribution of the principal components estimator of large factor models when factors are relatively weak. Dept. of Economics, Columbia University, 2006; http://www.columbia.edu/~ao2027/papers1.html.

[74] Paul, D., Asymptotics of sample eigenstructure for a large dimensional spiked covariance model. Technical report, Department of Statistics, Stanford University, 2004; *Statist. Sinica*, to appear.

[75] Pearson, K., On lines and planes of closest fit to systems of points in space. *Philosophical Magazine* **2** (6) (1901), 559–572,

[76] Persson, P.-O., Numerical methods for random matrices. 2002; http://www.mit.edu/~persson/numrand_report.pdf.

[77] Potters, M., Bouchaud, J. P., and Laloux, L., Financial applications of random matrix theory: Old laces and new pieces. *Acta Phys. Polon. B* **36** (2005), 2767–2784.

[78] Ramírez, J., Rider, B., and Virág, B., Beta ensembles, stochastic Airy spectrum, and a diffusion. 2006.

[79] Reimann, P., Van den Broeck, C., and Bex, G. J., A Gaussian scenario for unsupervised learning. *J. Phys. A* **29** (13) (1996), 3521–3535.

[80] Roweis, S. T., and Saul, L. K., Nonlinear Dimensionality Reduction by Locally Linear Embedding. *Science* **290** (5500) (2000), 2323–2326.

[81] Roy, S. N., p-statistics or some generalizations in analysis of variance appropriate to multivariate problems. *Sankhyā* **4** (1939), 381–396.

[82] Soshnikov, A., A note on universality of the distribution of the largest eigenvalues in certain classes of sample covariance matrices. *J. Statist. Phys.* **108** (2002), 1033–1056.

[83] Soshnikov, A., Poisson statistics for the largest eigenvalues in random matrix ensembles. In *Mathematical physics of quantum mechanics*, Lecture Notes in Phys. 690, Springer-Verlag, Berlin 2006, 351–364.

[84] Soshnikov, A., and Fyodorov, Y. V., On the largest singular values of random matrices with independent Cauchy entries. *J. Math. Phys.* **46** (3) (2005), 033302.

[85] Stein, C., Estimation of a covariance matrix. Unpublished manuscript, Stanford University, ca. 1977.

[86] Szegö, G., *Orthogonal Polynomials.* 3rd ed., Amer. Math. Soc. Colloq. Publ. 23, Amer. Math. Soc., Providence, R.I., 1967.

[87] Tenenbaum, J. B., de Silva, V., and Langford, J. C., A Global Geometric Framework for Nonlinear Dimensionality Reduction. *Science* **290** (5500) (2000), 2319–2323.

[88] Tracy, C. A., and Widom, H., Level-spacing distributions and the Airy kernel. *Comm. Math. Phys.* **159** (1994), 151–174.

[89] Tracy, C. A., and Widom, H., On orthogonal and symplectic matrix ensembles. *Comm. Math. Phys.* **177** (1996), 727–754.

[90] Tracy, C. A., and Widom, H., Correlation functions, cluster functions, and spacing distributions for random matrices. *J. Statist. Phys.* **92** (1998), 809–835.

[91] Tulino, A., and Verdu, S., *Random Matrix Theory and Wireless Communications*. Now Publishers Inc., 2004.

[92] Wachter, K. W., The strong limits of random matrix spectra for sample matrices of independent elements. *Ann. Probab.* **6** (1978), 1–18.

[93] Wachter, K. W., The limiting empirical measure of multiple discriminant ratios. *Ann. Statist.* **8** (1980), 937–957.

[94] Watkin, T. L. H., and Nadal, J.-P., Optimal unsupervised learning. *J. Phys. A* **27** (6) (1994), 1899–1915.

[95] Wigner, E. P., Characteristic vectors of bordered matrices of infinite dimensions. *Ann. of Math.* **62** (1955), 548–564.

[96] Wigner, E. P., On the distribution of the roots of certain symmetric matrices. *Ann. of Math.* **67** (1958), 325–328.

[97] Wishart, J., The generalised product moment distribution in samples from a normal multivariate population. *Biometrika* **20A** (1–2) (1928), 32–52.

[98] Yang, R., and Berger, J. O., Estimation of a covariance matrix using the reference prior. *Ann. Statist.* **22** (1994), 1195–1211.

Department of Statistics, Sequoia Hall, Stanford University, Stanford CA 94305, U.S.A.
E-mail: imj@stanford.edu

Iwasawa theory and generalizations

Kazuya Kato

Abstract. This is an introduction to Iwasawa theory and its generalizations. We discuss some main conjectures and related subjects.

Mathematics Subject Classification (2000). Primary 11R23; Secondary 11G40, 14G10.

Keywords. Iwasawa theory, zeta function.

Zeta values are infinitely attractive objects. They appear in many areas of mathematics, and also in physics. They lead us to the profound mysteries of mathematics.

Iwasawa theory is the best theory at present to understand the arithmetic meaning of zeta values. Classical Iwasawa theory describes the relation between zeta values and ideal class groups. It has been generalized to the study of the relation between zeta values and more general arithmetic objects (rational points and Selmer groups of elliptic curves, Galois representations, Galois cohomology groups, ...). Diagrammatically, we have

$$\begin{array}{ccc} \text{zeta values} & \longleftrightarrow & \text{ideal class groups, Selmer groups, } \ldots. \\ \text{(analytic objects)} & & \text{(arithmetic objects)} \end{array}$$

The mysterious point is that analytic objects and arithmetic objects are connected in spite of the vast distance between their innate natures. Via zeta values, arithmetic, algebra, analysis, geometry intersect. Deep and unexpected problems arise there.

The aim of this paper is to review some results, methods, and problems in Iwasawa theory and its generalizations. The author regrets that he cannot cover many important studies in this field.

The organization of this paper is as follows. In §1, we describe history. In §2, we describe the cyclotomic Iwasawa theory of elliptic curves comparing it with classical Iwasawa theory. In §3, we present non-commutative Iwasawa theory.

The author is very grateful to Professor John Coates for advice.

1. Overview

1.1. Euler. The study of zeta values was started by Euler. In 1735, Euler proved $1 + 1/2^2 + 1/3^2 + 1/4^2 + 1/5^2 + \cdots = \pi^2/6$. He was happy that he solved the

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

difficult question "what is the sum of the inverses of all squares?" and also that the answer he found (the appearance of π) was surprising.

Riemann's zeta function $\zeta(s)$ is defined as $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ for complex numbers s such that $\Re(s) > 1$, and by analytic continuation, it is extended to the whole complex s-plane as a meromorphic function which is holomorphic at any $s \neq 1$. The above result of Euler says that $\zeta(2) = \pi^2/6$.

Euler proved that $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, and more generally, for any even integer $r \geq 2$, he showed that $\zeta(r)/\pi^r \in \mathbb{Q}$. Euler did not know the theory of analytic continuation, but he had a method to find the correct values of $\zeta(s)$ at integers ≤ 0:

$$\zeta(0) = -1/2, \quad \zeta(r) = 0 \text{ for any even integer } r < 0,$$

$$\zeta(1-r) = 2 \cdot (r-1)! \cdot \zeta(r)/(2\pi i)^r \in \mathbb{Q}^\times \text{ if } r > 0 \text{ is even},$$

$$\zeta(-1) = -1/12, \ \zeta(-3) = 1/120, \ \zeta(-5) = -1/(2^2 \cdot 3^2 \cdot 7),$$

$$\zeta(-7) = 1/(2^4 \cdot 3 \cdot 5), \ \zeta(-9) = -1/(2^2 \cdot 3 \cdot 11), \ \zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13), \ldots.$$

Note that the prime number 691 suddenly appears as the numerator of $\zeta(-11)$.

1.2. Kummer. In the middle of 19th century, Kummer discovered that the special values of the Riemann zeta function have the following remarkable arithmetic properties: (1) a relation with the arithmetic of cyclotomic fields, and (2) a p-adic property. Neither could possibly be imagined from the analytic definition of $\zeta(s)$. These discoveries (1), (2) were the starting point of Iwasawa theory.

(1) *Kummer's criterion.* Let p be a prime number. Then p divides the numerator of $\zeta(r)$ for some negative odd integer r if and only if the class number of $\mathbb{Q}(\zeta_p)$ is divisible by p.

This (1) for example shows that the class number of $\mathbb{Q}(\zeta_{691})$ is divisible by 691 since the numerator of $\zeta(-11)$ is divisible by 691.

Recall that for a number field F (a finite extension of $\mathbb{Q}$) the class number of F is the order of the ideal class group $\mathrm{Cl}(F)$ of F, which is a finite group. We recall that the ideal class group of F is defined to be the quotient of the multiplicative group of non-zero fractional ideals of F divided by the subgroup consisting of principal ideals. It is the most important group in algebraic number theory. Unique factorization into prime elements in F holds if and only if $\mathrm{Cl}(F) = \{1\}$, and the failure of unique factorization in F becomes big (and the arithmetic of F becomes complicated) if the ideal class group of F is big. Kummer tried to prove Fermat's last theorem by studying the arithmetic of cyclotomic fields $\mathbb{Q}(\zeta_p)$ for odd primes p (where we denote by ζ_n a primitive n-th root of 1). The equation $x^p + y^p = z^p$ is rewritten as $\prod_{k=1}^{p}(x+\zeta_p^k y) = z^p$ in the multiplicative form, and hence the theory of multiplicative factorization in $\mathbb{Q}(\zeta_p)$ becomes important. Kummer proved that if the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p (so that the multiplicative arithmetic of $\mathbb{Q}(\zeta_p)$ becomes sufficiently simple), $x^p + y^p = z^p$ has no non-zero integral solution. This was the

most important result on Fermat's last theorem before the complete proof of Wiles by a different method.

Thus the ideal class group is a "bitter group" which seems to prevent the study of the arithmetic of number fields. But the above criterion (1) of Kummer shows that the ideal class group is in fact a "sweet group" which has a wonderful relation with zeta values.

I add that this study of Kummer was the start of the theory of ideals which became later important in algebraic number theory, algebraic geometry, and many areas of mathematics.

I add also that the final solution of Fermat's last theorem by Wiles [45] also uses the arithmetic of zeta values (generalized Iwasawa theory) of symmetric squares of modular forms.

(2) *Kummer's congruence.* If r is a negative odd integer and $r \not\equiv 1 \bmod (p-1)$, then $\zeta(r) \in \mathbb{Z}_{(p)} = \{m/n \mid (n, p) = 1\}$. If r' is also a negative odd integer and $r' \equiv r \bmod (p-1)$, then $\zeta(r') \equiv \zeta(r) \bmod p$.

On the other hand, if r is a negative odd integer such that $r \equiv 1 \bmod (p-1)$, p divides the denominator of $\zeta(r)$. Hence the results (1), (2) and the above list of $\zeta(0), \ldots, \zeta(-11)$ already show that the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p if $p = 3, 5, 7, 11, 13$, and hence $x^p + y^p = z^p$ has no non-zero integral solution for these p according to the result of Kummer. Kummer's congruence was generalized later to congruences modulo higher powers of p.

1.3. Class number formula. The class number formula of Dirichlet and Dedekind proved in the middle of 19th century is also a mysterious relationship between zeta functions and ideal class groups. Let F be a number field, and let $\zeta_F(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ ($\Re(s) > 1$) be the Dedekind zeta function of F, where $\mathfrak{a}$ ranges over all non-zero ideals of the integer ring O_F of F and $N(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$. Then $\zeta_F(s)$ has a meromorphic analytic continuation to the whole of $\mathbb{C}$ and is holomorphic at $s \neq 1$. If $F = \mathbb{Q}$, then $\zeta_F(s) = \zeta(s)$. The class number formula has the form

$$\lim_{s \to 0} \frac{1}{s^{r_1+r_2-1}} \zeta_F(s) = -\frac{h_F R_F}{w_F}.$$

Here h_F is the class number of F, R_F is the regulator of F (defined by using log of units in O_F), w_F is the number of all roots of 1 in F, r_1 is the number of real places of F, and r_2 is the number of complex places of F.

The class number formula is the first example of many similar formulae, for example, the Iwasawa main conjecture, the Birch and Swinnerton-Dyer conjecture, etc., which all have the form

$$\text{analytic invariant} = \text{arithmetic invariant}.$$

1.4. Iwasawa theory. In the later half of 20th century, studies of mysterious properties of zeta values evolved into a fruitful field of mathematics, Iwasawa theory.

Compared with Kummer's criterion and class number formula, Iwasawa theory is finer in the point that it describes not only the class number, i.e. the order of the ideal class group, but also the action of the Galois group on the ideal class group. In fact, one could even say that the aim of Iwasawa theory is to describe Galois actions on arithmetic objects in terms of zeta values.

For example, as we have seen, by Kummer's criterion, $\zeta(-11) = 691/(\cdots)$ tells that for $p = 691$, the ideal class group of $\mathbb{Q}(\zeta_p)$ contains a subgroup which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. But what does -11 here mean? By Iwasawa theory (this part is due to Ribet [35]), this -11 tells that for $p = 691$, as a module over the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains a submodule which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})(-11)$, where for $r \in \mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})(r)$ is a one-dimensional representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ on which $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\sigma(\zeta_p) = \zeta_p^c$ ($c \in (\mathbb{Z}/p\mathbb{Z})^\times$) acts as the multiplication by c^r.

The p-adic properties of values of the Riemann zeta function, which first appeared in Kummer's congruence, were summarized by Kubota and Leopoldt [24] as the existence of the p-adic Riemann zeta function which interpolates the zeta values $\zeta(r)$ ($r \in \mathbb{Z}, r \leq 0$) p-adically. Iwasawa showed that the p-adic zeta function was essentially an element of the Iwasawa algebra, and formulated the so-called Iwasawa main conjecture which has (roughly speaking) the form

$$p\text{-adic zeta function} = \text{ideal class group with Galois action.}$$

([20]; see 2.3.1 for the precise statement.) After efforts of Iwasawa, this conjecture was proved by Mazur–Wiles [32].

Wiles [44] exploiting the ideas of Hida, also proved the main conjectures for totally real fields. Moreover Rubin, using ideas of Kolyvagin, proved versions of Iwasawa's main conjecture for abelian extensions of imaginary quadratic fields ([37]). See, for example, [18] for discussions of various aspects of Iwasawa theory.

1.5. Elliptic curves. Recall that an elliptic curve E over a number field F is defined by an equation $y^2 = f(x)$ where $f(x)$ is a cubic polynomial over F without multiple root. The set $E(F) = \{(x, y) \in F \times F \mid y^2 = f(x)\} \cup \{(\infty, \infty)\}$ is endowed with the structure of an abelian group in which (∞, ∞) is the unit element, and the theorem of Mordell–Weil shows that $E(F)$ is finitely generated as an abelian group.

For example, for the elliptic curve $E\colon y^2 = x^3 + 1$ over $\mathbb{Q}$, if $P \in E(\mathbb{Q})$ denotes the point $(2, 3)$, then $2P = P + P = (0, 1)$, $3P = (-1, 0)$, $4P = (0, -1)$, $5P = (2, -3)$, $6P = (\infty, \infty)$, $\mathbb{Z}/6\mathbb{Z} \xrightarrow{\simeq} E(\mathbb{Q})$; $n \mapsto nP$. On the other hand, for the elliptic curve $y^2 = x^3 - 2$, if $P \in E(\mathbb{Q})$ denotes the point $(3, 5)$, then $\mathbb{Z} \xrightarrow{\simeq} E(\mathbb{Q})$; $n \mapsto nP$.

Zeta functions come to this arithmetic world. An elliptic curve E over a number field has its zeta function $L(E, s)$ (called the L-function of E). For $E\colon y^2 = x^3 + 1$ and $E\colon y^2 = x^3 - 2$ over $\mathbb{Q}$, the order of zero of $L(E, s)$ at $s = 1$ is 0 and 1, respectively, and is equal to the rank of $E(\mathbb{Q})$ as a finitely generated abelian group. Birch and Swinnerton-Dyer formulated the following conjecture [4].

Let E be an elliptic curve over a number field F. Then

(1) $\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\,(E(F))$.

(2) Let $r = \mathrm{ord}_{s=1} L(E, s)$. Then

$$\lim_{s \to 1} (s-1)^{-r} L(E, s) = \frac{h_E R_E \Omega_E \tau_E}{w_E}$$

where on the right-hand side, h_E is the order of the Tate–Shafarevich group $Ш(E)$ of E (which is an elliptic curve analogue of the ideal class group and is conjectured to be finite), R_E is the discriminant of the height pairing, Ω_E is the period of E, w_E is the square of the order of the torsion part of $E(F)$, and τ_E is "Tamagawa factor" which is a certain local term and is a non-zero rational number.

This is the elliptic curve version of the class number formula.

The first great result on this conjecture was obtained by Coates and Wiles [10]. Their result shows that if E has complex multiplication by an imaginary quadratic field K and if F is $\mathbb{Q}$ or K, then $E(F)$ is finite provided that $L(E, 1) \neq 0$.

The proof of Coates and Wiles is p-adic and was inspired by Iwasawa's generalization of Kummer's ideas. The principle of their method is that if we replace $\zeta(s)$ in Iwasawa theory by $L(E, s)$, then we can obtain a strong result on the relation between $L(E, s)$ and arithmetic.

The conjecture of Birch and Swinnerton-Dyer does not have a p-adic shape at all, but it is often important in mathematics to watch the right-hand side (p-adic world) of

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p,$$

not only the left-hand side (Archimedean world). Zeta functions are able to travel to the p-adic world, and to understand their relation to arithmetic, it is important to study their lifestyles in the p-adic world by the method of Iwasawa theory.

Iwasawa theory of elliptic curves was started by Mazur, and the analogue of the Iwasawa main conjecture for elliptic curves over $\mathbb{Q}$ was formulated by him (see 2.3.2, [29]). This main conjecture is now almost proved as I will explain in § 2.

This main conjecture is for cyclotomic Iwasawa theory of elliptic curves. Iwasawa theory of elliptic curves for anti-cyclotomic abelian extensions of imaginary quadratic fields was developed by Bertolini and Darmon and others (see [3] for example).

Coates has led developments of non-commutative Iwasawa theory of elliptic curves (here the Galois groups are non-commutative). The main conjecture for it was formulated in Venjakob [43] and Coates et al. [8], and this will be explained in §3.

1.6. Generalizations. Iwasawa theory of motives and Iwasawa theory of modular forms are now formulated and studied.

For motives which are of good ordinary reduction at p, main conjectures were formulated by Greenberg [17] and Schneider [40].

The conjectures of the type "$R = T$" concerning Galois deformations ([31]), which are important for the construction of non-commutative class field theory (Langlands program) and for which the work of Wiles [45] was a great contribution, are also regarded as generalizations of Iwasawa's main conjecture.

A very general form of main conjectures in generalized Iwasawa theory is given as equivariant Tamagawa number conjectures (these conjectures grew in Deligne [12], Beilinson [2], Bloch–Kato [5], Fontaine and Perrin-Riou [15], Perrin-Riou [34], Kato [21] for commutative Iwasawa theory of motives, and then in Burns–Flach [7], Huber–Kings [19] for non-commutative Iwasawa theory of motives). In the formulation of equivariant Tamagawa number conjecture, the worlds through which zeta functions travel are extended as $\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p \subset B_{\mathrm{dR}}$, where B_{dR} is the field of p-adic periods defined by Fontaine, which plays the role of complex numbers in p-adic Hodge theory (thus zeta functions now travel through Hodge theory and p-adic Hodge theory). The main conjecture presented in [19] in the previous ICM however did not involve p-adic zeta functions. The main conjecture in [43], [8] explained in § 3 involves p-adic zeta functions. The compatibility of this conjecture with the equivariant Tamagawa number conjecture is shown in [16].

In what follows, for the simplicity of description, we consider only Iwasawa theory for zeta functions associated to number fields and for zeta functions associated to elliptic curves. See [34], [16] etc. for more general motives.

2. Cyclotomic theory

We consider cyclotomic Iwasawa theory of elliptic curves, comparing it with classical Iwasawa theory. When we consider classical theory (resp. theory for elliptic curves), we will say that we are in Case I (resp. Case II). In Case II, assume we are given an elliptic curve E over $\mathbb{Q}$. Let p be a prime number. For simplicity of the description of the theory, we assume $p \neq 2$, and in Case II we assume that E has good ordinary reduction at p.

2.1. Arithmetic side

2.1.1. *Iwasawa algebras.* For a profinite group G, the completed group ring $\mathbb{Z}_p[[G]]$ is defined to be the inverse limit $\varprojlim_U \mathbb{Z}_p[G/U]$ of the usual group rings $\mathbb{Z}_p[G/U]$ where U ranges over all open normal subgroups of G. In the case $G = \mathrm{Gal}(L/F)$ for a Galois extension L of a number field F, the ring $\mathbb{Z}_p[[G]] = \varprojlim_{F'} \mathbb{Z}_p[\mathrm{Gal}(F'/F)]$, where F' ranges over all finite Galois extensions of F contained in L, is often called the Iwasawa algebra.

Let

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n}), \quad \mathbb{Q}(\zeta_{p^\infty})^+ = \mathbb{Q}(\zeta_{p^\infty}) \cap \mathbb{R},$$

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})^+/\mathbb{Q}) \quad \text{in Case I}, \quad G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \quad \text{in Case II}.$$

Let $\Lambda = \mathbb{Z}_p[[G]]$. Then in Case I (resp. II), Λ is isomorphic to the product of $(p-1)/2$ (resp. $p-1$) copies of the ring $\mathbb{Z}_p[[T]]$ of formal power series in one variable over $\mathbb{Z}_p$.

2.1.2. *Iwasawa modules.* Modules over Iwasawa algebras having arithmetic importance are often called Iwasawa modules, for Iwasawa first studied such modules in his papers. We define an Iwasawa module X over Λ as follows.

First assume that we are in Case I. Let $X = \mathrm{Gal}(M/\mathbb{Q}(\zeta_{p^\infty})^+)$ where M is the largest abelian pro-p extension of $\mathbb{Q}(\zeta_{p^\infty})^+$ in which any prime number different from p is unramified. Then G acts on X via inner automorphisms, and by this action X is regarded as a Λ-module.

This module X can also be expressed in terms of ideal class groups as

$$X \simeq \mathrm{Hom}\,(\varinjlim_n \mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))^-, (\mathbb{Q}_p/\mathbb{Z}_p)(1)).$$

Here $\mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))^-$ is the part of $\mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))$ on which the complex conjugate acts as -1, and $(\mathbb{Q}_p/\mathbb{Z}_p)(1)$ denotes the group of all roots of 1 of p-power orders. This isomorphism is deduced from Kummer theory. It preserves Galois actions (on the right-hand side, an element σ of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ acts as $h \mapsto \sigma \circ h \circ \sigma^{-1}$). By this isomorphism and by the finiteness of the ideal class groups, we can show that X is a finitely generated torsion Λ-module ("torsion" means that each element of X is killed by some non zero-divisor in Λ).

2.1.3. Next assume that we are in Case II. For a number field K, we have an exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/K) \to Ш(E/K) \to 0.$$

Here $\mathrm{Sel}(E/K)$ is the Selmer group of E over K which is a certain subgroup of the Galois cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})_{\mathrm{tor}})$, where $\overline{K}$ is the algebraic closure of K (= the algebraic closure of $\mathbb{Q}$) and $E(\overline{K})_{\mathrm{tor}}$ denotes the torsion part of $E(\overline{K})$. It is conjectured that the Tate–Shafarevich group $Ш(E/K)$ is always finite.

Define

$$X = \mathrm{Hom}\,(\varinjlim_n \mathrm{Sel}(E/\mathbb{Q}(\zeta_{p^n})), \mathbb{Q}_p/\mathbb{Z}_p).$$

Then X is regarded as a Λ-module via the natural action of G on it. It is a finitely generated Λ-module. Mazur conjectured that it is a torsion Λ-module, and this was proved in [22] (the case with complex multiplication is due to Rubin).

2.1.4. *Characteristic ideals.* For a finite abelian group (for example, for the ideal class group), the most important invariant is its order. For an Iwasawa module like X, the most important invariant is its characteristic ideal.

Recall that a finite abelian group M is isomorphic to a finite direct sum $\bigoplus_{i=1}^n \mathbb{Z}/(a_i)$ for non-zero integers $a_1, \ldots, a_n$, and the order $\sharp(M)$ of M is characterized by the equality $(\sharp(M)) = \left(\prod_{i=1}^n a_i\right)$ of ideals of $\mathbb{Z}$.

Now let R be a commutative ring which is isomorphic to a finite product of copies of $\mathbb{Z}_p[[T]]$, and let M be a finitely generated torsion R-module. Then there

are non zero-divisors $a_1, \dots, a_n$ of R and an injective homomorphism of R-modules $h\colon \bigoplus_{i=1}^n R/(a_i) \to M$ with finite cokernel. Define the characteristic ideal $\mathrm{Char}(M)$ of M as the principal ideal $\left(\prod_{i=1}^n a_i\right)$ of R. Then $\mathrm{Char}(M)$ is independent of the choices of $a_1, \dots, a_n$ and h as above.

2.2. Zeta side

2.2.1. Assume that we are in Case I. We review the p-adic Riemann zeta function.

Let $\kappa\colon \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \xrightarrow{\simeq} \mathbb{Z}_p^\times$ be the cyclotomic character, which is an isomorphism characterized by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(\sigma)}$ ($\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, $n \geq 1$). For an even integer r, the homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times;\ \sigma \mapsto \kappa(\sigma)^r$ factors through G, and we denote the induced homomorphism $G \to \mathbb{Z}_p^\times$ by κ^r.

For a commutative ring R, the total quotient ring is defined by

$$Q(R) = \left\{\tfrac{a}{b} \mid a, b \in R, b \text{ is a non zero-divisor}\right\}.$$

If R is an integral domain, $Q(R)$ is the field of fractions of R.

The p-adic Riemann zeta function ξ is the unique element of $Q(\Lambda)$ satisfying the following conditions (1) and (2):

(1) $(1-\sigma)\xi \in \Lambda$ for any $\sigma \in G$.

(2) For any even integer $r > 0$, the ring homomorphism $\Lambda \to \mathbb{Z}_p$ induced by $\kappa^r\colon G \to \mathbb{Z}_p^\times$ sends $(1-\sigma)\xi$ for $\sigma \in G$ to $(1-\kappa^r(\sigma))(1-p^{r-1})\zeta(1-r)$.

2.2.2. *Comparison with complex analysis.* The Riemann zeta function lives on the complex plane, but the p-adic Riemann zeta function lives in Galois theory. Though the complex plane and Galois theory are very much different, zeta can fly between these different worlds.

The ring Λ is the p-adic analogue of the ring A of all holomorphic functions on the complex plane. The total quotient ring $Q(\Lambda)$ is the p-adic analogue of the field $Q(A)$ of all meromorphic functions on the complex plane.

The p-adic Riemann zeta function $\xi \in Q(\Lambda)$ is the p-adic analogue of $\zeta(1-s) \in Q(A)$. For an even integer r, the ring homomorphism $\Lambda \to \mathbb{Z}_p;\ \sigma \mapsto \kappa^r(\sigma)$ ($\sigma \in G$) is the p-adic analogue of the ring homomorphism $A \to \mathbb{C};\ f \mapsto f(r)$. Let

$$I(A) = \{f \in A \mid f(0) = 0\}, \quad I(\Lambda) = \mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p;\ \sigma \mapsto 1\ (\sigma \in G)).$$

Then $I(\Lambda)$ is a principal prime ideal of Λ and is generated by $1-\sigma$ for all $\sigma \in G$. The fact $I(\Lambda)\xi \subset \Lambda$ (2.2.1, (1)) is the p-adic analogue of the fact that $I(A)\zeta(1-s) \subset A$.

The understanding of the ideal $I(A)\zeta(1-s) = (s\zeta(1-s))$ of A is equivalent to the understanding of zeros of $\zeta(s)$ counting multiplicity. Riemann's hypothesis is a beautiful statement about zeros of $\zeta(s)$, but it is not yet proved. On the other hand, for the p-adic side, there is also a beautiful statement about the ideal $I(\Lambda)\xi$ of Λ. It is Iwasawa's main conjecture introduced in 2.3.1 below, which was proved by Mazur–Wiles [32].

2.2.3. Assume that we are in Case II. The complex L-function $L(E, s)$ of E is defined as the Euler product $L(E, s) = \prod_\ell P_\ell(\ell^{-s})^{-1}$ for $\Re(s) > 3/2$, where ℓ ranges over all prime numbers and $P_\ell(T)$ is a polynomial described as follows. If E has good reduction at ℓ, $P_\ell(T) = 1 - a_\ell T + \ell T^2$ with $a_\ell = 1 + \ell - \sharp(E(\mathbb{F}_\ell))$. If E has bad reduction at ℓ, $P_\ell(T)$ is either $1 - T$, or $1 + T$, or 1. We can write $L(E, s)$ in the form of a Dirichlet series $\sum_{n=1}^\infty a_n n^{-s}$.

By the solution of the Shimura–Taniyama conjecture by Wiles, Breuil, Conrad, Diamond, Taylor [6], $\sum_{n=1}^\infty a_n q^n$ is the q-expansion of a cusp form of weight 2. From this we can deduce that the L-function of E twisted by a Dirichlet character χ defined as $L(E, s, \chi) = \sum_{n=1}^\infty a_n \chi(n) n^{-s}$ has an analytic continuation to the whole of $\mathbb{C}$ as a holomorphic function.

The p-adic L-function $L_p(E)$ of E is defined in $\Lambda[1/p]$. A difference with the case of the Riemann zeta function is that $L(E, r) = 0$ for all $r \in \mathbb{Z}_{\leq 0}$ and these values are not useful for the p-adic interpolation. The element $L_p(E)$ in $\Lambda[1/p]$ is characterized in the following way:

For any $n \geq 1$ and any Dirichlet character $\chi : (\mathbb{Z}/p^n\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$, the ring homomorphism $\Lambda \to \overline{\mathbb{Q}}_p$ induced by $G \to \overline{\mathbb{Q}}_p^\times$; $\sigma \mapsto \chi(\sigma)$ sends $L_p(E)$ to $L(E, 1, \chi)/((\text{period}) \times (\text{local term}))$. Here we regard χ as a character of G via the cyclotomic character. For the definitions of (period) and (local term) see [30], for example.

2.3. Main conjecture

2.3.1. In Case I, the Iwasawa main conjecture proved by Mazur–Wiles is stated as

$$I(\Lambda)\xi = \mathrm{Char}(X).$$

Here $I(\Lambda)$ denotes $\mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p; \sigma \mapsto 1\ (\sigma \in G))$ as in 2.2.2.

2.3.2. In Case II, the main conjecture formulated by Mazur is stated as

$$\Lambda L_p(E) = \mathrm{Char}(X).$$

(We recall that in Case II we assume that p is a good ordinary prime for E.)

2.3.3. The above conjecture of Mazur is now almost proved.

(1) Rubin [37]. If E has complex multiplication, then the conjecture is true.

(2) [22]. Assume E has no complex multiplication. Then there is $n \geq 0$ such that $\mathrm{Char}(X)$ divides $\Lambda p^n L_p(E)$. This n can be taken to be 0 under some mild assumptions. (Here "I divides J" means $J \subset I$.)

(3) Skinner and Urban [41]. Here to my present knowledge, the existence of some Galois representations associated to some automorphic forms on $U(2, 2)$ is

needed for the following result (but it seems that this existence will soon be proven).

$$\Lambda L_p(E) \text{ divides } \mathrm{Char}(X) \text{ under some mild assumptions.}$$

Ideas of the proofs of these results are sketched in the subsections 2.4 and 2.5.

2.3.4. We give some remarks on what is known about the Birch and Swinnerton-Dyer conjecture.

(1) In [25], Kolyvagin proved the following result.

If $\mathrm{ord}_{s=1} L(E, s) \leq 1$, then $\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\,(E(\mathbb{Q}))$ and $Ш(E)$ is finite.

(2) If $L(E, 1) \neq 0$, we can deduce from the main conjecture 2.3.2 that the ratio of the left side and the right side in part (2) of the Birch Swinnerton-Dyer conjecture stated in §1.5 is a rational number which is a p-adic unit.

(3) There is a p-adic analogue of the Birch and Swinnerton-Dyer conjecture ([30]) which states that

$$\mathrm{ord}_{s=1} L_p(E) = \mathrm{rank}\,(E(\mathbb{Q})).$$

Here $\mathrm{ord}_{s=1} L_p(E)$ is the order (valuation) of the image of $L_p(E)$ in the local ring of Λ at the prime ideal $I(\Lambda) = \mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p; \sigma \mapsto 1)$, which is a discrete valuation ring.

From the above result 2.3.3 (2), we can obtain that

$$\mathrm{rank}\,(E(\mathbb{Q})) \leq \mathrm{ord}_{s=1} L_p(E).$$

However for the original Birch and Swinnerton-Dyer conjecture, we do not have such general inequality, for the relation of $\mathrm{ord}_{s=1} L(E, s)$ and $\mathrm{ord}_{s=1} L_p(E)$ are not yet determined (although they are conjectured to be equal). At present, we cannot extend the above result (1) of Kolyvagin to the rank ≥ 2 case.[1]

2.3.5. It seems that zeta functions contain information about the structure of Iwasawa modules which is finer than the characteristic ideals.

For example, assume that X is either $\Lambda/(ab)$ or $\Lambda/(a) \oplus \Lambda/(b)$ for some $a, b \in \Lambda$. Since the characteristic ideals of both cases are (ab), we may think that p-adic zeta functions cannot tell which is the case. But in [28], Kurihara states the following with a sketch of the proof: In Case I, if we consider not only the single p-adic zeta function $\xi \in Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})^+/\mathbb{Q})]])$ but also the p-adic zeta functions in $Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})^+/\mathbb{Q})]])$ for all N which p-adically interpolate values of various Dirichlet L-functions, then these p-adic zeta functions can tell which is the case.

[1] *Added in the proof.* Skinner and Urban have obtained results for the rank ≥ 2 case. See their article in Volume II of the Proceedings of this ICM.

For a commutative ring R and for an R-module M of finite presentation, the r-th Fitting ideal of M is defined as follows. Take a presentation of M as the cokernel of an R-homomorphism $f\colon R^m \to R^n$. Then the r-th Fitting ideal of M is the ideal of R generated by the determinants of all $(n-r, n-r)$-minors of the matrix f. This is independent of the presentation of M. For example, the 0-th and the 1-st Fitting ideals of the Λ-module $\Lambda/(ab)$ are (ab) and Λ, respectively, whereas the 0-th and the 1-st Fitting ideals of $\Lambda/(a) \oplus \Lambda/(b)$ are (ab) and (a, b), respectively.

Kurihara [28] shows that for any $r \geq 0$, the r-th Fitting ideal of X is determined by the p-adic zeta functions in $Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})^+/\mathbb{Q})]])$ for varying N (his result is more general and can treat totally real fields). Partial results are proved in [26] and [27].

2.4. The modular form method. There are two proofs of the Iwasawa main conjecture for cyclotomic fields. One is the original proof of Mazur–Wiles using modular forms. The other is the proof of Rubin given later based on the method of Euler systems of Kolyvagin (see [38] for example). These two methods in Case I are both extended to Case II: The proofs of the results (1), (2) of 2.3.3 are by the Euler system methods, and the proof of the result (3) is an extension of the method of Mazur–Wiles (we will call a method of this type a modular form method).

In this subsection (resp. the next subsection), I sketch the ideas of the modular form method (resp. Euler system method).

By their natures, the modular form method is used to prove the divisibility, "the p-adic zeta function divides the characteristic ideal of the Iwasawa module", and the Euler system method is used to prove the converse divisibility. In Case 1, by the help of the class number formula, any one divisibility implies the converse divisibility.

2.4.1. Riemann's zeta function is regarded as the zeta function of a modular form of GL_1. The method of Mazur–Wiles in Case I is to use modular forms of the bigger algebraic group GL_2 to prove the main conjecture for a modular form of GL_1. The zeta function of an elliptic curve over $\mathbb{Q}$ is the zeta function of a modular form of GL_2. The method of Skinner–Urban in Case II is to use modular forms of the bigger algebraic group $U(2, 2)$ to prove the main conjecture for a modular form of GL_2.

2.4.2. There are three key points (a)–(c) about the method of Mazur–Wiles.

(a) Riemann zeta values appear as constant terms of Eisenstein series.

In fact, for k even ≥ 4, the Eisenstein series E_k of weight k has the q-expansion

$$E_k = \zeta(1-k)/2 + \textstyle\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Here $\sigma_m(n)$ denotes the sum of d^m for all divisors d of n.

(b) An eigen cusp form produces a two-dimensional irreducible p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

This is the theory of Eichler–Shimura and Deligne. In Langlands program, we expect that Galois representations arise from modular forms of various algebraic groups.

(c) The ideal class group is related to extensions of Galois representations with finite coefficients.

For example, for $r \in \mathbb{Z}$, there exists a non-trivial extension $0 \to \mathbb{Z}/p\mathbb{Z}(r) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$ of representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ which splits as a representation of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and is unramified outside p if and only if the Galois module $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains $(\mathbb{Z}/p\mathbb{Z})(r)$. (This can be proved by class field theory.)

2.4.3. To see how we can relate Riemann zeta values to the minus parts of ideal class groups by this method, we discuss simply how we can prove the "if part", due to Ribet [35], of the following theorem of Herbrand–Ribet: For $k \geq 2$ even, the Galois module $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains $(\mathbb{Z}/p\mathbb{Z})(1-k)$ if and only if p divides the numerator of $\zeta(1-k)$. In fact, this work of Ribet was a great hint for Mazur and Wiles in their work [32]. The proof goes in the following way.

We may and do assume that $4 \leq k \leq p-3$ and $k \not\equiv 0 \bmod (p-1)$. If p divides $\zeta(1-k)$, by 2.4.2 (a), $E_k \bmod p$ has no constant term. This shows that $E_k \equiv f \bmod p$ for some eigen cusp form f. For example, 691 divides $\zeta(-11)$ and $E_{12} \equiv \Delta \bmod 691$ where Δ is the eigen cusp form $q\prod_{n=1}^{\infty}(1-q^n)^{24}$. (This is Ramanujan's congruence.)

The congruence $f \cong E_k \bmod p$ tells that, by taking mod p of the 2-dimensional p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associated to f (2.4.2 (b)), we can obtain a 2-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ which is a non-trivial extension of the form $0 \to (\mathbb{Z}/p\mathbb{Z})(1-k) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$ having the properties in 2.4.2 (c).

Hence by 2.4.2 (c) above we have $(\mathbb{Z}/p\mathbb{Z})(1-k) \subset \mathrm{Cl}(\mathbb{Q}(\zeta_p))$ as Galois modules.

2.4.4. Skinner and Urban extended this approach to Case II. In place of 2.4.2 (a), the zeta values $L(E, 1, \chi)$ appear in the constant terms of the Eisenstein series of $U(2,2)$. In place of 2.4.2 (b), Galois representations associated to modular forms of $U(2,2)$ are used. In place of 2.4.2 (c), by the definition of Selmer group, an element of the Selmer group $\mathrm{Sel}(E/K)$ of order n corresponds to an extension $0 \to \mathrm{Ker}(n\colon E(\overline{K}) \to E(\overline{K})) \to ? \to \mathbb{Z}/n\mathbb{Z} \to 0$ of representations of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbb{Z}/n\mathbb{Z}$.

2.5. The Euler system method

2.5.1. It seems that zeta functions appear in this world showing three different shapes. First, they appear in the complex analytic world as complex analytic zeta functions, and are defined usually as Euler products. Secondly, they appear in the p-adic world as p-adic zeta functions. Now thirdly, they appear in the arithmetic world, as "arithmetic incarnations of zeta" such as cyclotomic units, elliptic units, Heegner points, and Beilinson elements. These incarnations are arithmetic objects which are related to zeta values in many ways. They form a family which has the property of being an

Euler system ([38]). I do not discuss the property of being an Euler system, but it is an arithmetic reflection of the fact that these incarnations are related to special values of Euler products.

For example, we call $1-\alpha$ (α a root of 1, $\alpha \neq 1$) a cyclotomic unit. The logarithms of cyclotomic units are related to complex zeta values as

$$\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \chi(a)\log(|1-\zeta_N^a|) = -2L'(0,\chi)$$

for any even Dirichlet character χ, where $\zeta_N = \exp(2\pi i/N)$.

Furthermore, as was discovered by Kummer and Iwasawa, cyclotomic units are related p-adically to zeta values $\zeta(r)$ for $r \in \mathbb{Z}$, $r \leq 0$, and furthermore produce the p-adic Riemann zeta function in a certain p-adic way.

Because the arithmetic incarnations of zeta are arithmetic in nature, they can play an important role in the study of arithmetic properties of zeta values. Cyclotomic units are important in classical Iwasawa theory, elliptic units in Iwasawa theory of imaginary quadratic fields and in Iwasawa theory of elliptic curves with complex multiplication (as in [10], [37]), Heegner points in anti-cyclotomic Iwasawa theory of elliptic curves (as in [25], [3]), and Beilinson elements in cyclotomic Iwasawa theory of elliptic curves.

2.5.2. The results 2.3.3 (1), (2) were obtained by using elliptic units and Beilinson elements, respectively. The methods are similar to the second proof of Iwasawa's main conjecture given by Rubin using cyclotomic units.

In these methods, the key points are that (a) these incarnations of zeta are related p-adically to p-adic zeta functions, and that (b) they form Euler systems.

I will explain the methods in Case I first, and then tell about Case II.

2.5.3. As is well known in classical Iwasawa theory thanks to deep works of Iwasawa, the Iwasawa main conjecture introduced in 2.3.1 is equivalent to

$$\mathrm{Char}(U/\Lambda z) = \mathrm{Char}(C^+).$$

Here U (resp. C^+) is the projective limit of

$$(\mathbb{Z}[\zeta_{p^n}, 1/p]^+)^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad (\text{resp. } \mathrm{Cl}(\mathbb{Q}(\zeta_{p^n})^+)(p))$$

with respect to norm maps ((p) denotes the p-primary part), and $z \in U$ is the system of cyclotomic units $((1-\zeta_{p^n})(1-\zeta_{p^n}^{-1}))_n$. To rewrite Iwasawa's main conjecture 2.3.1 in this form, we replace the p-adic zeta function in the conjecture 2.3.1 by z using the strong relation (2.5.2 (a)) between them, and replace X by C^+ using the fact that C^+ is a quotient Λ-module of X by class field theory. Note that in this rewritten form of Iwasawa's main conjecture, since the p-adic zeta function was replaced by the arithmetic incarnation, both sides became arithmetic sides.

We can prove that $\mathrm{Char}(C^+)$ divides $\mathrm{Char}(U/\Lambda z)$ by the method of Euler system (Kolyvagin's idea [25]; Thaine [42] had partially a similar idea) using the Euler system

property of cyclotomic units (2.5.2 (b)). The method here is simply speaking as in 2.5.4 below. This divisibility implies the divisibility $\mathrm{Char}(X) \mid I(\Lambda)\xi$ and gives the proof of Iwasawa's main conjecture.

2.5.4. The proof of $\mathrm{Char}(C^+) \mid \mathrm{Char}(U/\Lambda z)$ by the Euler system method is sketched roughly as follows.

Let $h\colon \bigoplus_{i=1}^n \Lambda/(a_i) \to C^+$ be an injective Λ-homomorphism with finite cokernel. The Λ-module U is isomorphic to Λ, and hence $U/\Lambda z \simeq \Lambda/(\mu)$ for some $\mu \in \Lambda$. Our task is to prove that $\prod_{i=1}^n a_i$ divides μ. For $1 \leq i \leq n$, denote the standard i-th generator in $\bigoplus_{i=1}^n \Lambda/(a_i)$ by e_i. Then by modifying cyclotomic units using their Euler system property, for each $m \geq 1$, we can construct a non-zero element α of $\mathbb{Q}(\zeta_{p^m})^+$ such that there is a non-zero fractional ideal of $\mathbb{Q}(\zeta_{p^m})^+$ whose class coincides with the image of $h(e_1)$ and which is sent by the action of μ to the principal ideal (α). This shows that μ kills $h(\Lambda e_1)$, and hence $a_1 \mid \mu$. Put $\mu = \mu_1 a_1$ with $\mu_1 \in \Lambda$. By a similar method, we can show that μ_1 kills $h(\Lambda e_1 \oplus \Lambda e_2)/h(\Lambda e_1)$. Hence $a_2 \mid \mu_1$. Put $\mu_1 = \mu_2 a_2$ with $\mu_2 \in \Lambda$. Then we can show that μ_2 kills $h(\Lambda e_1 \oplus \Lambda e_2 \oplus \Lambda e_3)/h(\Lambda e_1 \oplus \Lambda e_2)$. By repeating this, we have $\mu = \mu_n \prod_{i=1}^n a_i$ with $\mu_n \in \Lambda$.

For the precise description of the method see [38].

2.5.5. In Case II we can use similar methods to prove that X is Λ-torsion and to prove 2.3.3 (1), (2). I describe rough ideas about 2.3.3 (2).

Beilinson elements are defined in [2] as elements of K_2 of modular curves (K_2 is a group which appears in algebraic K-theory). Via the Weil parametrization of an elliptic curve E over $\mathbb{Q}$, and via the Archimedean regulator maps of K_2 (analogues of logarithms for the multiplicative group), they are related to $L'(E, 0, \chi)$. Furthermore, we can prove that they are related p-adically to the values $L(E, 1, \chi)$ and to the p-adic zeta function $L_p(E)$.

In Case I, the Λ-module U (resp. C^+) is isomorphic to the inverse limit of the étale cohomology groups $H^i(\mathbb{Z}[\zeta_{p^n}, 1/p]^+, \mathbb{Z}_p(1))$ with $i = 1$ (resp. $i = 2$). In Case II, in place of U (resp. C^+), we use the inverse limit $\mathfrak{H}^i$ of the étale cohomology groups $H^i(\mathbb{Z}[\zeta_{p^n}, 1/pN], T_pE)$ with $i = 1$ (resp. $i = 2$), where N is the conductor of E and T_pE is the p-adic Tate module of E. By using the strong relation of Beilinson elements and $L_p(E)$ (2.5.2 (a)), we can show that the fact "X is Λ-torsion and $\mathrm{Char}(X) \mid \Lambda L_p(E)$" is equivalent to the fact that "$\mathfrak{H}^1/\Lambda z$ and $\mathfrak{H}^2$ are Λ-torsion and $\mathrm{Char}(\mathfrak{H}^2) \mid \mathrm{Char}(\mathfrak{H}^1/\Lambda z)$" where $z \in \mathfrak{H}^1$ is an element which comes from Beilinson elements. In the case E has no complex multiplication, the last fact is proved by arguments similar to 2.5.4 using the Euler system property of Beilinson elements (2.5.2 (b)). (In this method, we make also a heavy use of the result by Rohrlich that $L_p(E)$ is a non zero-divisor of $\Lambda[1/p]$.)

2.5.6. We expect that the Euler system method works for any motives. However, a big difficulty is that at present we can find only few arithmetic incarnations of zeta, though we have found a lot of zeta functions.

3. Non-commutative Iwasawa theory

For an elliptic curve E over a number field F without complex multiplication, the field obtained by adjoining all p^n-torsion points of E to F for all n is a Galois extension of F whose Galois group is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of finite index (by a theorem of Serre) and hence is highly non-commutative. It is natural to look for a non-commutative Iwasawa theory for E.

In this section, I introduce the ideas in the papers [43] and [8] on non-commutative Iwasawa theory, and discuss related problems.

In this section, we consider two cases I, II. In Case I, we consider non-commutative Iwasawa theory of totally real fields. In Case II, we consider non-commutative Iwasawa theory of elliptic curves.

Fix a prime number p and assume $p \neq 2$ for simplicity. Both in the cases I, II, let F be a number field, and let F_∞ be a Galois extension of F satisfying the following conditions (i)–(iii).

(i) The Galois group $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group.

(ii) There are only finitely many primes of F which ramify in F_∞.

(iii) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F.

In Case I, we assume further that F_∞ is totally real, and that F_∞ contains $F(\zeta_{p^\infty})^+$.

In Case II, we assume that we are given an elliptic curve E over F which is of good ordinary reduction at any prime of F lying over p.

Let $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}}) \subset G$, so that H is a closed normal subgroup of G with $G/H \simeq \mathbb{Z}_p$. In Case I, fix a finite set Σ of primes of F which contain all primes of F lying over p and all primes of F which ramify in F_∞.

3.1. Arithmetic side

3.1.1. Let $\Lambda = \mathbb{Z}_p[[G]]$. By a Λ-module, we mean a left Λ-module. We define a Λ-module X as follows.

In Case I, let $X = \mathrm{Gal}(M/F_\infty)$ where M is the largest abelian pro-p extension of F_∞ which is unramified outside Σ.

In Case II, let $X = \mathrm{Hom}\,(\varinjlim_{F'} \mathrm{Sel}(E/F'), \mathbb{Q}_p/\mathbb{Z}_p)$ where F' ranges over all finite Galois extensions of F contained in F_∞.

Then in both cases X is a finitely generated Λ-module.

3.1.2. In Case I, X is a torsion Λ-module (that is, each element of X is killed by some non zero-divisor of Λ). In Case II, a natural conjecture is that X is Λ-torsion.

More precisely:

Conjecture 3.1.3. In Case I, X is finitely generated as a $\mathbb{Z}_p[[H]]$-module.

Conjecture 3.1.4. ([8] 5.1.) In Case II, $X/X(p)$ is finitely generated as a $\mathbb{Z}_p[[H]]$-module, where $X(p)$ denotes the part of X killed by some power of p.

Let F' be a finite extension of F contained in F_∞ such that F_∞/F' is a pro-p extension. In Case I, 3.1.3 is true if the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of F' is zero (it is conjectured by Iwasawa that the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of any number field is zero). In Case II, 3.1.4 is true if E is isogenous over F' to an elliptic curve E' such that the μ-invariant of E' for the cyclotomic $\mathbb{Z}_p$-extension of F' is zero.

3.2. Zeta side

3.2.1. Where do the p-adic zeta functions in non-commutative Iwasawa theory live? Non-commutative rings are not good places to live for complex zeta functions defined as Euler products, for the meaning of Euler product becomes unclear by the non-commutativity of the product. Though p-adic zeta functions are not Euler products, this gives us the impression that any p-adic zeta function cannot live in the non-commutative Λ.

However, for a non-commutative ring R, the non-commutativity of the product in $R^\times$ vanishes under the canonical homomorphism $R^\times \to K_1(R)$.

3.2.2. Recall that for a ring R, $K_1(R)$ is defined to be the abelian group

$$\mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)],$$

where $\mathrm{GL}(R) = \bigcup_n \mathrm{GL}_n(R)$ in which $\mathrm{GL}_n(R)$ is embedded in $\mathrm{GL}_{n+1}(R)$ by $T \mapsto \left(\begin{smallmatrix} T & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

3.2.3. As is explained below, in Case I (resp. Case II) we expect that the p-adic zeta function lives in K_1 of a certain localization of Λ (resp. of $\bar{\Lambda} = O[[G]]$ where O is the completion of the valuation ring of the maximal unramified extension of $\mathbb{Q}_p$) defined as follows. (Note that the theory of localizations of non-commutative rings is not so simple as that for commutative rings.) Define

$$S = \{s \in \Lambda \mid \Lambda/\Lambda s \text{ is a finitely generated } \mathbb{Z}_p[[H]]\text{-module}\}, \quad S^* = \bigcup_{n\geq 0} p^n S.$$

Then S and S^* are multiplicative subsets of Λ, consisting of left and right non zero-divisors and satisfying the left and right Ore conditions ([33]) in the localization theory of non-commutative rings. Hence we have rings $\Lambda_S = S^{-1}\Lambda = \Lambda S^{-1}$ by inverting elements of S, and also $\Lambda_{S^*} = \Lambda_S[1/p]$. In the case that H is finite and G is commutative, $\Lambda_{S^*} = Q(\Lambda)$.

Let $\mathfrak{N}_H(G)$ (resp. $\mathfrak{M}_H(G)$) be the category of finitely generated Λ-modules M such that M (resp. $M/M(p)$) is finitely generated as a $\mathbb{Z}_p[[H]]$-module. For a finitely generated Λ-module M, M is S-torsion if and only if it belongs to $\mathfrak{N}_H(G)$, and it is S^*-torsion if and only if it belongs to $\mathfrak{M}_H(G)$.

We have similarly multiplicative subsets $\bar{S}$ and $\bar{S}^* = \bigcup_{n\geq 0} \bar{S}p^n$ of $\bar{\Lambda}$ and localizations $\bar{\Lambda}_{\bar{S}}$, $\bar{\Lambda}_{\bar{S}^*}$.

3.2.4. We expect that the p-adic zeta function in non-commutative Iwasawa theory is characterized by the relation of its special values with complex zeta values. For an element f of $K_1(\Lambda_{S^*})$ and for a continuous representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C}_p)$ where $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$, the value $f(\rho) \in \mathbb{C}_p \cup \{\infty\}$ is defined in [8]. I do not give here the precise general definition, but a basic fact is that if f is the image of an element a of $\Lambda \cap (\Lambda_{S^*})^\times$, the value of f at ρ is equal to $\det(\rho(a))$, where $\rho(a)$ denotes the image of a under the ring homomorphism $\Lambda \to M_n(\mathbb{C}_p)$ induced by ρ.

We can define similarly the value $f(\rho) \in \mathbb{C}_p \cup \{\infty\}$ of an element f of $K_1(\bar{\Lambda}_{\bar{S}^*})$ at a continuous representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C}_p)$.

Now we state our conjecture for the existence of the p-adic zeta function in non-commutative Iwasawa theory.

Conjecture 3.2.5. (1) In Case I, there is an element $L_p(F_\infty/F) \in K_1(\Lambda_S)$ (called the p-adic zeta function for the extension F_∞/F) having the following property.

For any even integer $r \geq 1$ and any representation ρ of G which factors through a finite quotient Galois group, the value of $L_p(F_\infty/F)$ at the representation $\rho\kappa^r$ of G is the value $L_\Sigma(1-r, \rho)$ of the Artin L-function $L_\Sigma(s, \rho)$. (The subscript Σ means that the Euler factors at primes in Σ are removed from the Euler product.)

(2) In Case II, there is an element $L_p(E, F_\infty/F) \in K_1(\bar{\Lambda}_{\bar{S}^*})$ (called the p-adic zeta function of E for the extension F_∞/F) having the following property.

For any representation ρ of G which factors through a finite quotient Galois group, the value of $L_p(E, F_\infty/F)$ at ρ is $L(E, 1, \rho)/((\text{ period}) \times (\text{local term}))$.

Here $L(E, s, \rho)$ is the twist of $L(E, s)$ by ρ. The definitions of (period) and (local term) are given explicitly in [8] in the case $F = \mathbb{Q}$. In the case $F \neq \mathbb{Q}$, the definitions are given in [16] but they are not so explicit.

3.2.6. The idea that "zeta functions can live in K_1 of non-commutative group rings" may be true also for Selberg zeta functions. Such idea appears in the paper of Bass [1] for Ihara–Selberg zeta functions (Selberg zeta functions for p-adic fields). I learned about the work [1] from K. Hashimoto.

For a discrete co-compact torsion-free subgroup Γ of $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ and for a finite dimensional representation $\rho\colon \Gamma \to \mathrm{GL}_n(\mathbb{C})$, the Selberg zeta function of Γ with twist by ρ is defined to be $\prod_\gamma \det(1 - \rho(\gamma)N(\gamma)^{-s})^{-1}$ $(\Re(s) \gg 0)$ where γ ranges over all "prime elements" of Γ taken mod conjugacy. (Prime element means an element which is not an n-th power of any element for any $n \geq 2$. $N(\gamma) > 1$ is the absolute value of one of the eigen values of γ.)

I am not sure if it is reasonable to define the Selberg zeta function with values in $K_1(L^1(\Gamma))$, where $L^1(\Gamma)$ is the algebra of L^1-functions on Γ with the product structure by convolution, as follows.

$$\zeta_\Gamma(s) = \prod_\gamma (1 - \gamma N(\gamma)^{-s})^{-1}.$$

(The right-hand side is regarded as an element of $K_1(L^1(\Gamma))$.) For a finite dimensional unitary representation $\rho\colon \Gamma \to \mathrm{GL}_n(\mathbb{C})$, the ring homomorphism $L^1(\Gamma) \to M_n(\mathbb{C})$ induced by ρ defines a homomorphism $K_1(L^1(\Gamma)) \to K_1(M_n(\mathbb{C})) = \mathbb{C}^\times$ which sends $\zeta_\Gamma(s)$ to the Selberg zeta function of Γ with twist by ρ.

If $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ is replaced by $\mathrm{SL}_2(\mathbb{Q}_p)/\{\pm 1\}$, an analogue of the above $\zeta_\Gamma(s)$ is considered in Bass [1].

3.3. Main conjecture. We assume for simplicity that G is p-torsion-free in this subsection.

3.3.1. The localization theory in K-theory [46] gives exact sequences

$$K_1(\Lambda) \to K_1(\Lambda_S) \xrightarrow{\partial} K_0(\mathfrak{N}_H(G)) \to 0,$$
$$K_1(\Lambda) \to K_1(\Lambda_{S^*}) \xrightarrow{\partial} K_0(\mathfrak{M}_H(G)) \to 0.$$

Here for $\mathcal{C} = \mathfrak{N}_H(G)$ or $\mathfrak{M}_H(G)$, $K_0(\mathcal{C})$ denotes the Grothendieck group of $\mathcal{C}$, which is an abelian group defined by the following generators and relations. Generators: $[M]$ for objects M of $\mathcal{C}$. Relations: $[M] = [M'] + [M'']$ if M, M', M'' are objects of $\mathcal{C}$ such that there is an exact sequence $0 \to M' \to M \to M'' \to 0$. In the above first (resp. second) exact sequence, ∂ satisfies $\partial(s) = [\Lambda/\Lambda s]$ for $s \in S$ (resp. $s \in S^*$).

In the situation of §2 in which G is commutative, $\mathfrak{M}_H(G)$ coincides with the category of all finitely generated torsion Λ-modules, and for any finitely generated torsion Λ-module M and for any generator f of $\mathrm{Char}(M)$, we have $\partial(f) = [M]$ in $K_0(\mathfrak{M}_H(G))$. Hence $[M]$ can play the role of the characteristic ideal in §2.

The following is the main conjecture. ([43], [8]. Generalizations to motives are explained in the complementary paper [16] to [8].)

Conjecture 3.3.2. (1) In Case I, the homomorphism $\partial\colon K_1(\Lambda_S) \to K_0(\mathfrak{N}_H(G))$ sends $L_p(F_\infty/F)$ to $[X] - [\mathbb{Z}_p]$.

(2) In Case II, if f is an element of $K_1(\Lambda_{S^*})$ such that $\partial(f) = [X]$, we have $L_p(E, F_\infty/F) \equiv f$ modulo the image of $K_1(\bar{\Lambda}) \to K_1(\bar{\Lambda}_{\bar{S}^*})$.

3.4. Complements

3.4.1. In Case I, a main conjecture was formulated and studied by Ritter–Weiss ([39] etc.) under the assumption that H is finite (H can have p-torsion).

3.4.2. For an elliptic curve E with super-singular reduction at p, it is not known how to formulate p-adic zeta functions in non-commutative Iwasawa theory.

3.4.3. In history, studies of delicate properties of algebraic varieties motivated progress in the theory of commutative rings. Similarly, I expect that via non-commutative Iwasawa theory, delicate aspects in number theory motivate progress in the theory of non-commutative rings. The structure theorem of torsion modules over non-commutative Iwasawa type algebras by Coates–Schneider–Sujatha [9] is one such example.

3.4.4. An interesting aspect of non-commutative Iwasawa theory of elliptic curves is the relative prevalence, compared to the cyclotomic theory, of global root numbers equal to -1 (in the case of twists of an elliptic curve by self dual Artin characters of certain non-commutative p-adic Lie extensions, see, for example, Dokchitser [14], and Rohrlich [36]). This phenomenon has long been important in the study of Heegner points on elliptic curves, and recently H. Darmon and Y. Tian have obtained the first deep results about Heegner points in non-commutative Iwasawa theory of elliptic curves ([13], [11]).

3.4.5. As in Huber–Kings [19], §3.3, we can expect that non-commutative Iwasawa theory is strong enough to unify Iwasawa theories of all motives. This would imply that there are many still unknown congruences between p-adic zeta functions of different motives and also between modular forms of different algebraic groups.

In the rest of this section, assuming that G is isomorphic to a non-commutative semi-direct product of two copies of $\mathbb{Z}_p$, I report some conjectural congruences between p-adic zeta functions in commutative Iwasawa theory which would be implied by non-commutative Iwasawa theory. We can show conversely (Proposition 3.4.9, which I learned from D. Burns) that in Case I, under the same assumption, the existence of p-adic zeta function and the main conjecture in non-commutative Iwasawa theory are reduced to these conjectural congruences between p-adic zeta functions in commutative Iwasawa theory.

3.4.6. Assume that G is isomorphic to a non-commutative semi-direct product of two copies of $\mathbb{Z}_p$.

Then $H \simeq \mathbb{Z}_p$. Let $e \geq 1$ be the integer such that $H/[G,H]$ is of order p^e. Let $\Gamma = G/H$ and for $n \geq 0$, let $\Gamma_n \subset \Gamma$ be the unique subgroup of Γ of index $p^{\max(n-e,0)}$. Define commutative rings R_n and $R'_n \subset Q(R_n)$ $(n \geq 0)$ as follows: $R_n = \mathbb{Z}_p[\zeta_{p^{\min(n,e)}}][[\Gamma_n]]$, and R'_n is the local ring of R_n at the unique prime ideal of height 1 containing p. In [23], homomorphisms

$$\theta = (\theta_n)_n \colon K_1(\mathbb{Z}_p[[G]]) \to \prod_{n\geq 0} R_n^\times, \quad \theta' = (\theta'_n)_n \colon K_1(\mathbb{Z}_p[[G]]_S) \to \prod_{n\geq 0} (R'_n)^\times$$

such that θ' induces θ are defined. Furthermore subgroups

$$\Phi \subset \prod_{n\geq 0} R_n^\times, \quad \Phi' \subset \prod_{n\geq 0} (R'_n)^\times$$

such that $\Phi = \left(\prod_{n\geq 0} R_n^\times\right) \cap \Phi'$ are defined by using certain congruences.

The congruences defining Φ and Φ' are rather involved, and so for simplicity, I introduce them here only in the case $e = 1$.

Let $(a_n)_n$ be an element of $\prod_{n\geq 0} R_n^\times$ (resp. $\prod_{n\geq 0}(R'_n)^\times$). Let $b_n = a_n N_n(a_0)^{-1}$ where N_n is the norm map

$$\mathbb{Z}_p[[\Gamma]]^\times \to \mathbb{Z}_p[[\Gamma_n]]^\times \quad (\text{resp. } (\mathbb{Z}_p[[\Gamma]]_{(p)})^\times \to (\mathbb{Z}_p[[\Gamma_n]]_{(p)})^\times).$$

Let $c_n = b_n\varphi(b_{n-1})^{-1}$ for $n \geq 1$ where φ is the ring homomorphism induced by the p-th power homomorphism $\Gamma_{n-1} \to \Gamma_n$. Then in the case $e = 1$, $(a_n)_n$ belongs to Φ (resp. Φ') if and only if the following congruences are satisfied:

$$c_n^{p^{n-1}} \equiv N_n(N'\big(\textstyle\prod_{i=1}^{n-1} c_i)\big) \bmod p^{2(n-1)}(\zeta_p - 1) \quad \text{for any } n \geq 1$$

where N' denotes the norm map $R_1^\times \to \mathbb{Z}_p[[\Gamma]]^\times$ (resp. $(R_1')^\times \to (\mathbb{Z}_p[[\Gamma]]_{(p)})^\times$).

Proposition 3.4.7 ([23]). (1) *The map* $\theta\colon K_1(\mathbb{Z}_p[[G]]) \to \prod_{n\geq 0} R_n^\times$ *is injective and induces an isomorphism* $K_1(\mathbb{Z}_p[[G]]) \xrightarrow{\simeq} \Phi$.

(2) *The image of* $\theta'\colon K_1(\mathbb{Z}_p[[G]]_S) \to \prod_{n\geq 0} (R_n')^\times$ *is contained in* Φ'.

3.4.8. Assume that we are in Case I. For $n \geq 0$, let F_n be the finite extension of F contained in F^{cyc} corresponding to the subgroup Γ_n of Γ. Let $G_n \subset G$ be the inverse image of Γ_n in G. Then there is a one-dimensional representation $\chi_n\colon G_n \to \overline{\mathbb{Q}}^\times$ of G_n of order p^n whose restriction to H is still of order p^n. The p-adic L-function ξ_n of the totally real field F_n associated to the character χ_n belongs to $Q(R_n)$. The main conjecture of Iwasawa theory of F_n proved by Wiles shows that

(1) $(\xi_n) = \mathrm{Char}(X_n)$ for $n \geq 1$, and $I(R_0)\xi_0 = \mathrm{Char}(X_0)$

where X_n is the Iwasawa module of the Iwasawa theory of F_n associated to χ_n and $I(R_0)$ is the kernel of $R_0 = \mathbb{Z}_p[[\Gamma]] \to \mathbb{Z}_p; \sigma \mapsto 1$ $(\sigma \in \Gamma)$.

I did not explain the definitions of θ_n and θ_n', but the maps θ_n' have the following properties (2) and (3).

(2) Let ξ be an element of $K_1(\Lambda_S)$. Then ξ has the property of the p-adic zeta function $L_p(F_\infty/F)$ stated in 3.2.5 if and only if $\theta_n'(\xi) = \xi_n$ for all $n \geq 0$.

(3) If X belongs to $\mathfrak{N}_H(G)$ and f is an element of $K_1(\Lambda_S)$ such that $\partial(f) = [X] - [\mathbb{Z}_p]$, then $(\theta_n'(f)) = \mathrm{Char}(X_n)$ for $n \geq 1$, and $I(R_0)\theta_0'(f) = \mathrm{Char}(X_0)$.

If the p-adic zeta function $L_p(F_\infty/F) \in K_1(\Lambda_S)$ in non-commutative Iwasawa theory exists, then by the above (2) and by Prop. 3.4.7 (2), $(\xi_n)_n$ should be contained in Φ'. This shows that the p-adic L functions ξ_n in commutative Iwasawa theory should satisfy special congruences between them (which are not proven yet).

Conversely, assume $(\xi_n)_n \in \Phi'$. From the above (1), we can deduce $X \in \mathfrak{N}_H(G)$. Let f be an element of $K_1(\Lambda_S)$ such that $\partial(f) = [X] - [\mathbb{Z}_p]$. Then by (1) and (3), we have $(\xi_n) = (\theta_n'(f))$ for any $n \geq 0$. Hence $u_n := \xi_n\theta_n'(f)^{-1}$ is a unit of R_n. By Prop. 3.4.7 (2), $(u_n)_n \in \big(\prod_{n\geq 0} R_n^\times\big) \cap \Phi' = \Phi$. Hence by Prop. 3.4.7 (1), $(u_n)_n$ comes from an element u of $K_1(\Lambda)$. By (2), uf is the p-adic zeta function of F_∞/F in the non-commutative Iwasawa theory (which we were looking for), and $\partial(uf) = [X] - [\mathbb{Z}_p]$. This proves

Proposition 3.4.9. *Assume that we are in Case* I, *and assume that* G *is non-commutative and is a semi-direct product of two copies of* $\mathbb{Z}_p$. *If the family* $(\xi_n)_{n\geq 0}$ *of* p*-adic*

zeta functions in commutative Iwasawa theory belongs to Φ' (*i.e. satisfies special congruences*)*, then the* p*-adic zeta function for* F_∞/F *in non-commutative Iwasawa theory exists and the main conjecture in non-commutative Iwasawa theory for* F_∞/F *is true.*

From §2 we can have the idea that "the proofs of the main conjectures in commutative Iwasawa theory will be obtained by the modular form method and the Euler system method as in §2". The author learned from D. Burns not only Proposition 3.4.9 but also the following idea: "the proofs of the main conjectures in non-commutative Iwasawa theory might not be at infinite distance, but might be deduced from the main conjecture in commutative Iwasawa theory plus special congruences between p-adic zeta functions in commutative Iwasawa theory".

References

[1] Bass, H., The Ihara-Selberg zeta function of a tree lattice. *Internat. J. Math.* **3** (1992), 717–797.

[2] Beilinson, H., Higher regulators and values of L-functions. Current problems in mathematics **24** (1984), 181–238.

[3] Bertolini, M., and Darmon, H., Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions. *Ann. of Math.* **162** (2005), 1–64.

[4] Birch, B., J., and Swinnerton-Dyer, H. P. F., Notes on elliptic curves. I. *J. Reine Angew. Math.* **212** (1963), 7–25; II. *J. Reine Angew. Math.* **218** (1965), 79–108.

[5] Bloch, S., and Kato, K., L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift*, Vol. I, Progr. Math. 86, Birkhäuser, Boston, MA, 1990, 333–400.

[6] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), 843–939.

[7] Burns, D., and Flach, M., Tamagawa numbers for motives with (non-commutative) coefficients I. *Documenta Math.* **6** (2001), 501–570; II, *Amer. J. Math.* **125** (2003), 475–512.

[8] Coates, J., Fukaya, T., Kato K., Sujatha, R., and Venjakob, O., The GL_2 main conjecture for elliptic curves without complex multiplication. *Inst. Hautes Études Sci. Publ. Math.* **101** (2005), 163–208.

[9] Coates, J., Schneider, P., and Sujatha, R., Modules over Iwasawa algebras. *J. Inst. Math. Jussieu* **2** (2003), 73–108.

[10] Coates, J., and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), 223–251.

[11] Darmon, H., and Tian, Y., Heegner points over false Tate curve extension. Talk in Montreal; preprint.

[12] Deligne, P., Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions*, Part 2, Proc. Symp. Pure Math. 33, Amer. Math. Soc., Providence, R.I., 1979, 313–346.

[13] Dokchitser, T., and Dokchitser, V., Computations in non-commutative Iwasawa theory (with an appendix by J. Coates and R. Sujatha). *Proc. London Math. Soc.* **94** (2007), 211–272.

[14] Dokchitser V., Root numbers of non-abelian twists of elliptic curves. *Proc. London Math. Soc.* **91** (2005), 300–324.

[15] Fontaine, J.-M., and Perrin-Riou, B., Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives* (Seattle, WA, 1991), Proc. Symp. Pure Math. 55, Part 1, Amer. Math. Soc., Providence, RI, 1994, 599–706.

[16] Fukaya, T., and Kato, K., A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory. *Trudy Sankt-Peterburgskugo Matematicheskogo Obshchestva* **12** (2005), 1–101; English version to appear in Amer. Math. Soc. Transl. Ser. 2, Proc. St Petersburg Math. Soc.

[17] Greenberg, R., Iwasawa theory for p-adic representations. In *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, 97–137.

[18] Greenberg, R., Iwasawa theory—past and present. In *Class field theory—its centenary and prospect* (Tokyo, 1998), Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo 2001, 335–385.

[19] Huber, A., and Kings, G., Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. II, Higher Ed. Press, Beijing 2002, 149–162.

[20] Iwasawa, K., Analogies between number fields and function fields. In *Collected Papers*, Vol. II, Springer-Verlag, Tokyo 2001, 606–611.

[21] Kato, K., Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I. In *Arithmetic algebraic geometry* (Trento, 1991), Lecture Notes in Math. 1553, Springer-Verlag, Berlin 1993, 50–163.

[22] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque* **295** (2004), 117–290.

[23] Kato, K., K_1 of some non-commutative completed group rings. *K-theory* **34** (2005), 99–140.

[24] Kubota, K., and Leopoldt, H.-W., Eine p-adische Theorie der Zetawerte. I. *J. Reine Angew. Math.* **214/215** (1964), 328–339.

[25] Kolyvagin, V. Euler systems. In *The Grothendieck Festschrift*, Vol. II, Progr. Math. 87, Birkhäuser, Boston, MA, 1990, 435–483.

[26] Kurihara, M., Iwasawa theory and Fitting ideals. *J. Reine Angew. Math.* **561** (2003), 39–86.

[27] Kurihara, M., On the structure of ideal class groups of CM-fields. *Documenta Math.* Extra Vol. (2003), 539–563.

[28] Kurihara, M., On the structure of Iwasawa modules. *Sūrikaisekikenkyūsho Kōkyūroku* **1451** (2005), 216–224.

[29] Mazur, B., and Swinnerton-Dyer, P, Arithmetic of Weil curves. *Invent. Math.* **25** (1974), 1–61.

[30] Mazur, B., Tate, J., and Teitelbaum, J, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.* **84** (1986), 1–48.

[31] Mazur, B., and Tilouine, J, Représentations galoisiennes, différentielles de Kähler et "conjectures principales". *Inst. Hautes Études Sci. Publ. Math.* **71** (1990), 65–103.

[32] Mazur, B., and Wiles, A., Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.* **76** (1984), 179–330.

[33] McConnell, J. C., and Robson, J. C., *Noncommutative Noetherian rings*. Grad. Stud. in Math. 30, Amer. Math. Soc., Providence, RI, 2001.

[34] Perrin-Riou, B., Fonctions L p-adiques des représentations p-adiques. *Astérisque* **229** (1995).

[35] Ribet, K. A., A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.* **34** (1976), 151–162.

[36] Rohrlich, D. E., Root numbers of semi-stable elliptic curves in division towers. *Math. Res. Lett.* **13** (2–3) (2006), 359–376.

[37] Rubin, K., The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* **103** (1991), 25–68.

[38] Rubin, K., *Euler systems*. Ann. of Math. Stud. 147, Princeton University Press, Princeton, NJ, 2000.

[39] Ritter, J. and Weiss, A., Toward equivariant Iwasawa theory, II. *Indag. Math.* (*N.S.*) **15** (2004), 549–572.

[40] Schneider, P., Motivic Iwasawa theory. In *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, 421–456.

[41] Skinner, C., Main conjectures and modular forms. Preprint.

[42] Thaine, F., On the ideal class groups of real abelian number fields. *Ann. of Math.* **128** (1988), 1–18.

[43] Venjakob, O., Characteristic elements in non-commutative Iwasawa theory. *J. Reine Angew. Math.* **583** (2005), 193–236.

[44] Wiles, A., The Iwasawa conjecture for totally real fields. *Ann. of Math.* **131** (1990), 493–540.

[45] Wiles, A., Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* **141** (1995), 443–551.

[46] Weibel, C., and Yao, D., Localization for the K theory of noncommutative rings. In *Algebraic K-theory, commutative algebra, and algebraic geometry* (Santa Margherita Ligure, 1989), Contemp. Math. 126, Amer. Math. Soc., Providence, RI, 1992, 219–230.

Department of Mathematics, Kyoto University, Sakyo, Kyoto, Kyoto 606, Japan
E-mail: kzkt@math.kyoto-u.ac.jp

Energy-driven pattern formation

Robert V. Kohn*

Abstract. Many physical systems can be modelled by nonconvex variational problems regularized by higher-order terms. Examples include martensitic phase transformation, micromagnetics, and the Ginzburg–Landau model of nucleation. We are interested in the singular limit, when the coefficient of the higher-order term tends to zero. Our attention is on the internal structure of walls, and the character of microstructure when it forms. We also study the pathways of thermally-activated transitions, modeled via the minimization of action rather than energy. Our viewpoint is variational, focusing on matching upper and lower bounds.

Mathematics Subject Classification (2000). Primary 49-02, 82-02; Secondary 74N15, 82B24, 82D40.

Keywords. Action minimization, Aviles–Giga problem, calculus of variations, cross-tie wall, martensitic transformation, micromagnetics, microstructure.

1. Introduction

Many physical systems are described by nonconvex variational problems regularized by higher-order terms. Two of the simplest examples are the Ginzburg–Landau energy

$$\int_\Omega (u^2-1)^2 + \varepsilon^2 |\nabla u|^2$$

and the Aviles–Giga energy

$$\int_\Omega (|\nabla u|^2-1)^2 + \varepsilon^2 |\nabla\nabla u|^2.$$

The former is a basic model of nucleation; we shall discuss it in Section 4. The latter arises in many settings, including convective pattern formation and magnetic thin films; we shall discuss it in Section 3. Other, more complicated examples include micromagnetics and martensitic transformation; we shall discuss them too, in Section 2. Our focus is always on the singular limit $\varepsilon \to 0$.

In some settings, minimizers get increasingly complicated as $\varepsilon \to 0$. We call this the development of *microstructure*. We shall discuss two examples in Section 2, involving twinning in martensite [40] and the branching of domains in a uniaxial

*This work was partially supported by NSF, most recently through grant DMS0313744.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

ferromagnet [13]. When microstructure forms, we are interested in its local character and length scale.

In most settings, minimizers develop sharp transition layers where there is rapid spatial variation. Outside these layers the solution is relatively smooth. We call the transition layers *walls* and the smooth regions *domains*. We are interested in the internal structure of walls, and in evaluating their surface energies. We shall discuss two examples in Section 3, involving the Aviles–Giga energy [38] and cross-tie walls in ferromagnetic thin films [1].

Finally, we are interested in local as well as global minimizers, and in thermally-activated transitions between them. We shall explain in Section 4.1 how large deviation theory leads to the minimization of *action* rather than energy. Then, in Section 4.2, we discuss the singular limit of action minimization for the Ginzburg–Landau functional [42].

Our viewpoint is variational: we focus on the leading-order dependence of the energy upon ε. In problems with microstructure we find the optimal scaling law (Section 2); though the argument does not determine the minimizer, it does give information about its character. In problems involving walls (Sections 3 and 4) the scaling law is obvious and our achievement is to find the prefactor. In the process, we also determine an example of a minimizer.

Upper bounds on the minimum energy are usually easy, by considering appropriate test functions. Lower bounds are much more difficult, however, since our functionals are nonconvex. The main mathematical accomplishment in each of our examples is an ansatz-independent lower bound:

(a) For the examples involving microstructure (Section 2), the heart of the matter is an interpolation inequality (10). It expresses mathematically the fact that development of fine-scale microstructure requires a lot of surface energy.

(b) For the examples involving walls (Section 3), the heart of the matter is the use of a suitable "entropy." Recall that for a conservation law, entropy is dissipated at shocks. Our entropies are analogous, in the sense that the divergence is concentrated at walls.

(c) For the example involving action minimization (Section 4), the heart of the matter is the separation of the action into two parts: the "nucleation cost" and the "propagation cost."

It should be clear by now that our goal is not to survey the field of energy-driven pattern formation. Such a survey would be extremely difficult, because the subject is vast and ill-defined. Even if we limited attention to recent mathematical work based on singularly perturbed variational problems, a survey would have to include diblock-copolymers [11], [55], energy-driven coarsening [41], compressed thin film blisters [7], dislocation patterns in plasticity [17], vortex patterns in type-II superconductors [59], the intermediate state of a type-I superconductor [14], and many

additional examples from micromagnetics [21]. (This list is of course incomplete, and the citations are simply examples selected from a huge literature.)

Our aim is much more limited. The primary goal of this paper is to communicate the methodological developments summarized in (a)–(c) above. In addition, we will explain the materials science problems that led to these developments.

Proving lower bounds is difficult, but guessing them is easier. This is particularly true in problems from physics, where experimental observations are available. Therefore it should not be surprising that many of our results were guessed long ago. For example, the scaling of the minimum energy for a uniaxial ferromagnet (Section 2.2) has been "known" for decades [33], [52]. The cross-tie wall, however, is an exception to this rule. As we shall explain in Section 3.2, the analysis of [1] finds the optimal wall structure explicitly. Prior to that work the structure was known only from numerical and physical experiments [50].

1.1. Warmup: one space dimension. For context and background, it is useful to review a simple 1D example. Consider the minimization of

$$\int_0^1 \frac{1}{\varepsilon}(u_x^2 - 1)^2 + \varepsilon u_{xx}^2 + \alpha u^2 \tag{1}$$

where ε and α are positive. The first term prefers $u_x = \pm 1$; the second penalizes changes of slope; the third penalizes deviations from 0. Their preferences are incompatible, and the competition between them determines the character of the minimizer. When ε is small, the optimal u is a sawtooth function as shown in Figure 1. Its slope is nearly ± 1 except for a transition region (whose length is of order ε) near each peak and valley. The distance between peaks and valleys is determined by the competition

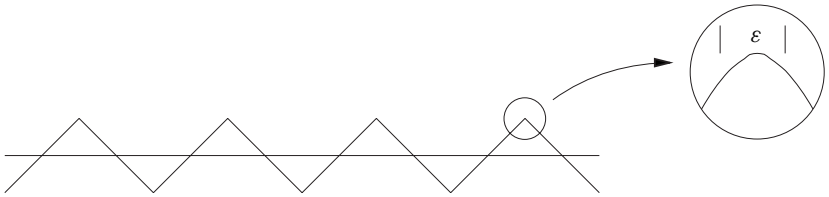


Figure 1. A minimizer of (1).

between the first two terms (which attribute energy to each peak and valley) and the last term (which prefers u to be small). This is most evident in the limit $\varepsilon \to 0$, when each transition layer shrinks to a point. If $2c_0$ is the energy of an (optimal) transition layer, then the limiting variational problem as $\varepsilon \to 0$ is the minimization of

$$\int_0^1 c_0|u_{xx}| + \alpha u^2 \tag{2}$$

subject to the condition $u_x = \pm 1$.

The statement that (2) captures the asymptotic behavior of (1) can be proved with mathematical rigor: this is a basic example of Γ-convergence, see e.g. [9]. In this article we shall work mainly at positive ε, so we do not make use of Γ-convergence in any formal sense. Our viewpoint, however, is very similar. In particular, the following argument – which amounts to the identification of the constant c_0 in (2) [46] – will recur repeatedly. Consider a function u such that $u_x = -1$ near $x = a$ and $u_x = +1$ near $x = b$. Then

$$\int_a^b \frac{1}{\varepsilon}(u_x^2 - 1)^2 + \varepsilon u_{xx}^2 \geq \int_a^b 2|1 - u_x^2||u_{xx}| = \int_a^b |[\Phi(u_x)]_x| \tag{3}$$

if $\Phi'(t) = 2|1 - t^2|$. Since

$$\int_a^b |[\Phi(u_x)]_x| \geq \left| \int_a^b [\Phi(u_x)]_x \right| = |\Phi(1) - \Phi(-1)| = 2\int_{-1}^1 (1 - t^2)$$

we conclude that the cost $2c_0$ of a peak or valley in (1) is at least

$$2\int_{-1}^1 (1 - t^2) = 8/3.$$

Moreover this estimate is sharp, and it reveals the internal character of the transition layer: for equality to hold in (3) we need

$$|1 - u_x^2| = \varepsilon |u_{xx}|$$

from which it follows easily that $u_x = \tanh(x/\varepsilon)$. We have omitted some details, of course; at finite ε the assumptions $u_x(a) = -1$ and $u_x(b) = +1$ are only approximately valid. Still, the preceding calculation captures the heart of the matter.

Our example (1) is local, in the sense that the energy involves only u, u_x, and u_{xx}. But it can also be viewed as a nonlocal problem. Indeed, if we treat $v = u_x$ as our basic variable, and write $u = \nabla^{-1} v$ as an indefinite integral of v, then (1) is equivalent to minimizing

$$\int_0^1 \frac{1}{\varepsilon}(v^2 - 1)^2 + \varepsilon v_x^2 + \alpha |\nabla^{-1} v|^2. \tag{4}$$

From this perspective, space gets divided into "domains" where $v \approx \pm 1$, separated by "walls" where v changes rapidly, on a length scale of order ε.

The problems considered in Sections 2–4 can be viewed as multidimensional analogues of (1) or (4). The multidimensional setting introduces new challenges, and many phenomena not seen in one space dimension. But 1D examples are rich, and their analysis has taught us a lot. For example, these functionals have many local minima, and it is natural to inquire about the character of those states. Are they periodic in x, or can they have "defects"? For studies of this type see [48], [54], [62], [64].

2. Singular perturbation and the development of microstructure

We say a singularly-perturbed variational problem develops microstructure if its minimizers become increasingly complicated as $\varepsilon \to 0$. In this section we discuss two examples, from martensitic transformation and micromagnetics.

2.1. Refinement of twins. A simple 2D analogue of (2) was introduced in 1992 by Kohn and Müller:

$$\min_{\substack{u_y=\pm 1 \\ u=0 \text{ at } x=0}} \int_0^1 \int_0^L u_x^2 + \varepsilon |u_{yy}| \, dx \, dy \tag{5}$$

where $u = u(x, y)$ is scalar-valued. The constraint $u_y = \pm 1$ applies in the interior of the region $(0, L) \times (0, 1)$. It is clearly incompatible with the boundary condition $u = 0$ at $x = 0$, so we expect ∇u to be oscillatory near $x = 0$. The regions where $u_y = \pm 1$ are "domains," and the discontinuities of u_y are "walls." The term $\iint \varepsilon |u_{yy}| \, dx \, dy$ in (5) represents surface energy: since u_y jumps between ± 1 at each interface, it simply counts 2ε times the number of interfaces above x then integrates over $x \in (0, L)$.

This is a simplified model for the geometry of twinning near an austenite twinned-martensite interface, in a crystalline solid undergoing a martensitic phase transformation [39]. Briefly: in the "twinned" region $(0, L) \times (0, 1)$ there are two preferred values $\nabla u = (0, 1)$ and $\nabla u = (0, -1)$, corresponding to two "variants" of martensite. The first term in (5) represents "elastic energy;" it penalizes deviations from the preferred values of ∇u. The second term represents the surface energy of the twin boundaries. We suppose the material occupying the region $x < 0$ is untwinned and rigid; hence the boundary condition $u = 0$ at $x = 0$. See [39] for a more detailed account of the crystallography behind (5), and [8] for a modern introduction to martensitic phase transformation with a variational viewpoint.

The most basic result about (5) is the assertion that

$$C\varepsilon^{2/3} L^{1/3} \leq \text{minimum energy} \leq C' \varepsilon^{2/3} L^{1/3} \tag{6}$$

when ε / L is sufficiently small [40]. Thus, we know the *scaling law* of the minimum energy – though not the prefactor.

The right hand side of (6) – the upper bound – is relatively easy to prove. It suffices to give a single example of a function u with the desired scaling. The convenient construction is self-similar; in particular, the length scale of the twins at x decreases geometrically as x approaches 0. Figure 2a sketches the construction by showing two generations of refinement.

The left hand side of (6) – the lower bound – requires an entirely different type of argument. No example or numerical simulation can be of any use. Rather, we require a geometry-independent argument explaining why no microstructure can do better. In a convex variational problem we would turn to the convex dual. But our example is very nonconvex, due to the constraint $u_y = \pm 1$.

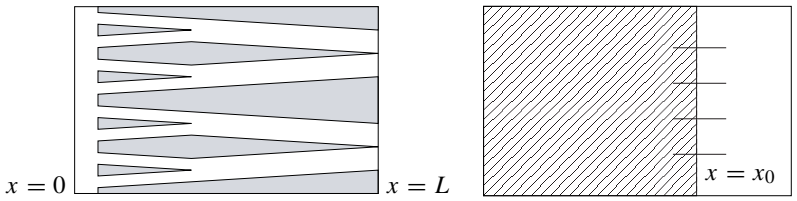


Figure 2. (a) Two generations of the self-similar construction used to prove the upper bound. (b) Visual aid for the lower bound. If there are few interfaces at x_0 then the integral of u_x^2 over the hatched region must be large.

The successful argument is actually quite elementary. It rests on two simple facts:

Fact 1. *If the graph of f is a sawtooth with few teeth, then it must make large excursions. More precisely: if $f_y = \pm 1$ then*

$$\int_0^1 f^2\,dy \geq C/(N+1)^2 \quad \textit{if the slope changes } N \textit{ times.}$$

Fact 2. *The integral of u_x^2 controls the variation of u with respect to x. In particular:*

$$\int_0^1 |u(b,y) - u(a,y)|^2\,dy \leq (b-a)\int_0^1 \int_a^b u_x^2\,dx\,dy.$$

Using these, the lower bound is proved as follows (c.f. Figure 2b). For any u such that $u = 0$ at $x = 0$ and $u_y = \pm 1$, let

$$E = \int_0^1 \int_0^L u_x^2 + \varepsilon |u_{yy}|\,dx\,dy$$

be the associated energy.

Step 1. Since the second term in E controls the wall energy, for some $0 < x_0 < L$ the number of walls above x_0 is less than or equal a constant times $E/\varepsilon L$. We conclude using Fact 1 that

$$\int_0^1 u^2(x_0,y)\,dy \geq C\varepsilon^2 L^2/E^2.$$

Step 2. Since the first term in E is u_x^2, the boundary condition together with Fact 2 give

$$LE \geq \int_0^1 u^2(x_0,y)\,dy.$$

Step 3. Combining both steps, we have shown that $LE \geq C\varepsilon^2 L^2/E^2$. Rearrangement gives the desired lower bound $E \geq C\varepsilon^{2/3}L^{1/3}$.

This argument is so easy it leaves one a bit uncomfortable. What makes it work, and how can it be generalized? The answer will become evident in Section 2.2.

In focusing on upper and lower bounds, we have presented only the most basic result concerning (5). Much more can be proved, including an estimate for the length scale of twinning as a function of x [40]. Conti has studied the fine-scale structure of a minimizer near $x = 0$, showing roughly speaking that it is asymptotically self-similar [15].

2.2. Branching of magnetic domains. The branching of domains in a uniaxial ferromagnet combines features of our 1D model problem (1) and our 2D example (5). The problem is richer and more difficult, however, because the domain patterns are fully three-dimensional. A sharp-interface version of this problem was treated in [13]. The following discussion, based on standard micromagnetics and drawn from [21], is only slightly different.

The phenomenon we wish to capture is sketched in Figure 3b; experimental images (which are of course much richer and more detailed) can be found in Section 5.2.1 of [34]. Briefly: we are considering a cylinder occupied by a uniaxial ferromagnet. The magnetization has two preferred values, $m = (1, 0, 0)$ or $m = (-1, 0, 0)$. The observed configurations are local minima of the micromagnetic energy, which is defined by

$$\int_{\text{magnet}} Q(m_2^2 + m_3^2) + \varepsilon^2 |\nabla m|^2 \; + \int_{\text{all space}} |\nabla \phi|^2 \tag{7}$$

where m is the magnetization (a unit vector field defined on the magnet, extended by 0 outside) and ϕ is defined by solving

$$\Delta \phi = \operatorname{div} m. \tag{8}$$

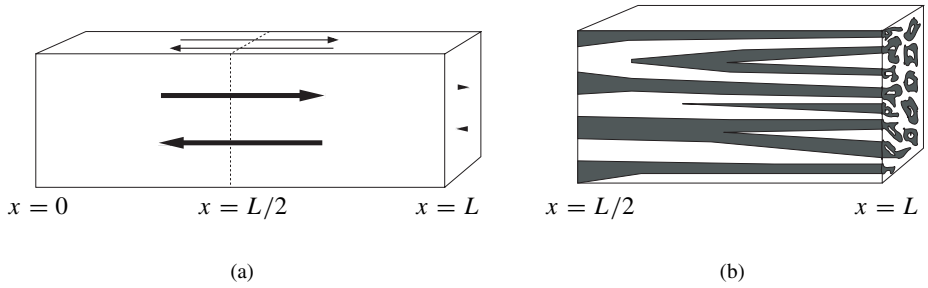


Figure 3. (a) Sketch of our uniaxial ferromagnet, with the preferred magnetization direction parallel to the axis. (b) Sketch of the magnetic domain structure.

The first term in (7) expresses the anisotropy of the crystal, in other words its preference for $m = (\pm 1, 0, 0)$. The second term, known as the exchange energy, penalizes sharp changes in m and is directly analogous to the term εu_{xx}^2 in our one-dimensional example; when ε is small it forces the creation of walls and determines their energy. The nonlocal magnetostatic energy $\int |\nabla \phi|^2$ comes from Maxwell's equations. It expresses a preference for m to be divergence-free, since (8) is equivalent to the statement that

$$m = \nabla \phi + \text{divergence-free}.$$

(Thus, $\nabla \phi$ is the Helmholtz projection of m onto the space of gradients.)

The origin of the microstructure sketched in Figure 3b is easy to explain heuristically. The magnetization wants to be $(\pm 1, 0, 0)$ in the cylinder, but its extension by 0 to all $\mathbb{R}^3$ wants to be weakly divergence-free. It cannot do both, since being divergence-free would require $m \cdot n$ to vanish at the end of the cylinder. So the magnetization compromises, making the magnetostatic energy small by oscillating rapidly in space between the preferred values $(\pm 1, 0, 0)$ at the end of the cylinder. This requires the introduction of walls across which m_1 changes from 1 to -1. The magnetostatic term likes walls parallel to the x_1-axis (since such walls are weakly divergence-free). However the walls carry surface energy, on account of the exchange term $\varepsilon^2 |\nabla m|^2$. So the domain structure coarsens away from the end of the cylinder – though this means the walls are not exactly parallel to the axis.

Overall: the situation is quite similar to the twinning example discussed in Section 2.1. There ∇u was two-dimensional and exactly curl-free; it developed fine-scale structure near $x = 0$ due to the boundary condition $u = 0$ at $x = 0$. Here m is three-dimensional and only approximately divergence-free; it develops fine-scale structure so that $m \cdot n$ is approximately zero at the end of the cylinder.

Mathematically: the analogue of (6) in this setting is the assertion that for a minimizer,

$$C Q^{1/3} \varepsilon^{2/3} L^{1/3} \leq \frac{\text{energy}}{\text{cross-sectional area}} \leq C' Q^{1/3} \varepsilon^{2/3} L^{1/3} \tag{9}$$

provided Q is sufficiently large and ε / L sufficiently small.

Proving the upper bound is conceptually easy. One must simply give an example of an m with the desired scaling. This is done in [12], [52] for a slightly different model in which interfaces are sharp rather than diffuse. (See see also [21] for a concise summary.) The convenient construction involves branching, but none of the 3D complexity of Figure 3b. Thus the magnetization patterns seen in real magnets are geometrically complicated not because complexity is required for the optimal scaling law, but rather because complexity is a feature of the many local minima consistent with this scaling.

As in Section 2.1, the lower bound provides an entirely different and more interesting challenge. It is natural to simplify the problem slightly by assuming periodicity (rather than a finite-sized magnet) in the x_2 and x_3 variables. This helps by permitting us to focus on the essential physics – namely the competing effects of the anisotropy,

exchange and magnetostatic energies. The main steps are parallel to those of our twinning example:

Fact 0. *The energy controls wall area.*

Fact 1. *Consider a particular section $x_1 = a$. If in this slice the perimeter of the walls is small, then the H^{-1} norm of m_1 must be large.*

Fact 2. *The energy controls the variation of m_1 in the H^{-1} norm.*

Let us explain each assertion briefly. Our twinning example had the wall energy built into the functional, so the analogue of Fact 0 was automatic there. In the present setting we must instead argue as for (3). Since $2xy \le x^2 + y^2$ we have

$$2\varepsilon Q^{1/2}|\nabla m_1| \le \frac{\varepsilon^2}{1-m_1^2}|\nabla m_1|^2 + Q(1-m_1^2).$$

But by differentiating the constraint $m_1^2 + m_2^2 + m_3^2 = 1$ one easily sees that

$$\frac{|\nabla m_1|^2}{1-m_1^2} \le |\nabla m|^2.$$

Therefore

$$2\varepsilon Q^{1/2}\int |\nabla m_1| \le \int Q(m_2^2+m_3^2) + \varepsilon^2|\nabla m|^2.$$

Since $m_1 \approx \pm 1$ in the domains, the left hand side is roughly a constant times the total surface area of the walls. Thus the wall energy is controlled by the sum of anisotropy and exchange energy.

The essence of Fact 1 is the following interpolation inequality: if $S = [0,1]^n$ is the unit cube in $\mathbb{R}^n$ and $g\colon S \to \mathbb{R}$ is periodic with mean value 0 then

$$\int_S g^2 \le C\|g\|_{L^\infty}^{2/3}\left(\int_S |\nabla g|\right)^{2/3}\|g\|_{H^{-1}(S)}^{2/3} \tag{10}$$

where the H^{-1} norm is defined by

$$\|g\|_{H^{-1}(S)}^2 = \int_S |\nabla \Delta^{-1} g|^2$$

Substituting m_1 for g and a scaled section of our cylinder for S, the left hand side of (10) is fixed so the right hand side stipulates a tradeoff between the perimeter $\int |\nabla m_1|$ and the H^{-1} norm of m_1. The interpolation inequality (10) is not exactly standard, but the proof is relatively easy; see e.g. [16] for a concise proof and an interesting extension. Such interpolation inequalities have been used a lot in recent work on energy-driven pattern formation, not only for understanding the consequences of energy minimization, but also for proving bounds on coarsening rates, see e.g. [16], [41], [44]. Their broad importance is due to the special form of the right hand side,

which relates the BV norm (a proxy for perimeter) to a negative norm (a proxy for the length scale of microstructure). Our Fact 1 in Section 2.1 did not assume periodicity; however when f_y is periodic it is an immediate consequence of (10), obtained by taking $S = [0, 1]$ and $g = f_y$.

The essence of Fact 2 is easiest to see in the special case when $\operatorname{div} m = 0$. We also assume m is periodic in x_2 and x_3 with period cell S. Then the variation of m_1 with respect to x_1 is estimated by

$$\|m_1(a,\cdot) - m_1(b,\cdot)\|_{H^{-1}(S)} = \sup_{\int |\nabla v|^2 \le 1} \int_S [m_1(a,\cdot) - m_1(b,\cdot)]v$$

and the right hand side equals

$$\begin{aligned}\int_a^b \int_S (\partial_1 m_1)v &= -\int_a^b \int_S (\partial_2 m_2 + \partial_3 m_3)v \\ &= \int_a^b \int_S (m_2, m_3)\cdot \nabla v \\ &\le \left(\int_a^b \int_S m_2^2 + m_3^2\right)^{1/2} \left(\int_a^b \int_S |\nabla v|^2\right)^{1/2}.\end{aligned}$$

Thus when $\operatorname{div} m = 0$ the variation of m_1 with respect to x_1 in the H^{-1} norm is controlled by the anisotropy energy.

The argument for the lower bound in (9) is parallel to the one sketched in Section 2.1 for (6).

Step 1. If the energy is small then in a generic section the walls have small perimeter (Fact 0). So the H^{-1} norm of m_1 in the section is large (Fact 1).

Step 2. If the energy is small then the H^{-1} norm of m_1 cannot change significantly as x_1 varies (Fact 2). So the H^{-1} norm is large at the end of the cylinder, and (simplifying the argument a bit) this forces the magnetostatic energy to be large.

Step 3. Combining both steps, we find that the energy cannot be small after all.

We have cheated a little. In truth m_1 is neither divergence-free nor exactly mean 0 in each section. The full argument, presented in [13] and [21], proceeds a bit differently, working in Fourier space to take full advantage of the magnetostatic energy. The bottom line, however, is similar to the steps sketched above.

Our understanding of this problem is far less complete than the one discussed in Section 2.1. In particular, while our methods give an estimate for the total area of all the domain boundaries in the magnet, they do not give rigorous results on the local length scale as a function of x.

There are many other problems where nonlocal effects promote microstructure. Bounds analogous to (9) have been proved for a few of them, including diblock

copolymers [11] and the intermediate state of a type-I superconductor [14]. However there are limits to what can be achieved this way. For example, in diblock copolymers the choice of microstructure seems to depend mainly on volume fraction. This cannot be seen from the scaling law; rather, different patterns achieve different prefactors.

3. Singular perturbation and the structure of walls

The problems considered in Section 2 develop microstructure, in the sense that minimizers become increasingly complex as $\varepsilon \to 0$. In proving energy scaling laws, we acquire insight about the character of this microstructure.

Here we turn to a different issue, namely the internal structure of a wall. This question is meaningful and interesting even when there is no microstructure. We begin with a problem of that type – the Aviles–Giga energy – which provides a convenient warmup. Then we discuss the striking recent work of Alouges, Rivière, and Serfaty on the internal structure of a cross-tie wall [1].

3.1. The Aviles–Giga problem. Aviles and Giga asked in [4], [5] what we know about

$$\min_{u=0 \text{ at } \partial\Omega} \int_\Omega \frac{1}{\varepsilon}(|\nabla u|^2 - 1)^2 + \varepsilon |\nabla \nabla u|^2 \tag{11}$$

where Ω is a bounded domain in $\mathbb{R}^2$ and u is a scalar-valued function. Their motivation came from the modeling of smectic liquid crystals, but the same functional arises in the Cross–Newell approach to convective pattern formation [27] and in the modeling of a soft, thin magnetic film with cross-section Ω [38], [63]. Explaining just the last interpretation: the magnetostatic energy prefers $\operatorname{div} m = 0$ in the film and $m \cdot n = 0$ at its edges. If we suppose m depends only on (x, y) then these conditions are equivalent to $(m_1, m_2) = (u_y, -u_x)$ in Ω with $u = 0$ at $\partial\Omega$. The magnetostatic term also prefers $m_3 = \sqrt{1 - |\nabla u|^2}$ to be zero. Thus the sum of magnetostatic and exchange energy is a lot like (11).

As $\varepsilon \to 0$ the energy clearly prefers $|\nabla u| = 1$. If Ω is not a circle then the graph of u must have "folds," and it is natural to guess that if u_ε minimizes (11) then $\lim u_\varepsilon = u_0$ exists and solves a suitable "asymptotic problem" of the form

$$\min_{\substack{|\nabla u|=1 \\ u=0 \text{ at } \partial\Omega}} \int_{\text{folds}} \text{fold energy}. \tag{12}$$

Notice that the class of admissible functions for (12) is somewhat rigid; two examples are shown in Figure 4a.

What is the fold energy? If we assume that the internal structure of a fold is "one-dimensional," i.e. that ∇u depends only on the variable transverse to the fold,

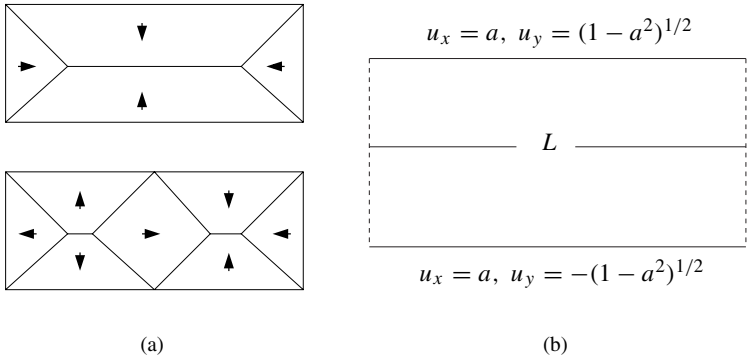


Figure 4. (a) Two admissible configurations for the asymptotic energy (12) (the arrow shows the direction of ∇u). (b) The boundary value problem used to determine the fold energy.

then the energy is easily calculated by an argument similar to (3). The answer is

$$\text{fold energy} = \int_{\text{fold}} \frac{1}{3} \, |[\partial u/\partial n]|^3 \tag{13}$$

where the square bracket denotes the jump of the normal derivative of u across the fold. Thus for a fold parallel to the x-axis across which ∇u jumps from $(a, \sqrt{1-a^2})$ to $(a, -\sqrt{1-a^2})$, the fold energy per unit arc length would be $\frac{8}{3}(1-a^2)^{3/2}$.

But is this calculation right? A proper calculation of the fold energy should assume nothing about its internal structure, proving rather than assuming that it is one dimensional. A scheme for achieving this was introduced in [38]. Focusing for simplicity on folds parallel to the x-axis, the idea is to consider the Aviles–Giga energy in a rectangle, with boundary conditions consistent with a fold as shown in Figure 4b. The height of the strip is 1; the length is L; and ∇u is assumed to be periodic in x with period L. If we can show for such u that

$$\liminf_{\varepsilon \to 0} \int \frac{1}{\varepsilon}(|\nabla u|^2 - 1)^2 + \varepsilon |\nabla \nabla u|^2 \geq \frac{8}{3}(1-a^2)^{3/2} L \tag{14}$$

we will effectively have shown that folds are indeed one-dimensional – or more precisely that there is no incentive to be otherwise.

The proof of (14) involves little more than a clever integration by parts. Suppose we can find a smooth $\Sigma : \mathbb{R}^2 \to \mathbb{R}^2$ such that

$$|\text{div}\, \Sigma(\nabla u)| \leq \frac{1}{\varepsilon}(|\nabla u|^2 - 1)^2 + \varepsilon |\nabla \nabla u|^2 \tag{15}$$

for any $u(x, y)$, with the further property that

$$\Sigma(a, \sqrt{1-a^2}) \cdot (0, 1) + \Sigma(a, -\sqrt{1-a^2}) \cdot (0, -1) = \frac{8}{3}(1-a^2)^{3/2}. \tag{16}$$

Then the integral of the Aviles–Giga energy is bounded below by

$$\int |\text{div } \Sigma(\nabla u)| \geq \left| \int \text{div } \Sigma(\nabla u) \right| = \frac{8}{3}(1-a^2)^{3/2}L \tag{17}$$

using the boundary conditions and periodicity in the last step. This is the desired inequality.

The convenient choice of Σ is

$$\Sigma(\nabla u) = 2\Big(-\frac{1}{3}u_x^3 - u_x u_y^2 + u_x, \frac{1}{3}u_y^3 + u_y u_x^2 - u_y \Big).$$

It satisfies (16), and almost satisfies (15) – there is an extra term on the right hand side, whose value after integration is a constant times ε. Thus the extra term does not matter in the limit $\varepsilon \to 0$, and our argument shows that a one-dimensional wall is asymptotically optimal.

We call Σ an *entropy*. To explain why, notice that if Σ satisfies (15), then (by letting $\varepsilon \to 0$) $\Sigma(\nabla u)$ must be divergence-free wherever u is smooth and $|\nabla u| = 1$. Thus Σ bears the same relation to the eikonal equation that an entropy entropy-flux pair bears to a conservation law.

Our argument shows that a one-dimensional wall is optimal, but it does not show the wall *has* to be one-dimensional. In fact it does not: when $a = 0$ the optimal fold energy is also achieved as $\varepsilon \to 0$ by a two-dimensional pattern similar to a cross-tie wall [60].

We have focused rather narrowly, on the identification of the fold energy, but much more is known. In writing (12) we implicitly assumed that ∇u_ε remains compact, so $|\nabla u_0| = 1$ in the limit; this is true, but the proof is far from trivial [2], [19]. The introduction of entropies and the analogy with conservation laws has led to a lot of progress on this and related problems, including [3], [6], [18], [36], [37], [38], [45], [56], [57]. But the subject is far from finished. In particular, (12) has not yet been shown to be the Γ-limit of (11) as $\varepsilon \to 0$.

3.2. Cross-tie walls. The cross-tie wall is a specific type of domain wall seen in ferromagnetic thin films. Its striking feature is that the cross-tie wall is *not* one dimensional; rather, its structure varies along the wall as well as across it. Its pattern is certainly energy-driven: numerical minimization of the micromagnetic energy produces results quite similar to those seen in real materials. But the simulations do not tell us why the pattern forms or what determines its structure. These questions were recently addressed by Alouges, Rivière, and Serfaty [1]. Our summary will be a bit different from their exposition, following instead the discussion in [21].

As in Section 2.2, our starting point is the micromagnetic energy

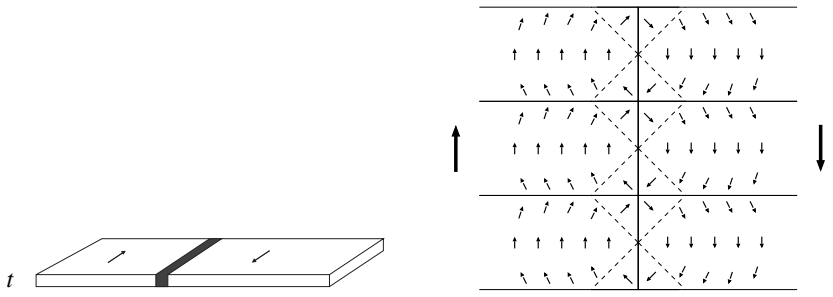
$$E = \int_{\text{film}} Q(m_2^2 + m_3^2) + \varepsilon^2 |\nabla m|^2 \; + \int_{\text{all space}} |\nabla \phi|^2$$

where $|m| = 1$ in the film, $m = 0$ outside, and

$$\Delta\phi = \operatorname{div} m.$$

However we are now interested in a soft thin film. The term "soft" means Q is small; in fact we shall take $Q = 0$. The film thickness t should be small, but not too small; when the material is permalloy, cross-tie walls are seen for thicknesses of order 30–80 nm. The model developed in [1] assumes the magnetization m depends only on (x_1, x_2); this is not required energetically [51], but it seems to be a good approximation for a cross-tie wall.

A cross-tie wall can have any angle greater than 90 degrees. To be specific, however, we focus on the case of a 180-degree wall. Its structure is sketched in Figure 5b. This is the magnetization, seen from the top of the film and zooming in on the wall. Far from the wall $(m_1, m_2) = (0, 1)$ at one extreme and $(0, -1)$ at the other. Within the wall m is piecewise smooth and weakly divergence-free. At the discontinuities (which are themselves walls) the angle changes by 90 degrees or less. Experimental images and numerical simulations very much like the figure can be found in [50] (see also [34]).



(a) (b)

Figure 5. (a) A thin film with a cross-tie wall, viewed from afar. (b) Magnetization within a 180-degree cross-tie wall, viewed from above the film. In each of the squares along the axis m is piecewise constant; outside those squares the lines of magnetization form circles. The solid vertical and horizontal lines are 1D Néel walls. The dashed lines mark places where m is continuous but not C^1; they are not walls.

The cross-tie wall forms because one-dimensional walls are very expensive when the wall angle is large. The structure shown in Figure 5b consists, in essence, of an ensemble of one-dimensional low-angle walls, whose total energy is less than that of a one-dimensional 180-degree wall.

The preceding intuition is old. It suffices to explain why one should not see large-angle one-dimensional walls. But it does not explain why the specific pattern shown in Figure 5b is optimal. Mathematically: the structure in the figure gives an upper

bound on the wall energy. To know it is optimal we need a matching lower bound. Its proof has three main steps:

Step 1. Simplification of the nonlocal term.

Step 2. Evaluation of the energy of a one-dimensional wall.

Step 3. Use of an appropriate entropy to show the cross-tie pattern is optimal.

We summarize each in turn.

Step 1. The hypothesis that m depends only on (x_1, x_2) makes it easy to evaluate the magnetostatic energy $\int |\nabla\phi|^2$ in terms of the Fourier transform of m. If we assume the relevant spatial frequencies ξ satisfy $t|\xi| \gg 1$ then the expression simplifies and

$$\begin{aligned}\int_{\mathbb{R}^3} |\nabla\phi|^2\,dx &\approx t\int_{\mathbb{R}^2} \frac{|\xi\cdot\hat{m}'|^2}{|\xi|^2}\,d\xi + \int_{\mathbb{R}^2}\frac{|\hat{m}_3|^2}{|\xi|}\,d\xi \\ &= t\|\operatorname{div} m'\|^2_{H^{-1}} + \|m_3\|^2_{H^{-1/2}}\end{aligned} \tag{18}$$

with the convention $m = (m_1, m_2, m_3) = (m', m_3)$. In assuming $t|\xi| \gg 1$ we are not assuming that t is large compared to the width of the cross-tie wall; rather, we are assuming that it is large compared to the width of the low-angle one-dimensional walls inside it. In practice this means $t/\varepsilon \gg 1$. For permalloy the value of ε is 5–10 nm and cross-tie walls are seen when the thickness t is 30–80 nm. Therefore the simplification leading to (18) is plausible, if not entirely compelling.

Step 2. The analysis of a one-dimensional wall in this regime is classical (it is sometimes called a "thick-film Néel wall"). Since the term involving m_3 in (18) has no factor of t, nonzero m_3 is very expensive. Therefore it is natural to assume that $m_3 = 0$. Suppose the wall is perpendicular to the x-axis, with $m = (\cos\theta_\infty, \sin\theta_\infty, 0)$ at one extreme and $m = (\cos\theta_\infty, -\sin\theta_\infty, 0)$ at the other. If the wall profile is $m = (\cos\theta(x), \sin\theta(x), 0)$ then its energy per unit length is

$$\begin{aligned}\int_{\text{film}} \varepsilon^2|\nabla m|^2 + \int_{\text{space}} |\nabla\phi|^2 &= t\int \varepsilon^2|\theta_x|^2\,dx + t\|m_{1x}\|^2_{H^{-1}} \\ &= t\int \varepsilon^2|\theta_x|^2 + |\cos\theta - \cos\theta_\infty|^2\,dx.\end{aligned} \tag{19}$$

This is a one-dimensional variational problem, similar to (1). Solving it, one finds

$$\text{energy density of a 1D wall} = 4\varepsilon t(\sin\theta_\infty - \theta_\infty\cos\theta_\infty). \tag{20}$$

Step 3. It is easy to see that the pattern sketched in Figure 5b does better than a one-dimensional 180-degree wall. Indeed, using (20) and doing some elementary integrations one finds that the figure achieves energy per unit length

$$4\varepsilon t(\sqrt{2} - 1). \tag{21}$$

This beats $4\varepsilon t\big(\sin\frac{\pi}{2} - \frac{\pi}{2}\cos\frac{\pi}{2}\big) = 4\varepsilon t$, the energy of the one-dimensional wall.

But why is the figure optimal? Proceeding as we did for the Aviles–Giga problem, it is natural to consider a rectangle with $(m_1, m_2) = (0, 1)$ on the left, $(m_1, m_2) = (0, -1)$ on the right, and periodic boundary conditions on the top and bottom. Let us focus for simplicity on magnetizations m that are piecewise smooth, with $m_3 = 0$ and $m_1^2 + m_2^2 = 1$, such that $\operatorname{div} m = 0$ weakly (even across any walls). Suppose we can find a differentiable function $\Sigma = [\Sigma_1(m_1, m_2), \Sigma_2(m_1, m_2)]$ such that

$$\operatorname{div} \Sigma(m) = 0 \text{ when } m \text{ is smooth with } \operatorname{div} m = 0 \text{ and } |m| = 1, \tag{22}$$

and such that when m has a weakly divergence-free wall

$$|[\Sigma(m) \cdot n]| \leq \text{1D wall energy density}, \tag{23}$$

where $[\Sigma(m) \cdot n]$ is the jump in $\Sigma(m) \cdot n$. Then arguing as in (17), we find that the total energy of the walls in the rectangle is bounded below by the integral of $\Sigma(m) \cdot n$ over the boundary. This shows that

$$\text{energy density of any pattern} \geq \Sigma(0, 1) \cdot (-1, 0) + \Sigma(0, -1) \cdot (1, 0). \tag{24}$$

If in addition to (22) and (23) the right side of (24) is equal to (21) then this argument shows the pattern is optimal within the class under consideration. Remarkably such a Σ exists! The formula is

$$\frac{1}{2\varepsilon t}\Sigma(m) = \begin{cases} \theta m + m^\perp + (0, -\sqrt{2}) & \text{for } -\frac{\pi}{4} \leq \theta \leq \frac{\pi}{4} \\ \left(\frac{\pi}{2} - \theta\right) m - m^\perp + (-\sqrt{2}, 0) & \text{for } \frac{\pi}{4} \leq \theta \leq \frac{3\pi}{4} \\ (\theta - \pi) m + m^\perp + (0, \sqrt{2}) & \text{for } \frac{3\pi}{4} \leq \theta \leq \frac{5\pi}{4} \\ \left(\frac{3\pi}{2} - \theta\right) m - m^\perp + (\sqrt{2}, 0) & \text{for } \frac{5\pi}{4} \leq \theta \leq \frac{7\pi}{4} \end{cases} \tag{25}$$

when $m = (\cos\theta, \sin\theta)$ and $m^\perp = (-\sin\theta, \cos\theta)$. We emphasize that $\Sigma(m)$ is well-defined for any $m \in S^1$, though θ is only defined modulo 2π. This is important, because there is no reason for θ to be well-defined throughout the rectangle. Rather, the internal walls (where m is discontinuous) can contain vortices – indeed, this is the case for the pattern in Figure 5b.

Why, exactly, does the pattern in the figure achieve equality in the lower bound? The formula (25) specifies Σ separately in four quadrants. One can show that if the internal walls remain in a single quadrant then equality holds in (24). Thus the crucial feature of Figure 5b is that it achieves the effect of a 180-degree wall using only walls with angle 90 degrees or less.

We assumed m was piecewise smooth to capture the main ideas in their simplest possible form. The micromagnetic energy does not permit sharp discontinuities. Therefore the one-dimensional walls in the pattern should be diffuse not sharp; moreover inside such walls we must expect that $\operatorname{div} m \neq 0$, and even (near vortices) that $m_3 \neq 0$. The argument in [1] addresses these subtleties.

It is natural to ask what sets the internal length scale of a cross-tie wall. The answer involves effects we have thus far ignored [20]. Briefly: the anisotropy energy

is small but nonzero; it prefers the length scale to be as small as possible. But at finite t/ε, one-dimensional Néel walls have long tails, which interact repulsively; this favors longer length scales. The internal period of the wall structure is set by the competition between these two effects.

The cross-tie wall is not the only case of a singularly perturbed variational problem whose transition layers are multidimensional. This example is special, however, because we have matching upper and lower bounds – i.e. we know the wall energy, and an optimal wall profile.

4. Action rather than energy minimization

We have been discussing nonconvex variational problems from materials science. Their local minima represent stable states. Since the nonconvexity is extreme, we expect the energy to have multiple minima. We have nevertheless focused on upper and lower bounds rather than on identifying the local minima. This approach is reasonable: in some cases (such as cross-tie walls) nature seems to find the ground state, and in other cases (such as uniaxial ferromagnets) the accessible local minima seem to share many features with the ground state.

But the fact remains: nature finds *local* not global minima. The evidence is all around us. Crystals have defects. Water can be heated above 100 degrees. The bubbles atop a glass of beer appear stable, but they eventually disappear.

These examples reveal more than the mere existence of local minima. They also show that nature escapes from local minima, as a consequence of thermal fluctuation. For a finite-dimensional system with energy $E(z)$, the competition between energy minimization and thermal fluctuation is captured by the stochastic differential equation

$$dz = -\nabla E\, dt + \sqrt{2\gamma}\, dw \tag{26}$$

where w is Brownian motion [32]. If γ is small then the system spends most of its time near the local minima of E. Transitions between the local minima are rare, but they do occur. Their timescales and pathways are predicted by the theory of large deviations [30].

4.1. Action minimization. Suppose $E(z)$ has local minima at z_0 and z_1. The large deviation principle says, roughly speaking, that if a transition from z_0 to z_1 occurs within time T then its pathway is (with very high probability) near the minimizer of the deterministic variational problem

$$S_T = \min_{\substack{z(0)=z_0 \\ z(T)=z_1}} \frac{1}{4}\int_0^T |z_t + \nabla E|^2\, dt. \tag{27}$$

Moreover the transitions are Poisson events, with timescale $e^{-S_T/\gamma}$.

The right hand side of (27) is called the *action*. It amounts in this example to the integrated "equation error" of the deterministic dynamics $z_t = -\nabla E$.

In the limit $T \to \infty$ the action-minimizing path is easy to describe: it goes directly uphill to the lowest mountain pass (saddle point) between z_0 and z_1, then proceeds directly downhill from there. The optimality of this choice is a consequence of the elementary relation

$$\frac{1}{4}\int_0^\tau |z_t + \nabla E|^2\,dt = \frac{1}{4}\int_0^\tau |z_t - \nabla E|^2\,dt + \int_0^\tau \langle z_t, \nabla E\rangle\,dt. \tag{28}$$

The first term is nonnegative, and the second term is $E(z(\tau)) - E(z_0)$. Let τ be the time when the trajectory crosses the ridge between z_0 and z_1. Then the right-hand side of (28) is minimized by the path for which the first term vanishes and $z(\tau)$ is the saddle point. Thus the action-minimizing path goes through the saddle, and the minimal action is the height of the mountain pass. This calculation explains why many studies of phase transition and nucleation reduce to the analysis of saddle points, viewed as "critical nuclei."

Saddle points are only relevant in the limit $T \to \infty$. Indeed, our argument suggested that $\int_0^\tau |z_t - \nabla E|^2\,dt$ should vanish for the optimal trajectory. But climbing from z_0 to the saddle along the steepest-ascent trajectory $z_t = \nabla E$ takes an infinite amount of time. So our calculation is only valid in the limit of large transition times.

Transitions occurring at shorter times T need not go through saddle points, but they are still interesting. This may seem counterintuitive, since such transitions are atypical and extremely rare (the minimum action S_T is a decreasing function of T). But rare, atypical events are often the ones we care about most. For example, suppose the typical lifespan of the hard disk in a computer is 10 years – longer than the lifespan of the machine itself. Then failures within the first year are rare and atypical – but hardly unimportant.

4.2. Ginzburg–Landau. What about infinite dimensional energy-driven systems, like those considered in Sections 2 and 3? Can we understand the character of action-minimizing pathways in the limit $\varepsilon \to 0$? For problems with the complexity of micromagnetics or martensitic phase transformation this question remains open. However for the simpler case of a scalar Ginzburg–Landau model there has been some progress [42], [43].

The Ginzburg–Landau functional is

$$E = \int_\Omega \frac{1}{4\varepsilon}(u^2-1)^2 + \frac{\varepsilon}{2}|\nabla u|^2 \tag{29}$$

where u is scalar valued. In one space dimension this is essentially our warmup problem (4) with $\alpha = 0$. In higher dimensions it is sometimes called the Modica-Mortola functional, and its Γ-limit as $\varepsilon \to 0$ is a constant times the perimeter of the interface separating the two "phases" $u = 1$ and $u = -1$ [46]. The associated

steepest-descent PDE $\dot{u} = -\nabla E$ is known as the Allen–Cahn equation. Its natural timescale (in dimension $n \geq 2$) is $1/\varepsilon$. Rescaling time so the dynamics proceeds with velocity of order 1, i.e. taking $\dot{u} = \varepsilon u_t$, the evolution becomes

$$\varepsilon u_t = \varepsilon \Delta u - \frac{1}{\varepsilon}(u^3 - u). \tag{30}$$

We can write this as $\varepsilon^{1/2} u_t = -\varepsilon^{-1/2} \nabla E$. If Ω is bounded and convex then $u \equiv +1$ and $u \equiv -1$ are the only stable local minima of E [10].

The modeling of thermal fluctuation in this setting is a bit subtle. The analogue of (26) is a stochastic partial differential equation obtained by adding noise to the right hand side of (30). There is no problem if the noise is smooth enough in space. But for modeling thermal fluctuation the noise should be white in space as well as time. The interpretation of such stochastic PDE's and the development of an associated large deviation theory is only complete in space dimension one [28], [31].

Never mind. Action minimization is a deterministic variational problem. It is known to give the pathways and timescales of thermally-activated transitions for the Ginzburg–Landau energy (29) when Ω is one-dimensional. And it seems likely that the same is true when Ω is multidimensional.

Thus we are interested in the minimization of $\int_0^T \int_\Omega |\varepsilon^{1/2} u_t + \varepsilon^{-1/2} \nabla E|^2 \, dx \, dt$. With less shorthand: we are interested in the limiting behavior of

$$\min_{\substack{u \equiv -1 \text{ at } t=0 \\ u \equiv +1 \text{ at } t=T}} \frac{1}{4} \int_0^T \int_\Omega \left| \varepsilon^{1/2} u_t - \varepsilon^{-1/2} (\varepsilon \Delta u - \varepsilon^{-1} (u^3 - u)) \right|^2 dx \, dt \tag{31}$$

as $\varepsilon \to 0$. For simplicity we focus on the case when the domain Ω is a cube in $\mathbb{R}^n$ with periodic boundary conditions.

In one space dimension the answer was found numerically and formally in [24] (see also [29]) and proved in [43]. The optimal pathway is shown schematically in Figure 6. Starting from $u = -1$, it begins by nucleating N equispaced seeds of the $u = 1$ phase (creating $2N$ interfaces). The seeds then grow at constant velocity,

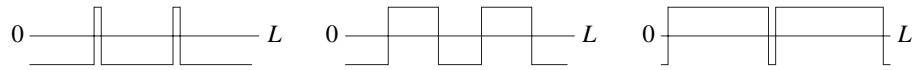


Figure 6. The action-minimizing path for $1D$ Ginzburg–Landau, if the optimal number of seeds is $N = 2$. The configuration is shown at $t = \delta$, $t = T/2$, and $t = T - \delta$.

colliding at exactly time T, leaving the entire interval filled with the $u = 1$ phase. The associated action is

$$\min_{N \geq 1} \left\{ 2N c_0 + \frac{L^2}{9NTc_0} \right\} \tag{32}$$

where N is the number of seeds, $c_0 = 2\sqrt{2}/3$ is the energy of an interface, and L is the length of the interval. The first term in (32) is the cost of nucleating $2N$ interfaces; the second is the cost of their constant-velocity motion.

In two space dimensions the problem has been studied numerically in [24] and analytically in [42], but a complete analysis is still lacking. The anticipated answer is similar to the one-dimensional case, except that (i) if the seeds are points rather than lines then their nucleation cost is negligible; and (ii) if a boundary moves via motion by mean curvature then its propagation cost is negligible. The analogue of (32) is thus

$$\min_{\text{pathways}} \left[(\text{nucleation cost, if any}) + \int_0^T \int (v_{\text{nor}} + \kappa)^2 \right]$$

where v_{nor} is the normal velocity of the moving phase boundary and κ is its curvature. A candidate pathway involving two seeds is shown in Figure 7.

Figure 7. A candidate pathway for $2D$ Ginzburg–Landau, if the optimal number of seeds is $N = 2$. The configuration is shown at $t = \delta$, $t = T/2$, and $t = T - \delta$.

To give a flavor of the analysis, we show under two simplifying assumptions that in one space dimension (with periodic boundary conditions) the action can be no smaller than (32).

Assumption 1. *All interfaces are created at* $t = 0$ *and all annihilations occur at* $t = T$.

Assumption 2. *The energy is "equipartitioned," i.e.*

$$\int_0^L \frac{\varepsilon}{2} u_x^2 \, dx = \int_0^L \frac{1}{4\varepsilon} (u^2 - 1)^2 \, dx = \frac{1}{2} E$$

at each time $0 < t < T$.

If one accepts these, the argument is elementary:

Step 1. If N nuclei form at time 0 (creating $2N$ interfaces), then an application of (28) with $\tau = \delta > 0$ gives

$$\frac{1}{4} \int_0^\delta \int_0^L \left| \varepsilon^{1/2} u_t + \varepsilon^{-1/2} \nabla E \right|^2 \, dx \, dt \geq E(\delta) - E(0) \geq 2N c_0.$$

This accounts for the first term in (32) (the "nucleation cost"). In the rest of argument, we shall show that the remaining action

$$\frac{1}{4} \int_\delta^{T-\delta} \int_0^L \left| \varepsilon^{1/2} u_t + \varepsilon^{-1/2} \nabla E \right|^2 \, dx \, dt$$

is bounded below by the second term in (32) (the "propagation cost").

Step 2. Since no interfaces are created or annihilated at intermediate times (Assumption 2), we have

$$\frac{1}{4}\int_\delta^{T-\delta}\int_0^L \varepsilon u_t^2\,dx\,dt \le \frac{1}{4}\int_\delta^{T-\delta}\int_0^L \varepsilon u_t^2 + \varepsilon^{-1}|\nabla E|^2\,dx\,dt$$
$$= \frac{1}{4}\int_\delta^{T-\delta}\int_0^L \left|\varepsilon^{1/2}u_t + \varepsilon^{-1/2}\nabla E\right|^2\,dx\,dt.$$

Step 3. If N nuclei form (creating $2N$ interfaces), then from Assumptions 1 and 2 we get

$$\int_\delta^{T-\delta}\int_0^L \varepsilon^{-1}(1-u^2)^2\,dx\,dt = \int_\delta^{T-\delta} 2E\,dt = 4c_0N(T-2\delta).$$

where c_0 is the energy of a wall.

Step 4. Using the end conditions $u \equiv -1$ at $t = 0$ and $u \equiv 1$ at $t = T$ we get

$$\int_\delta^{T-\delta}\int_0^L u_t(1-u^2)\,dx\,dt = \frac{4}{3}L + o(1)$$

where $o(1)$ indicates a term tending to 0 with δ. Now,

$$\int_\delta^{T-\delta}\int_0^L u_t(1-u^2)\,dx\,dt \le \left(\int_\delta^{T-\delta}\int_0^L \varepsilon u_t^2\right)^{1/2}\left(\int_\delta^{T-\delta}\int_0^L \varepsilon^{-1}(1-u^2)^2\right)^{1/2}.$$

Step 5. Combining Steps 2, 3, and 4, we find that

$$\liminf_{\delta\to 0}\frac{1}{4}\int_\delta^{T-\delta}\int_0^L \left|\varepsilon^{1/2}u_t + \varepsilon^{-1/2}\nabla E\right|^2 \ge \frac{1}{4}\frac{(4L/3)^2}{4c_0NT} = \frac{L^2}{9c_0NT}.$$

This is the desired bound on the propagation cost.

The rigorous proof in [43] is a bit different. It does not start by demonstrating our two assumptions; rather, their validity becomes clear in the course of the argument. Interestingly, the analysis shares many elements with work on the $\varepsilon \to 0$ limit of the Allen–Cahn equation [35], [61]. The multidimensional problem is also closely related to a conjecture of DeGiorgi concerning the sharp-interface limits of variational problems like

$$\int_\Omega |\nabla E|^2\,dx = \int_\Omega \left|\varepsilon\Delta u - \frac{1}{\varepsilon}(u^3-u)\right|^2 dx;$$

for recent progress on this topic see [47], [49], [58].

We have focused on the singular limit $\varepsilon \to 0$, but there are many other issues in the analysis of thermally-activated transitions. As $T \to \infty$ the pathways go through

mountain passes (saddle points). Surprisingly, though the "mountain pass lemma" has been used by analysts for decades, methods for finding saddle points and transition pathways numerically in high-dimensional systems have mainly been developed by chemists and physicists rather than mathematicians. This is beginning to change; in particular, the "string method" introduced by E, Ren, and Vanden-Eijnden represents an important algorithmic development [22], [23], [25], [26], [53].

References

[1] Alouges F., Rivière, T., Serfaty, S., Néel and cross-tie wall energies for planar magnetic configurations. *ESAIM Control Optim. Calc. Var.* **8** (2002), 31–68.

[2] Ambrosio, L., De Lellis C., Mantegazza, C., Line energies for gradient vector fields in the plane. *Calc. Var. PDE*, **9** (1999), 327–355.

[3] Ambrosio, L., Lecumberry, M., Rivière, T., A viscosity property of minimizing micromagnetic configurations. *Comm. Pure Appl. Math.* **56** (2003), 681–688.

[4] Aviles, P., Giga, Y., A mathematical problem related to the physical theory of liquid crystal configurations. In *Miniconference on geometry and partial differential equations.* 2 (J. Hutchinson and L. Simon, eds.), Proc. Centre Math. Anal. Austral. Nat. Univ. 12, Australian National University, Centre for Mathematical Analysis, Canberra 1987, 1–16.

[5] Aviles, P., Giga, Y., The distance function and defect energy. *Proc. Roy. Soc. Edinburgh* **126A** (1996), 923–938.

[6] Aviles, P., Giga, Y., On lower semicontinuity of a defect obtained by a singular limit of the Ginzburg–Landau type energy for gradient fields. *Proc. Roy. Soc. Edinburgh* **129A** (1999) 1–17.

[7] Ben Belgacem, H., Conti, S., DeSimone, A., Müller, S., Energy scaling of compressed elastic films – three-dimensional elasticity and reduced theories. *Arch. Rational Mech. Anal.* **164** (2002), 1–37.

[8] Bhattacharya, K., *Microstructure of Martensite: Why it forms and how it gives rise to the shape-memory effect*. Oxford Series on Materials Modelling, Oxford University Press, Oxford 2003.

[9] Braides, A., Γ*-Convergence for Beginners*. Oxford University Press, Oxford 2002.

[10] Casten, R. G., Holland, C. J., Instability results for reaction diffusion equations with Neumann boundary conditions. *J. Differential Equations* **27** (1978), 266–273.

[11] Choksi, R., Scaling laws in microphase separation of diblock copolymers. *J. Nonlinear Sci.* **11** (2001), 223–236.

[12] Choksi, R., Kohn, R. V., Bounds on the micromagnetic energy of a uniaxial ferromagnet. *Comm. Pure Appl. Math.* **51** (1998), 259–289.

[13] Choksi, R., Kohn, R. V., Otto, F., Domain branching in uniaxial ferromagnets: a scaling law for the minimum energy. *Comm. Math. Phys.* **201** (1999), 61–79.

[14] Choksi, R., Kohn, R. V., Otto, F., Energy minimization and flux domain structure in the intermediate state of a type-I superconductor. *J. Nonlinear Sci.* **14** (2004), 119–171.

[15] Conti, S., Branched microstructures: scaling and asymptotic self-similarity. *Comm. Pure Appl. Math.* **53** (2000), 1448–1474.

[16] Conti, S., Niethammer, B., Otto, F., Coarsening rates in off-critical mixtures. *SIAM J. Math. Anal.* **37** (2006), 1732–1741.

[17] Conti, S., Theil, F., Single-slip elastoplastic microstructures. *Arch. Rational Mech. Anal.* **178** (2005), 125–148.

[18] DeLellis, C., Otto, F., Structure of entropy solutions to the eikonal equation. *J. Eur. Math. Soc.* **5** (2003), 107–145.

[19] DeSimone, A., Kohn, R. V., Müller, S., Otto, F., A compactness result in the gradient theory of phase transitions. *Proc. Roy. Soc. Edinburgh* **131A** (2001), 833–844.

[20] DeSimone, A., Kohn, R. V., Müller, S., Otto, F., Repulsive interaction of Néel walls, and the internal length scale of the cross–tie wall. *Multiscale Model. Simul.* **1** (2003), 57–104.

[21] DeSimone, A., Kohn, R. V., Müller, S., Otto, F., Recent analytical developments in micromagnetics. In *The Science of Hysteresis II: Physical Modeling, Micromagnetics, and Magnetization Dynamics* (G. Bertotti and I. Mayergoyz, eds.), Elsevier, 2006, 269–381.

[22] E, W., Ren, W., Vanden-Eijnden, E., String method for the study of rare events. *Phys. Rev. B* **66** (2002), 052301.

[23] E, W., Ren, W., Vanden-Eijnden, E., Energy landscape and thermally activated switching of submicron-size ferromagnetic elements. *J. Appl. Phys.* **93** (2003), 2275–2282.

[24] E, W., Ren, W., Vanden-Eijnden, E., Minimum action method for the study of rare events. *Comm. Pure Appl. Math* **57** (2004), 637–656.

[25] E, W., Ren, W., Vanden-Eijnden, E., Finite temperature string method for the study of rare events. *J. Chem. Phys.* **109B** (2005), 6688-6693.

[26] E, W., Ren, W., Vanden-Eijnden, E., Transition pathways in complex systems: Reaction coordinates, isocommittor surfaces, and transition tubes. *Chem. Phys. Lett.* **413** (2005), 242–247.

[27] Ercolani, N., Indik, R., Newell, A. C., Passot, T., The geometry of the phase diffusion equation. *J. Nonlinear Sci.* **10** (2000), 223–274.

[28] Faris, W. G., Jona-Lasinio, G., Large fluctuations for a nonlinear heat equation with noise. *J. Phys. A: Math. Gen.* **15** (1982), 3025–3055.

[29] Fogedby, H. C., Hertz, J., Svane, A., Domain wall propagation and nucleation in a two-level system. *Phys. Rev. E* **70** (2004), 031105.

[30] Freidlin, M. L., Wentzell, A. D., *Random Perturbations of Dynamical Systems*. Second edition, Grundlehren Math. Wiss. 260, Springer-Verlag, New York 1998.

[31] Funaki, T., The scaling limit for a stochastic PDE and the separation of phases. *Probab. Theory Related Fields* **102** (1995), 221–288.

[32] Gardiner, C. W., *Handbook of Stochastic Methods for Physics, Chemistry, and the Natural Sciences*. Third edition, Springer Ser. Synergetics 13, Springer-Verlag, Berlin 2004.

[33] Hubert, A., Zur Theorie der zweiphasigen Domänenstrukturen in Supraleitern und Ferromagneten. *Phys. Stat. Solidi* **24** (1967), 669–682.

[34] Hubert, A., R. Schäfer, R., *Magnetic Domains: The Analysis of Magnetic Microstructures*. Springer-Verlag, 1998.

[35] Hutchinson, J., Tonegawa, Y., Convergence of phase interfaces in the van der Waals-Cahn-Hilliard theory. *Calc. Var. PDE* **10** (2000), 49–84.

[36] Jabin, P. E., Perthame, B., Compactness in Ginzburg-Landau energy by kinetic averaging. *Comm. Pure Appl. Math.* **54** (2001), 1096–1109.

[37] Jabin, P. E., Perthame, B., Otto, F., Line-energy Ginzburg-Landau models: zero-energy states. *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **1** (2002), 187–202.

[38] Jin, W., Kohn, R. V., Singular perturbation and the energy of folds. *J. Nonlinear Sci.* **10** (2000), 355–390.

[39] Kohn, R. V., Müller, S., Branching of twins near an austenite-twinned-martensite interface. *Phil. Mag. A* **66** (1992), 697–715.

[40] Kohn, R. V., Müller, S., Surface energy and microstructure in coherent phase transitions. *Comm. Pure Appl. Math.* **47** (1994), 405–435.

[41] Kohn, R. V., Otto, F., Upper bounds on coarsening rates. *Comm. Math. Phys.* **229** (2002), 375–395.

[42] Kohn, R. V., Otto, F., Reznikoff, M. G., Vanden-Eijnden, E., Action minimization and sharp-interface limits for the stochastic Allen-Cahn equation *Comm. Pure Appl. Math.* **60** (2007), 393–438.

[43] Kohn, R. V., Reznikoff, M.G., Tonegawa, Y., The sharp-interface limit of the action functional for Allen-Cahn in one space dimension. *Calc. Var. PDE* **25** (2006), 503–534.

[44] Kohn, R. V., Yan, X., Coarsening rates for models of multicomponent phase separation. *Interfaces Free Bound.* **6** (2004) 135–149.

[45] Lecumberry, M., Rivière, T., Regularity for micromagnetic configurations having zero jump energy. *Calc. Var. PDE* **15** (2002) 389–402.

[46] Modica, L., Mortola, S., Un esempio di Γ-convergenza. *Boll. Un. Mat. Ital.* **14** (1977), 285–299.

[47] Moser, R., A higher-order asymptotic problem related to phase transitions. *SIAM J. Math. Anal.* **37** (2005) 712–736.

[48] Müller, S., Singular perturbation as a selection mechanism for periodic minimizing sequences. *Calc. Var. PDE* **1** (1993), 169–204.

[49] Nagase, Y., Tonegawa, Y., A singular perturbation problem with integral curvature bound. Preprint.

[50] Nakatani, Y., Uesaka, Y., Hayashi, N., Direct solution for the Landau-Lifshitz-Gilbert equation for micromagnetics. *Japan J. Appl. Phys.* **28** (1989), 2485–2507.

[51] Otto, F., Cross-over in scaling laws: a simple example from micromagnetics. *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. III, Higher Ed. Press, Beijing 2002, 829–838.

[52] Privorotskii, I. *Thermodynamics of Domain Structures*. John Wiley & Sons, 1976.

[53] Ren, W., Higher order string method for finding minimum energy paths. *Comm. Math. Sci.* **1** (2003), 377–384.

[54] Ren, X., Truskinovsky, L., Finite scale microstructures in nonlocal elasticity. *J. Elasticity* **59** (2000), 319–355.

[55] Ren, X., Wei, J., On energy minimizers of the diblock copolymer problem. *Interfaces Free Bound.* **5** (2003), 193–238.

[56] Rivière, T., Serfaty, S., Limiting domain wall energy for a problem related to micromagnetics. *Comm. Pure Appl. Math.* **54** (2001), 294–338.

[57] Rivière, T., Serfaty, S., Compactness, kinetic formulation, and entropies for a problem related to micromagnetics, *Comm. Partial Differential Equations* **28** (2003), 249–269.

[58] Röger, M., Schätzle, R., On a modified conjecture of DeGiorgi. Preprint.

[59] Sandier, E., Serfaty, S., *Vortices in the Magnetic Ginzburg–Landau Model*. Progr. Nonlinear Differential Equations Appl. 70, Birkhäuser, Boston 2007.

[60] Serfaty, S., personal communication.

[61] Tonegawa, Y., Phase field model with a variable chemical potential. *Proc. Roy. Soc. Edinburgh* **132A** (2002), 993–1019.

[62] Truskinovsky, L., Zanzotto, G., Ericksen's bar revisited: energy wiggles. *J. Mech. Phys. Solids* **44** (1996), 1371–1408.

[63] van den Berg, H. A. M. Self–consistent domain theory in soft–ferromagnetic media. II. Basic domain structures in thin film objects. *J. Appl. Phys.* **60** (1986), 1104–1113.

[64] Yip, N. K., Structure of stable solutions of a one-dimensional variational problem. *ESAIM Control Optim. Calc. Var.* **12** (2006), 721–751.

Courant Institute, NYU, 251 Mercer Street, New York, NY 10012, U.S.A.
E-mail: kohn@cims.nyu.edu

Moduli spaces from a topological viewpoint

Ib Madsen

Abstract. This text aims to explain what topology, at present, has to say about a few of the many moduli spaces that are currently under study in mathematics.

The most prominent one is the moduli space $\mathcal{M}_g$ of all Riemann surfaces of genus g. Other examples include the Gromov–Witten moduli space of pseudo-holomorphic curves in a symplectic background, the moduli space of graphs and Waldhausen's algebraic K-theory of spaces.

Mathematics Subject Classification (2000). 19D55, 32G15, 55P42, 57N70.

Keywords. Moduli spaces, mapping class groups, cobordism, algebraic K-theory of spaces.

Introduction

The classical Riemann moduli space $\mathcal{M}_g$ is a $(6g-6)$-dimensional manifold with mild singularities (an orbifold). One would like to characterize its homotopy type, but in reality one must settle for less. Even the rational cohomology ring of $\mathcal{M}_g$ appears to be far too difficult; it is known today only for $g \leq 4$.

The central theme of the article revolves around Mumford's standard conjecture about the stable cohomology of $\mathcal{M}_g$, settled in my joint work with Michael Weiss a few years back [47]. The conjecture predicts the rational cohomology groups of $\mathcal{M}_g$ in a modest range of dimensions, the stable range. More accurately, [47] proves a generalized version of Mumford's conjecture, proposed in [46]: the (integral) cohomology ring of the (infinite genus) mapping class group is equal to the cohomology ring of a rather well-studied space in algebraic topology, a space associated with cobordism theory. From this Mumford's conjectured answer for the stable rational cohomology of $\mathcal{M}_g$ is easily deduced.

The new topological method in the study of the Riemann moduli space, presented below, has three key ingredients: Harer's stability theorem resulting from the action of mapping class groups on complexes of curves, Phillips' submersion theorem in singularity theory and Gromov's generalization thereof, and not least the Pontryagin–Thom theory of cobordisms of smooth manifolds. These tools are all rather old, known for at least twenty years, and one may wonder why they have not before been put to use in connection with the Riemann moduli space. Maybe we lacked the inspiration that comes from the renewed interaction with physics, exemplified in conformal field theories.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

1. Spaces of surfaces

1.1. Moduli and mapping classes. Fix a closed smooth and oriented surface F of genus g. One way to define the moduli space $\mathcal{M}_g$ is to start with the set of almost complex structures on F, compatible with the orientation. Such a structure is a fibrewise map $J: TF \to TF$ of the tangent bundle with $J^2 = -\mathrm{id}$ and with the property that $\{v, Jv\}$ is an oriented basis for each non-zero tangent vector v. The map J can be thought of as a section of the fibre bundle associated to TF with fibre $\mathrm{GL}_2^+(\mathbb{R})/\mathrm{GL}_1(\mathbb{C})$. We topologize this section space by the C^∞ Whitney topology and denote it $\mathcal{S}_{\mathbb{C}}(TF)$. The group $\mathrm{Diff}(F)$ of orientation preserving diffeomorphisms of F acts on $\mathcal{S}_{\mathbb{C}}(TF)$. The orbit space is the moduli space

$$\mathcal{M}_g = \mathcal{M}(F) = \mathcal{S}_{\mathbb{C}}(TF)/\mathrm{Diff}(F).$$

By a theorem of Gauss, $\mathcal{S}_{\mathbb{C}}(TF)$ is equal to the set of maximal holomorphic atlasses on F that respect the orientation: elements of $\mathcal{S}_{\mathbb{C}}(TF)$ are Riemann surfaces with underlying manifold F.

The moduli space $\mathcal{M}_0$ is a single point by Riemann's mapping theorem, $\mathcal{M}_1 = \mathbb{R}^2$, so we can concentrate on $\mathcal{M}_g$ for $g \geq 2$, where the moduli space is not contractible. Any Riemann surface Σ of genus $g \geq 2$ is covered by the upper half plane $H \subset \mathbb{C}$, so it is a holomorphic space form $\Sigma = H/\Gamma$ with Γ a cocompact torsion free subgroup of the group $\mathrm{PSL}_2(\mathbb{R})$ of all Möbius transformations of H. $\mathrm{PSL}_2(\mathbb{R})$ is also the group of all isometries of H in its standard hyperbolic metric $ds^2 = |dz|^2/y^2$, so Σ is a hyperbolic space form as well, and $\mathcal{S}_{\mathbb{C}}(TF)$ could be replaced with the space of hyperbolic metrics in the definition of $\mathcal{M}_g$, $g \geq 2$.

The connected component $\mathrm{Diff}_1(F)$ of the identity acts freely on $\mathcal{S}_{\mathbb{C}}(TF)$ by an easy fact from hyperbolic geometry. The associated orbit space

$$\mathcal{T}_g = \mathcal{T}(F) = \mathcal{S}_{\mathbb{C}}(TF)/\mathrm{Diff}_1(F)$$

is the Teichmüller space. It is homeomorphic to $\mathbb{R}^{6g-6}$. The rest of the $\mathrm{Diff}(F)$ action on $\mathcal{S}_{\mathbb{C}}(TF)$ is the action of the mapping class group,

$$\Gamma_g = \Gamma(F) = \pi_0 \mathrm{Diff}(F),$$

on $\mathcal{T}_g$. It acts discontinuously with finite isotropy groups, so $\mathcal{M}_g = \mathcal{T}_g/\Gamma_g$ is a $(6g-6)$-dimensional orbifold. Had the action been free, then $\mathcal{M}_g$ would have been homotopy equivalent to the space $B\Gamma_g$, classifying Γ_g-covering spaces. As it is, there is a map from $B\Gamma_g$ to $\mathcal{M}_g$ that induces isomorphisms

$$H^*(\mathcal{M}_g; \mathbb{Q}) \xrightarrow{\cong} H^*(B\Gamma_g; \mathbb{Q}) \tag{1.1}$$

on rational cohomology.

Because $\mathcal{S}_{\mathbb{C}}(TF)$ is the space of sections in a fibre bundle with contractible fibre $\mathrm{GL}_2^+(\mathbb{R})/\mathrm{GL}_1(\mathbb{C})$, it is itself contractible. Earle and Eells [15] proved that the orbit

map of the $\mathrm{Diff}_1(F)$ action,

$$\pi : \mathcal{S}_{\mathbb{C}}(TF) \to \mathcal{T}(F)$$

locally has a section, so that π is a fibre bundle. The total space and the base space both being contractible, they concluded that $\mathrm{Diff}_1(F)$ (and hence any other connected component of $\mathrm{Diff}(F)$) is contractible. This gives the homotopy equivalence

$$B\,\mathrm{Diff}(F) \xrightarrow{\simeq} B\Gamma(F) \tag{1.2}$$

of classifying spaces; cf. §2.1 below for a general discussion of classifying spaces.

The model of $B\,\mathrm{Diff}(F)$ that we use is the space of all oriented surfaces of euclidean space (of arbitrary dimension) that are diffeomorphic to F. This is equal to the orbit space

$$\mathrm{Emb}(F, \mathbb{R}^\infty)/\,\mathrm{Diff}(F)$$

of the free $\mathrm{Diff}(F)$ action on the space of smooth embeddings of F in infinite dimensional euclidean space. The embedding space is contractible [80] and the orbit map is a fibre bundle. This implies the homotopy equivalence

$$\mathrm{Emb}(F, \mathbb{R}^\infty)/\,\mathrm{Diff}(F) \simeq B\,\mathrm{Diff}(F).$$

Each surface in euclidean space inherits a Riemannian metric from the surroundings, which together with the orientation defines, a complex structure. This leads to a concrete map

$$\mathrm{Emb}(F, \mathbb{R}^\infty)/\,\mathrm{Diff}(F) \to \mathcal{M}(F)$$

that induces isomorphism on rational cohomology.

1.2. Stability and Mumford's standard conjecture. Ideally, one would like to compute the rational cohomology ring of each individual $\mathcal{M}_g$. This has been done for $g \le 4$ in [44], [72], but seems too ambitious for larger genus. Following Mumford [57], one should instead attempt a partial calculation of $H^*(\mathcal{M}_g)$, namely in a certain stable range. For $g \ge 2$, Mumford defined tautological classes in the rational Chow ring of the Deligne–Mumford compactification $\overline{\mathcal{M}}_g$, and proposed that their images in $H^*(\mathcal{M}_g; \mathbb{Q})$ freely generate the entire rational cohomology ring as $g \to \infty$. The proposal is similar in spirit to what happens for the Grassmannian of d-dimensional linear subspaces of $\mathbb{C}^n$; as $n \to \infty$, the cohomology becomes a polynomial algebra in the Chern classes of the tautological d-dimensional vector bundle. See also [28], [41].

More precisely, Mumford predicted that, in a range of dimensions that tends to infinity with g, the cohomology ring $H^*(\mathcal{M}_g; \mathbb{Q})$ is isomorphic with the polynomial algebra $\mathbb{Q}[\kappa_1, \kappa_2, \ldots]$ in the tautological classes κ_i of degree $2i$.

Miller [52] and Morita [56] used topological methods to define integral cohomology classes in $B\Gamma_g$ that agree with Mumford's classes under the isomorphism (1.1). I recall the definition. Choose a point $p \in F$ and consider the subgroup $\mathrm{Diff}(F;\, p)$ of orientation-preserving diffeomorphisms that fixes p. It has contractible components [16] and mapping class group $\Gamma_g^1 = \pi_0 \mathrm{Diff}(F;\, p)$. In the diagram

$$\begin{array}{ccccc} B\,\mathrm{Diff}(F;\, p) & \longrightarrow & B\Gamma_g^1 & \longrightarrow & \mathcal{M}_g^1 \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ B\,\mathrm{Diff}(F) & \longrightarrow & B\Gamma_g & \longrightarrow & \mathcal{M}_g, \end{array}$$

the left-hand horizontal maps are homotopy equivalences and the right-hand ones are rational cohomology isomorphisms. The right-hand vertical map is the "universal curve"; the left-hand π is (homotopic to) a smooth fibre bundle with fibre F and oriented relative tangent bundle $T\pi$. Morita defines

$$\kappa_i = (-1)^{i+1}\pi_!(c_1(T\pi)^{i+1}) \in H^{2i}(B\Gamma_g;\, \mathbb{Z}), \tag{1.3}$$

where $\pi_!$ is the Gysin (or integration along the fibres) homomorphism.

The "differential at p" gives a map from $\mathrm{Diff}(F;\, p)$ to $\mathrm{GL}_2^+(\mathbb{R})$, and the associated map

$$d\colon B\,\mathrm{Diff}(F;\, p) \to B\,\mathrm{GL}_2^+(\mathbb{R}) \simeq \mathbb{C}P^\infty$$

classifies $T\pi$. Its (homotopy theoretic) fibre is the classifying space of the group $\mathrm{Diff}(F;\, D(p))$ of orientation-preserving diffeomorphisms that fix the points of a small disc $D(p)$ around p. Let $\Gamma_{g,1} = \pi_0 \mathrm{Diff}(F;\, D(p))$ be its mapping class group so that we have the fibration

$$B\Gamma_{g,1} \xrightarrow{\pi} B\Gamma_g^1 \xrightarrow{d} \mathbb{C}P^\infty$$

to relate the cohomology of $B\Gamma_{g,1}$ and $B\Gamma_g^1$. Note that $\mathrm{Diff}(F,\, D(g)) = \mathrm{Diff}(F_{g,1};\, \partial)$, where $F_{g,1} = F - \mathrm{int}\, D(p)$ is a genus g surface with one boundary circle. Since $F_{g+1,1}$ is the union of $F_{g,1}$ with a torus $F_{1,2}$ with two boundary circles, there is a map $\Gamma_{g,1} \to \Gamma_{g+1,1}$. Forgetting $D(p) \subset F$ (or filling out the hole in $F_{g,1}$) gives a map $\Gamma_{g,1} \to \Gamma_g$. The following theorem [27] with an improvement from [38] is of crucial importance to us. This is Harer's stability theorem.

Theorem 1.1 ([27], [38]). *The induced maps*

$$H_k(B\Gamma_{g,1};\, \mathbb{Z}) \to H_k(B\Gamma_{g+1,1};\, \mathbb{Z}) \quad \textit{and} \quad H_k(B\Gamma_{g,1};\, \mathbb{Z}) \to H_k(B\Gamma_g;\, \mathbb{Z})$$

are isomorphisms when $2k < g - 1$.

The stable mapping class group $\Gamma_{\infty,1}$ is the direct limit of the groups $\Gamma_{g,1}$ as $g \to \infty$. By the theorem,

$$H^k(B\Gamma_{\infty,1}; \mathbb{Z}) \cong H^k(B\Gamma_g; \mathbb{Z})$$

when $2k < g - 1$. Miller and Morita proved in [52] and [56] that $H^*(B\Gamma_{\infty,1}; \mathbb{Q})$ contains the polynomial algebra $\mathbb{Q}[\kappa_1, \kappa_2, \ldots]$.

Let $\mathbb{C}P^n$ denote the complex projective n-space, and let $L_n^\perp \subset \mathbb{C}P^n \times \mathbb{C}^{n+1}$ be the subspace of pairs (l, v) with v orthogonal to l. Consider the space $MT(n)$ of all proper maps from $\mathbb{C}^{n+1}$ to $L_n^\perp$. The cohomology groups $H^k(MT(n); \mathbb{Z})$ are independent of n for $k < 2n$. One form of the generalized Mumford conjecture is the statement

Theorem 1.2 ([47]). *For $k < 2n$ there is an isomorphism*

$$H^k(B\Gamma_{\infty,1}; \mathbb{Z}) \cong H^k(MT(n); \mathbb{Z}).$$

Corollary 1.3 ([47]). *The rational cohomology ring of $B\Gamma_{\infty,1}$ is a polynomial algebra in the classes $\kappa_1, \kappa_2, \ldots$.*

In view of (1.1), this also calculates $H^*(\mathcal{M}_g; \mathbb{Q})$ for a range of dimensions, and affirms Mumford's conjecture.

The stability theorem from [27], [38] is more general than stated above. Let $F_{g,b}^s$ be a surface of genus g with $b \geq 0$ boundary circles and s distinct points in the interior, and let $\Gamma_{g,b}^s$ be the associated mapping class group.

Addendum 1.4. For $b > 0$, the maps

$$B\Gamma_{g,b-1}^s \leftarrow B\Gamma_{g,b}^s \to B\Gamma_{g+1,b}^s$$

induce isomorphisms in integral cohomology in degrees less than $(g - 1)/2$.

The addendum implies that $H^*(B\Gamma_{\infty,b}^s; \mathbb{Z})$ is independent of the number of boundary circles. Consequently, we sometimes drop the subscript b from the notation and write Γ_∞^s instead of $\Gamma_{\infty,b}^s$. In the diagram

$$\begin{array}{ccccc} B\Gamma_{g,b+s} & \longrightarrow & B\Gamma_{g,b}^s & \xrightarrow{d} & \prod^s \mathbb{C}P^\infty \\ & \searrow & \downarrow & & \\ & & B\Gamma_{g,b}\,, & & \end{array}$$

the skew map is a cohomology isomorphism in the stability range, so

$$H^*(B\Gamma_{\infty,b}^s; \mathbb{Z}) = H^*(B\Gamma_{\infty,1}; \mathbb{Z}) \otimes \mathbb{Z}[\psi_1, \ldots, \psi_s] \tag{1.4}$$

with $\deg \psi_i = 2$. See also [6].

2. Cobordism categories and their spaces

In this section we explain work of S. Galatius, U. Tillmann, M. Weiss and the author in various combinations. The most relevant references are [22], [23], [46], [47]. The section contains, in outline, a proof of the generalized Mumford conjecture, different from the original one, but still based on concepts and results from [47].

2.1. The classifying space of a category. In [53], Milnor associated to each topological group G a space BG by a functorial construction, characterized up to homotopy by being the base of a principal G-bundle with contractible total space. Moreover, isomorphim classes of principal G-bundles with base X are in one to one correspondence with homotopy classes of maps from X to BG.

The space $B\mathcal{C}$ associated to a (small) category $\mathcal{C}$ is a similar construction [64]. The objects of $\mathcal{C}$ are the vertices in a simplicial set. Two objects span a 1-simplex if there is a morphism between them. A k-simplex corresponds to k composable arrows of $\mathcal{C}$. Formally, let $N_k\mathcal{C}$ be the set of k-tuples of morphisms,

$$c_0 \xrightarrow{f_1} c_1 \xrightarrow{f_2} c_2 \longrightarrow \cdots \xrightarrow{f_k} c_k,$$

and define face operators

$$d_i \colon N_k\mathcal{C} \to N_{k-1}\mathcal{C}, \quad i = 0, 1, \ldots, k$$

by removing c_i (and composing f_i and f_{i+1} when $i \neq 0, k$). Then

$$B\mathcal{C} = \coprod_{k=0}^{\infty} \Delta^k \times N_k\mathcal{C} \big/ (d^i t,\, f) \equiv (t, d_i f) \tag{2.1}$$

with $t \in \Delta^{k-1}$ and $f \in N_k\mathcal{C}$. Here Δ^k is the standard euclidean k-simplex and $d^i \colon \Delta^{k-1} \to \Delta^k$ the inclusion as the i'th face.

The categories we use below are *topological* categories. This means that the total set of objects and the total set of morphisms have topologies, and that the structure maps (source, target and composition) are continuous. In this case $N_k\mathcal{C}$ is a space and d_i is continuous. I refer to [79] for a discussion of the kind of objects that $B\mathcal{C}$ actually classifies.

A topological category M with a single object is precisely a topological monoid. In this case, the 1-skeleton in (2.1) gives a map from $\Delta^1 \times M$ into BM, or equivalently a map from M into the loop space ΩBM. It takes the monoid $\pi_0 M$ of connected components into the fundamental group $\pi_1 BM$. If $\pi_0 M$ is a group then $M \to \Omega BM$ turns out to be a homotopy equivalence. More generally, we have the group completion theorem that goes back to Quillen's work in K-theory. The composition law in M yields a ring structure on $H_*(M)$, and we have

Theorem 2.1 ([4], [51]). *Suppose that $\pi_0 M$ is central in $H_*(M)$. Then*

$$H_*(M)[\pi_0 M^{-1}] \xrightarrow{\cong} H_*(\Omega B M)$$

is an isomorphism.

In typical applications of Theorem 2.1, $\pi_0 M = \mathbb{N}$ and the left-hand side has the following interpretation. Let $m \in M$ represent $1 \in \pi_0 M$ and define M_∞ to be the direct limit of $M \xrightarrow{m} M \xrightarrow{m} M \xrightarrow{m} \cdots$. Then $H_*(M)[\pi_0 M^{-1}]$ is the homology of $\mathbb{Z} \times M_\infty$.

Remark 2.2. In general, the direct limit (or colimit) of a string of spaces $f_i \colon X_i \to X_{i+1}$ does not commute with homology, unless the maps f_i are closed injections. When this is not the case, the colimit should be replaced with the homotopy colimit (or telescope) of [54]. This construction always commutes with homology. The right definition of M_∞ is therefore

$$M_\infty = \operatorname{hocolim}(M \xrightarrow{m} M \xrightarrow{m} M \xrightarrow{m} \cdots).$$

Alternatively, we can apply Quillen's plus-construction [5] to M_∞ to get a homotopy equivalence

$$\mathbb{Z} \times M_\infty^+ \xrightarrow{\simeq} \Omega B M. \tag{2.2}$$

This applies to the monoids $M = \bigsqcup B\Sigma_n$, $\bigsqcup B\,\mathrm{GL}_n(R)$ or $\bigsqcup B\Gamma_{g,2}$ where the composition law is induced from the direct sum of permutations and matrices and, in the case of the mapping class group, from gluing along one boundary circle. There are homotopy equivalences

$$\begin{aligned} \mathbb{Z} \times B\Sigma_\infty^+ &\xrightarrow{\simeq} \Omega B\big(\textstyle\bigsqcup B\Sigma_n\big), \\ \mathbb{Z} \times B\,\mathrm{GL}_\infty(R)^+ &\xrightarrow{\simeq} \Omega B\big(\textstyle\bigsqcup B\,\mathrm{GL}_n(R)\big), \\ \mathbb{Z} \times B\Gamma_{\infty,2}^+ &\xrightarrow{\simeq} \Omega B\big(\textstyle\bigsqcup B\Gamma_{n,2}\big). \end{aligned} \tag{2.3}$$

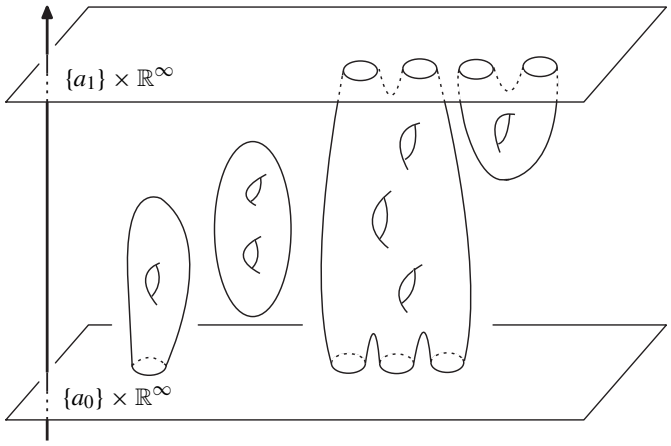
The effect of the plus-construction is quite dramatic. While it leaves homology groups unchanged, it produces extra homotopy groups. The spaces $B\Sigma_\infty$, $B\,\mathrm{GL}_\infty(R)$, and $B\Gamma_{\infty,2}$ have vanishing homotopy groups past the fundamental group, but their plus-constructions have very interesting homotopy groups: $\pi_i B\Sigma_\infty^+$ is the i'th stable homotopy group of spheres, and $\pi_i B\,\mathrm{GL}_\infty(R)^+$ is Quillen's higher K-group $K_i(R)$ [61], [62].

2.2. Riemann's surface category and generalizations. The Riemann surface category $\mathcal{S}$ has attracted attention with G. Segal's treatment of conformal field theories [65], [66]. It is the category with one object C_m for each non-negative integer m, namely the disjoint union of m parametrized circles. A morphism from C_m to C_n

is a pair (Σ, φ), consisting of a Riemann surface Σ and an orientation-preserving diffeomorphism $\varphi\colon \partial\Sigma \to (-C_m) \sqcup C_n$. (The topology on the set of morphisms is induced from the topology of the moduli spaces.)

As indicated at the end of §1.1, one may replace the moduli space $\mathcal{M}_g$ with the space of surfaces in euclidean space without changing the rational homology. For $\mathcal{M}_{g,b}$ with $b > 0$, the replacement does not even change the homotopy type. This leads to the category $\mathcal{C}_2$ of embedded surfaces. Once we go to embedded surfaces instead of Riemann surfaces, there are no added complications in generalizing from 2 dimensions to d dimensions. This leads to the category $\mathcal{C}_d$.

An object of $\mathcal{C}_d$ is a $(d-1)$-dimensional closed, oriented submanifold of $\{a\} \times \mathbb{R}^{n+d-1} \subset \mathbb{R}^{n+d}$ for some real number a and some large n. A morphism is a compact, oriented d-dimensional manifold W^d contained in a strip $[a_0, a_1] \times \mathbb{R}^{n+d-1}$ $(a_0 < a_1)$ such that $\partial W = (-\partial_0 W) \sqcup \partial_1 W$, where $\partial_i W = W \cap \{a_i\} \times \mathbb{R}^{n+d-1}$. For technical reasons, we require that W meets the walls $\{a_i\} \times \mathbb{R}^{n+d-1}$ orthogonally and that W is constant near the walls. Here is a schematic picture of W:



The number n is arbitrarily large, and not part of the structure. From now on, I often write $n = \infty$. A submanifold of $\mathbb{R}^{\infty+d-1}$ can be parametrized in the sense that it is the image of an embedding. Thus we have the identifications

$$N_0\mathcal{C}_d \cong \coprod_{\{M\},a} \operatorname{Emb}(M^{d-1}, \{a\} \times \mathbb{R}^{\infty+d-1}) / \operatorname{Diff}(M), \tag{2.4a}$$

$$N_1\mathcal{C}_d \cong \Big(\coprod_{\{W\},a_0<a_1} \operatorname{Emb}(W^d, [a_0, a_1] \times \mathbb{R}^{\infty+d-1}) / \operatorname{Diff}(W^d) \Big) \sqcup N_0\mathcal{C}_d. \tag{2.4b}$$

The disjoint unions vary over the set of diffeomorphism classes of smooth compact, oriented manifolds and over real numbers a, a_i. The embedding spaces are equipped with the "convenient topology", [42]; the action of the diffeomorphism groups is by composition. The quotient maps are principal fibre bundles [42], and the embedding

spaces are contractible, so the individual terms in (2.4) are homotopy equivalent to $B\,\mathrm{Diff}(M^{d-1})$ and $B\,\mathrm{Diff}(W^d) \sqcup B\,\mathrm{Diff}(M^{d-1})$, respectively. See also [46, §2].

The group of connected components $\pi_0 B\mathcal{C}_d$ is equal to the cobordism group Ω_{d-1} of oriented closed $(d-1)$-manifolds. This group has been tabulated for all d [78]. It vanishes for $d \leq 4$.

Proposition 2.3 ([22]). *The classifying space $B\mathcal{C}_2$ has the same rational homology as the classifying space $B\mathcal{S}$ of the Riemann surface category.*

2.3. Thom spaces and embedded cobordisms. The Thom space $\mathrm{Th}(\xi)$ (sometimes denoted X^ξ) of a vector bundle ξ on X is a construction that has been of fundamental importance in topology for more than fifty years. The homotopy theory of specific Thom spaces has helped solve many geometric problems. Early results can be found in [59], [60], [69], [70]. Our use of Thom spaces are not far from this original tradition. The modern development is described in [35].

For a vector bundle ξ over a compact base space, $\mathrm{Th}(\xi)$ is the one point compactification of its total space. Equivalently, it is the quotient of the projective bundle $P(\xi \oplus \mathbb{R})$ by $P(\xi)$.

Two geometric properties might help explain the usefulness of the construction. First, the complement $\mathrm{Th}(\xi) - X$ of the zero section is contractible so that $\mathrm{Th}(\xi)$ is a kind of homotopy theoretic localization of ξ near X. Second, if ξ is the normal bundle of a submanifold $X^m \subset \mathbb{R}^{m+k}$, then one has the Pontryagin–Thom collapse map,

$$c_X \colon S^{m+k} \longrightarrow \mathrm{Th}(\xi),$$

by considering ξ to be an open tubular neighborhood of X in $\mathbb{R}^{m+k}$.

On the algebraic side, we have the Thom isomorphism

$$H^i(X; \mathbb{Z}) \cong H^{i+k}(\mathrm{Th}(\xi); \mathbb{Z})$$

provided that ξ is an oriented vector bundle of dimension k.

Let $G(d, n)$ denote the Grassmannian of *oriented* d-dimensional linear subspaces of $\mathbb{R}^{d+n}$, and let

$$U_{d,n} = \{(V, v) \in G(d, n) \times \mathbb{R}^{d+n} \mid v \in V\},$$
$$U_{d,n}^\perp = \{(V, v) \in G(d, n) \times \mathbb{R}^{d+n} \mid v \perp V\}$$

be the two canonical vector bundles over it.

The restriction of $U_{d,n+1}^\perp$ to $G(d, n)$ is the product $\mathbb{R} \times U_{d,n}^\perp$. Its inclusion into $U_{d,n+1}^\perp$ is a proper map, so it induces a map $\varepsilon_{d,n}$ of one point compactifications from the suspension $\Sigma\,\mathrm{Th}(U_{d,n}^\perp)$ to $\mathrm{Th}(U_{d,n+1}^\perp)$.

At this point, it is convenient to introduce the concept of a prespectrum $E = \{E_n, \varepsilon_n\}$. It consists of a sequence of pointed spaces E_n for $n = 0, 1, \ldots$ together

with maps $\varepsilon_n\colon \Sigma E_n \to E_{n+1}$, where

$$\Sigma E_n = S^1 \times E_n/(* \times E_n \cup S^1 \times *).$$

The infinite loop space associated with E is defined to be

$$\Omega^\infty E = \operatorname{hocolim}(\cdots \to \Omega^n E_n \xrightarrow{\varepsilon'_n} \Omega^{n+1} E_{n+1} \to \cdots)$$

with ε'_n being the adjoint of ε_n. We shall also need its deloop $\Omega^{\infty-1}E$. This is the homotopy colimit of $\Omega^{n-1}E_n$.

The pairs $\{\mathrm{Th}(U^\perp_{d,n}), \varepsilon_{d,n}\}$ form the prespectrum $\mathbb{G}_{-d}$; its n'th space is $\mathrm{Th}(U^\perp_{d,n-d})$ if $n \geq d$ and otherwise a single point. The sphere prespectrum $\mathbb{S}$ has the n-sphere as its n'th space and ε_n is the canonical identification $\Sigma S^n = S^{n+1}$. The associated infinite loop spaces are

$$\Omega^\infty \mathbb{S} = \operatorname{hocolim} \Omega^n S^n, \quad \Omega^\infty \mathbb{G}_{-d} = \operatorname{hocolim} \Omega^{n+d} \mathrm{Th}(U^\perp_{d,n}).$$

In both cases, the inclusion of the n'th term into the limit space induces an isomorphism on homology groups in a range of dimensions that tends to infinity with n. The space $G(2,\infty)$ is homotopy equivalent to $\mathbb{C}P^\infty$, and $\mathbb{G}_{-2}$ becomes homotopy equivalent to the prespectrum $\mathbb{C}P^\infty_{-1}$. This has $(2n+2)$nd space equal to the Thom space $\mathrm{Th}(L^\perp_n)$ of the complement $L^\perp_n$ to the canonical line bundle over $\mathbb{C}P^n$. The associated infinite loop spaces are homotopy equivalent,

$$\Omega^\infty \mathbb{G}_{-2} \simeq \Omega^\infty \mathbb{C}P^\infty_{-1}. \tag{2.5}$$

Theorem 2.4 ([22]). *For $d \geq 0$, $B\mathcal{C}_d$ is homotopy equivalent to $\Omega^{\infty-1}\mathbb{G}_{-d}$.*

A few words of explanation are in order. Suppose that $W^d \subset [a_0, a_1] \times \mathbb{R}^{n+d-1}$ is a morphism of $\mathcal{C}_d$. For each $p \in W$, the tangent space T_pW is an element of $G(d,n)$ and the normal space at p is precisely the fibre of $U^\perp_{d,n}$ at T_pW. The Pontryagin–Thom collapse map

$$[a_0, a_1] \times (S^{n+d-1}, \infty) \to (\mathrm{Th}(U^\perp_{d,n}), \infty)$$

defines a path in $\Omega^{n+d-1}\mathrm{Th}(U^\perp_{d,n})$, and hence for $n \to \infty$, a path in $\Omega^{\infty-1}\mathbb{G}_{-d}$. More generally, an element of $N_k\mathcal{C}_d$ gives a set of k composable paths in $\Omega^{\infty-1}\mathbb{G}_{-d}$.

To any space X, one can associate the path category Path X. Its space of objects is $\mathbb{R} \times X$, and a morphism from (a_0, x_0) to (a_1, x_1) is a path $\gamma\colon [a_0, a_1] \to X$ from x_0 to x_1. The classifying space of Path X is homotopy equivalent to X, $B\,\mathrm{Path}\, X \simeq X$. In the situation above, this leads to a well-defined homotopy class

$$\beta_d\colon B\mathcal{C}_d \longrightarrow B(\mathrm{Path}\, \Omega^{\infty-1}\mathbb{G}_{-d}) \simeq \Omega^{\infty-1}\mathbb{G}_{-d},$$

and Theorem 2.4 is the statement that β_d is a homotopy equivalence.

I shall attempt to explain the strategy of proof of Theorem 2.4 by breaking it down into its three major parts.

Let $\mathcal{T}_d(\mathbb{R}^{n+d})$ be the space of oriented d-dimensional submanifolds $E^d \subset \mathbb{R}^{n+d}$ contained in a tube $\mathbb{R} \times D^{n+d-1}$ as a closed subset. Let $\mathcal{T}_d(\mathbb{R}^{\infty+d})$ be the union of these spaces.

We topologize $\mathcal{T}_d(\mathbb{R}^{n+d})$, not by the Whitney embedding topology used above, but by a coarser topology that allows manifolds to be pushed to infinity. The topology we want has the property that a map from a k-dimensional manifold X^k into $\mathcal{T}_d(\mathbb{R}^{n+d})$ produces a submanifold M^{k+d} of $X^k \times \mathbb{R} \times \mathbb{R}^{n+d-1}$, such that the projection onto $X \times \mathbb{R}$ is proper and the projection on X is a submersion (and not necessarily a fibre bundle).

There is a partially ordered set $\mathcal{D}_d$ associated with $\mathcal{T}_d(\mathbb{R}^{\infty+d})$. It consists of pairs (a, E) with $a \in \mathbb{R}$, $E \in \mathcal{T}_d(\mathbb{R}^{\infty+d})$, such that E intersects the wall $a \times \mathbb{R}^{\infty+d-1}$ orthogonally. The partial ordering is that $(a_0, E_0) \leq (a_1, E_1)$ if $a_0 \leq a_1$ and $E_0 = E_1$. A partially ordered set is a category with one arrow for each order relation $(a_0, E_0) \leq (a_1, E_1)$.

Three maps connect the spaces involved:

$$r\colon \mathcal{D}_d \to \mathcal{C}_d, \quad s\colon \mathcal{D}_d \to \mathcal{T}_d(\mathbb{R}^{\infty+d}), \quad t\colon \mathcal{T}_d(\mathbb{R}^{\infty+d}) \to \Omega^{\infty-1}\mathbb{G}_{-d}.$$

The map r intersects E^d with the wall $\{a\} \times \mathbb{R}^{\infty+d-1}$, and the morphism $(a_0, E) \leq (a_1, E)$ with the strip $[a_0, a_1] \times \mathbb{R}^{\infty+d-1}$; s forgets the first coordinate, and t is the Pontryagin–Thom collapse map. The proof is now to show that each of the induced maps

$$r\colon B\mathcal{D}_d \to B\mathcal{C}_d, \tag{2.6a}$$

$$s\colon B\mathcal{D}_d \to \mathcal{T}_d(\mathbb{R}^{\infty+d}), \tag{2.6b}$$

$$t\colon \mathcal{T}_d(\mathbb{R}^{\infty+d}) \to \Omega^{\infty-1}\mathbb{G}_{-d} \tag{2.6c}$$

are a homotopy equivalences. It suffices to check on homotopy groups, i.e. that $\pi_n(r)$, $\pi_n(s)$, and $\pi_n(t)$ are isomorphisms. This is done geometrically as in [47], by interpreting the homotopy groups of the given spaces as cobordism classes of families of the involved structures indexed by the sphere S^n.

It is (2.6c) that requires an h-principle from singularity theory. Given an element of $\pi_n(\Omega^{\infty-1}\mathbb{G}_{-d})$ one uses transversality together with Phillips' submersion theorem [58] to obtain a cobordism class of triples (E^{n+d}, π, f), where $\pi\colon E^{n+d} \to S^n$ is a submersion, and $f\colon E^{n+d} \to \mathbb{R}$ is a proper map. This represents an element of $\pi_n\mathcal{T}_d(\mathbb{R}^{\infty+d})$. Injectivity is proved by relative considerations.

Remark 2.5. The d-fold suspensions $\Sigma^d\mathbb{G}_{-d}$ fit together via maps $\Sigma^d\mathbb{G}_{-d} \to \Sigma^{d+1}\mathbb{G}_{-(d+1)}$. Their homotopy colimit is the prespectrum MSO whose homotopy groups are the cobordism groups Ω_*, by [70].

2.4. Consequences of Harer stability. For clarity, I begin with a discussion of abstract stability in a topological category $\mathcal{C}$, generalizing the group completion theorem.

Given a string of morphisms in $\mathcal{C}$,

$$b_1 \xrightarrow{\beta_1} b_2 \xrightarrow{\beta_2} b_3 \longrightarrow \cdots,$$

we have functors

$$F_i\colon \mathcal{C}^{\mathrm{op}} \to \text{spaces}; \quad F_\beta\colon C^{\mathrm{op}} \to \text{spaces}$$

with $F_i(c) = \mathcal{C}(c, b_i)$, the space of morphisms from c to b_i, and

$$F_\beta(c) = \operatorname{hocolim}(F_1(c) \xrightarrow{\beta_1} F_2(c) \xrightarrow{\beta_2} F_3(c) \longrightarrow \cdots).$$

Lemma 2.6. *Suppose $B\mathcal{C}$ is connected, and suppose for each morphism $c_1 \to c_2$ in $\mathcal{C}$ that $F_\beta(c_2) \to F_\beta(c_1)$ is an integral homology isomorphism. Then there is an integral homology isomorphism $F_\beta(c) \to \Omega B\mathcal{C}$ for each object c of $\mathcal{C}$.*

This follows from [51]: Consider the category $F_\beta \wr \mathcal{C}$. Its objects are pairs (x, c) with $x \in F_\beta(c)$, and it has the obvious morphisms. Its classifying space is contractible because it is the homotopy colimit of the contractible spaces $B(F_i \wr \mathcal{C})$[†]. The map $\pi\colon B(F_\beta \wr \mathcal{C}) \to B\mathcal{C}$ is a homology fibration. The fibre $\pi^{-1}(c) = F_\beta(c)$ is therefore homology equivalent to the homotopy fibre, which is $\Omega B\mathcal{C}$.

The condition of Lemma 2.6 is not satisfied for the embedded surface category $\mathcal{C}_2$ of §2.3, but it is satisfied for a certain subcategory $\mathcal{C}_2^{\mathrm{res}} \subset \mathcal{C}_2$, originally introduced in [71] for that very reason.

The restricted category $\mathcal{C}_d^{\mathrm{res}} \subset \mathcal{C}_d$ has the same space of objects but a restricted space of morphisms: A morphism $W^d \subset [a_0, a_1] \times \mathbb{R}^{\infty+d-1}$ of $\mathcal{C}_d$ belongs to $\mathcal{C}_d^{\mathrm{res}}$ if each connected component of W has a non-empty intersection with $\{a_1\} \times \mathbb{R}^{\infty+d-1}$.

Theorem 2.7 ([22]). *For $d > 1$, $B\mathcal{C}_d^{\mathrm{res}} \to B\mathcal{C}_d$ is a homotopy equivalence.*[‡]

The proof is, roughly speaking, to perform surgery (connected sum) on morphisms of $\mathcal{C}_d$ to replace them with morphisms from $\mathcal{C}_d^{\mathrm{res}}$.

Given Theorem 2.4 and Theorem 2.7, and using the notation (2.5), we can adopt Tillmann's argument [71] to prove the generalized Mumford conjecture,

Theorem 2.8 ([47]). *The space $\mathbb{Z} \times B\Gamma^+_{\infty,1}$ is homotopy equivalent to the space $\Omega^\infty \mathbb{C}P^\infty_{-1}$.*

We take $\mathcal{C} = \mathcal{C}_2^{\mathrm{res}}$ and b_i to be the object consisting of a standard circle in $\{i\} \times \mathbb{R}^{\infty+1}$. The morphism β_i is the torus $F_{1,2}$ with two boundary circles embedded in $[i, i+1] \times \mathbb{R}^{\infty+1}$ so that $\partial\beta_i = b_{i+1} \sqcup -b_i$. Then

$$F_\beta(c) \simeq \mathbb{Z} \times B\Gamma_{\infty,|c|+1},$$

[†] $F_i \wr \mathcal{C}$ has the terminal object (b_i, id).

[‡] The theorem is almost certainly valid also for $d = 1$, but the present proof works only for $d > 1$.

where $|c|$ is the number of components in the object c. Addendum 1.4 and Lemma 2.6 apply.

Remark 2.9. The analogue of Theorem 2.8 has been established for the spin mapping class group, and for the non-orientable mapping class group in [21] and [73], respectively. The stable cohomology in the spin case differs only from the orientable case in 2-torsion. In the non-orientable case, the stable rational cohomology is a polynomial algebra in $4i$-dimensional classes.

2.5. Cohomology of $\Omega^\infty\mathbb{G}_{-d}$. The cohomology groups of a prespectrum E are defined to be inverse limits of the cohomology of the individual terms

$$H^k(E) = \varprojlim_n H^{k+n}(E_n; *), \tag{2.7}$$

with the maps in the inverse limit induced by ε_n. Note that $H^k(E)$ might be non-zero also for negative values of k. For example we have

$$H^k(\mathbb{S}) = \mathbb{Z} \qquad \text{for } k = 0,$$
$$H^k(\mathbb{S}) = 0 \qquad \text{for } k \neq 0,$$

and

$$H^k(\mathbb{G}_{-d}) = H^{k+d}(G(d, \infty)).$$

The homotopy groups and homology groups of E are the direct limits

$$\pi_k E = \operatorname{colim} \pi_{k+n}(E_n; *), \quad H_k E = \operatorname{colim} H_{k+n}(E_n; *).$$

Given a spectrum $E = \{E_n, \varepsilon_n\}$ and a space X, we can form the spectrum

$$E \wedge X_+ = \{E_n \wedge X_+, \varepsilon \wedge \mathrm{id}_X\} \quad (E_n \wedge X_+ = E_n \times X/* \times X)$$

and its associated infinite loop space $\Omega^\infty(E \wedge X_+)$. The homotopy groups

$$E_*(X) = \pi_*(E \wedge X_+)$$

form a generalized homology theory: they satisfy the axioms of usual homology, save the dimensional axiom that $H_k(\mathrm{pt})$ vanishes for $k \neq 0$. We shall apply the construction in §3.2 with $E = \mathbb{C}P^\infty_{-1}$.

The cohomology groups of $\Omega^\infty E$ and the cohomology groups of E, as defined in (2.7), are related by the cohomology suspension homomorphism

$$\sigma^*\colon H^k(E) \to H^k(\Omega^\infty_0 E),$$

where $\Omega^\infty_0 E$ denotes the component of the trivial loop[†]. The suspension σ^* is induced from the evaluation map from $\Sigma^n\Omega^n E_n$ to E_n.

[†]The components of $\Omega^\infty E$ are all homotopy equivalent, because $\pi_0(\Omega^\infty E)$ is a group.

The cohomology groups of $\Omega^\infty E$ are usually a lot harder to calculate than the cohomology groups of E, except if one takes cohomology with rational coefficients where the relationship can be described explicitly, as follows:

Given a graded $\mathbb{Q}$-vector space $P^* = \{P^k \mid k > 0\}$, let $A(P^*)$ be the free, graded commutative algebra generated by P^*. It is a polynomial algebra if P^* is concentrated in even degrees, an exterior algebra if P^* is concentrated in odd degrees, and a tensor product of the two in general. A graded basis for P^* serves as multiplicative generators for $A(P^*)$. We give $A(P^*)$ a graded Hopf algebra structure by requiring that P^* be the vector space of primitive elements, so that $A(P^*)$ is primitively generated. The general theory of graded Hopf algebras [55] implies

Theorem 2.10. *There is an isomorphism of Hopf algebras,*

$$H^*(\Omega^\infty_0 E; \mathbb{Q}) \cong A(H^{*>0}(E; \mathbb{Q})).$$

For $E = \mathbb{C}P^\infty_{-1}$, the Thom isomorphism shows that $H^*(\mathbb{C}P^\infty_{-1}; \mathbb{Z})$ has one $\mathbb{Z}$ in each even dimension ≥ -2, and hence by the theorem above that

$$H^*(\Omega^\infty_0 \mathbb{C}P^\infty_{-1}; \mathbb{Q}) = \mathbb{Q}[\kappa_1, \kappa_2, \ldots], \quad \deg \kappa_i = 2i.$$

In view of Theorem 2.8, this proves Corollary 1.3.

The κ_i are integral cohomology classes, namely the image under the cohomology suspension of generators of $H^*(\mathbb{C}P^\infty_{-1}, \mathbb{Z})$. They correspond to the cohomology classes defined in (1.3), cf. [23]. The main result of [23] is the following theorem about their divisibility in the integral lattice of $H^*(B\Gamma_\infty; \mathbb{Q})$,

$$H^*_{\text{free}}(B\Gamma_\infty; \mathbb{Z}) = H^*(B\Gamma_\infty; \mathbb{Z})/\text{Torsion}.$$

Theorem 2.11 ([23]). *Let D_i be the maximal divisor of κ_i in the integral lattice. It is given by the formulas*

$$D_{2i} = 2 \quad \textit{and} \quad D_{2i-1} = \text{denom}(B_i/2i)$$

with B_i equal to the i'th Bernoulli number.

The maximal divisibility of κ_{2i-1} is what could be expected from the Riemann–Roch theorem [57], [56]. The integral cohomology of $\Omega^\infty \mathbb{C}P^\infty_{-1}$, and thus of $B\Gamma_\infty$, contains a wealth of torsion classes of all orders. This follows from [20] which completely calculates $H^*(B\Gamma_\infty; \mathbb{F}_p)$.

The action of the mapping class group on the first homology group of the underlying surface defines a symplectic representation with kernel equal to the Torelli group. In infinite genus, we get a fibration

$$BT_{\infty,1} \xrightarrow{j} B\Gamma_{\infty,1} \xrightarrow{\pi} B\,\mathrm{SP}_\infty(\mathbb{Z}). \tag{2.8}$$

The rational cohomology ring of $B\,\mathrm{SP}_\infty(\mathbb{Z})$ is a polynomial algebra on $(4i-2)$-dimensional generators that map to non-zero multiples of the κ_{2i-1}, cf. [9], [37]. In (2.8) however, the action of $\mathrm{SP}_\infty(\mathbb{Z})$ on $H^*(BT_{\infty,1})$ is highly non-trivial, so one cannot conclude that $j^*(\kappa_{2i}) \neq 0$. Indeed, this is a wide open problem even for κ_2!

3. Auxiliary moduli spaces

This section presents two extensions of the material in §2. Section 3.1 is an account of the automorphism group of a free group, due entirely to S. Galatius [19]. Section 3.2 presents a topological variant of the Gromov–Witten moduli space of pseudo-holomorphic curves in a background, following the joint work with R. Cohen from [12].

3.1. The moduli space of graphs. Let Aut_n denote the automorphism group of a free group on n letters and Out_n its quotient of outer automorphisms. Using 3-manifold techniques, Hatcher [29] proved that the homomorphisms

$$H_k(B\,\mathrm{Out}_n;\mathbb{Z}) \leftarrow H_k(B\,\mathrm{Aut}_n;\mathbb{Z}) \rightarrow H_k(B\,\mathrm{Aut}_{n+1};\mathbb{Z}) \tag{3.1}$$

are isomorphisms in a range that increases with n. See also [31]. The limit Aut_∞ has perfect commutator subgroup (of index 2), and

$$\mathbb{Z}\times B\,\mathrm{Aut}_\infty^+ \xrightarrow{\simeq} \Omega B\big(\textstyle\coprod^n B\,\mathrm{Aut}_n\big).$$

Theorem 3.1 ([19]). *The space $\mathbb{Z}\times B\,\mathrm{Aut}_\infty^+$ is homotopy equivalent to the infinite loop space $\Omega^\infty\mathbb{S}$ of the sphere spectrum.*

We remember that $\Omega^\infty\mathbb{S} = \Omega^\infty S^\infty$ is the homotopy colimit of $\Omega^n S^n$ as $n\to\infty$. Its homotopy groups are the stable homotopy groups of spheres; they are finite except for the group of components [67]. The "standard conjecture" in this case:

$$H^k(B\,\mathrm{Aut}_\infty;\mathbb{Q}) = 0 \quad \text{for } k>0, \tag{3.2}$$

is therefore an immediate consequence of Theorem 3.1.

In spirit, the proof of Theorem 3.1 is analogous to the proof of Theorem 2.8: Graphs are 1-dimensional manifolds with singularities. Below, I shall outline the similarities and the new ideas required to prove Theorem 3.1.

Let U be an open set of $\mathbb{R}^{n+1}$. A graph Y in U is a closed subset with the following property. Each $p\in U$ admits an open neighborhood U_p such that one of the following three cases occurs:

(i) $Y\cap U_p = \emptyset$,

(ii) $Y\cap U_p$ is the image of a smooth embedding $(-\varepsilon,\varepsilon)\hookrightarrow U_p$,

(iii) $Y\cap U_p$ is the image of a continuous embedding of the one point union $\bigvee^k[0,\infty)$, $k\geq 3$; the embedding is smooth on each branch and has transverse intersection at the branch point.

The set $\Phi(U)$ of all graphs in U is topologized in a way that allows the (non-loop) edges to shrink to a vertex and allows graphs to be pushed to infinity. The topology

on $\Phi(U)$ is similar to the topology on the space $\mathcal{T}_d(\mathbb{R}^{n+d}$ from § 2.3. More precisely, Φ is a space-valued sheaf on the category of open sets of $\mathbb{R}^{n+1}$ and their embeddings. It is an equivariant, continuous sheaf on $\mathbb{R}^{n+1}$ in the terminology of [25, §2.2]. In particular, the restriction $\Phi(\mathbb{R}^{n+1}) \to \Phi(B_\varepsilon(0))$ onto an open ε-ball is a homotopy equivalence.

Graphs in $\mathbb{R}^{n+1}$ give rise to the embedded cobordism category $\mathcal{G}(\mathbb{R}^{n+1})$. Its objects consist of a finite number of points in a slice $\{a\} \times \mathbb{R}^n$. A morphism is a "graph with legs (or leaves)" embedded in a strip $[a_0, a_1] \times \mathbb{R}^n$ with the legs meeting the walls orthogonally.

The restriction of a morphism to the open strip is an element of $\Phi((a_0, a_1) \times \mathbb{R}^n)$. Define

$$G(\mathbb{R}^{n+1}) = \{Y \in \Phi(\mathbb{R}^{n+1}) \mid Y \subset \mathbb{R} \times D^n\}.$$

The proofs of (2.4a) and (2.4b) can be adapted to graphs and show

$$B\mathcal{G}(\mathbb{R}^{n+1}) \simeq G(\mathbb{R}^{n+1}). \tag{3.3}$$

Transversality and Phillips' submersion theorem, used in the proof of Theorem 2.8, requires tangent spaces. This approach is not available for graphs, but instead we have Gromov's general h-principle from [25].

Galatius proves that the sheaf Φ is *microflexible*, and concludes from [25, §2.2] that there is a homotopy equivalence

$$G(\mathbb{R}^{n+1}) \simeq \Omega^n \Phi(\mathbb{R}^{n+1}). \tag{3.4}$$

The collection $\Phi(\mathbb{R}^n)$, with the empty graph as basepoint, forms a spectrum $\mathbf{\Phi}$. The structure maps are induced from the map

$$\mathbb{R} \times \Phi(\mathbb{R}^n) \to \Phi(\mathbb{R}^{n+1})$$

that sends (t, Y) to $\{t\} \times Y \subset \mathbb{R} \times \mathbb{R}^n$. It factors over $\Sigma\Phi(\mathbb{R}^n)$. Let $\mathcal{G} = \mathcal{G}(\mathbb{R}^{\infty+1})$ be the union of the $\mathcal{G}(\mathbb{R}^{n+1})$. In the limit over n, (3.3) and (3.4) yield homotopy equivalences

$$B\mathcal{G} \simeq G(\mathbb{R}^{\infty+1}) \simeq \Omega^{\infty-1}\mathbf{\Phi}. \tag{3.5}$$

Theorem 3.2 ([19]). *The spectrum $\mathbf{\Phi}$ is homotopy equivalent to the sphere spectrum $\mathbb{S}$. In particular $\Omega B\mathcal{G} \simeq \Omega^\infty S^\infty$.*

The proof uses the Handel's theorem from [26] that the space $\exp(X)$ of finite subsets of a connected space X is contractible.

Remark 3.3. One of the advantages of Gromov's h-principle over Phillips' submersion theorem, even in the case of manifolds, is that it permits unstable information.

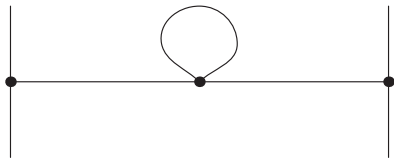
Let $\mathcal{C}_d(\mathbb{R}^{n+d})$ be the category of d-dimensional cobordisms embedded in $\mathbb{R}^{n+d}$ for fixed n. Its classifying space can be identified as

$$B\mathcal{C}_d(\mathbb{R}^{n+d}) \simeq \Omega^{n+d-1}\Psi_d(\mathbb{R}^{n+d}),$$

where $\Psi(\mathbb{R}^{n+d})$ is a space of d-dimensional submanifolds in $\mathbb{R}^{n+d}$, with a topology similar to the above topology on $\Phi(\mathbb{R}^{n+1})$. Theorem 3.2 is replaced by $\Psi_d(\mathbb{R}^{n+d}) \simeq \mathrm{Th}(U_{d,n}^{\perp})$, and we get the following unstable version of Theorem 2.4, valid for any $d \geq 0$ and $n \geq 0$:

$$B\mathcal{C}_d(\mathbb{R}^{n+d}) \simeq \Omega^{n+d-1}\,\mathrm{Th}(U_{d,n}^{\perp}).$$

The final step is to prove that $\Omega B\mathcal{G}$ is homotopy equivalent to $\mathbb{Z} \times B\,\mathrm{Aut}_{\infty}^{+}$. This is very similar to the proof of Theorem 2.7 and Theorem 2.8 in the case of the mapping class group. The contractibility of "outer space" [13], [37, ch. 8] identifies $B\,\mathrm{Aut}_n$ and $B\,\mathrm{Out}_n$ as components of morphism spaces of $\mathcal{G}^{\mathrm{res}}$. Instead of Harer's stability theorem, one uses the generalization [30], [31] of the homology isomorphisms (3.1). The element β_i needed to stabilize the morphism space is the graph



It is an obvious problem to generalize the above to other situations of manifolds with singularities, for example to the case of orbifolds.

3.2. Surfaces in a background. Fix a background space X. What is the stable homology type of the moduli space of pairs (Σ, f) of a Riemann surface Σ, and a continuous map $f\colon \Sigma \to X$?

Let $\mathrm{Emb}_{g,b}^{\infty}$ denote the space of embeddings of a fixed differentiable surface $F = F_{g,b}$ into the strip $[0, 1] \times \mathbb{R}^{\infty+1}$ with boundary circles mapped to $\{0, 1\} \times \mathbb{R}^{\infty+1}$ when $b > 0$. The moduli space in question can be displayed as the orbit space

$$\mathcal{S}_{g,b}(X) = \mathrm{Emb}_{g,b}^{\infty} \times_{\mathrm{Diff}(F,\partial)} \mathrm{Map}(F, X)$$

of the free $\mathrm{Diff}(F, \partial)$ action on the Cartesian product of $\mathrm{Emb}_{g,b}^{\infty}$ and the space $\mathrm{Map}(F, X)$ of continuous mappings of F into X.

It fibres over the free loop space of X^b, $\pi\colon \mathcal{S}_{g,b}(X) \to LX^b$. The space LX is connected when X is simply connected, and in this case the fibres of π are all homotopy equivalent to the space

$$\mathcal{S}_{g,b}(X; x_0) = \mathrm{Emb}_{g,b}^{\infty} \times_{\mathrm{Diff}(F;\partial F)} \mathrm{Map}((F; \partial F), (X; x_0)).$$

Theorem 3.4 ([12]). *For simply connected X and $b > 0$, the maps*

$$\mathcal{S}_{g,b-1}(X; x_0) \leftarrow \mathcal{S}_{g,b}(X; x_0) \to \mathcal{S}_{g+1,b}(X; x_0)$$

induce isomorphisms in integral homology in degrees less than or equal to $g/2 - 2$.

Theorem 3.4 might appear a surprise from the following viewpoint: In the fibration

$$\mathrm{Map}((F, \partial F), (X; x_0)) \to \mathcal{S}_{g,b}(X; x_0) \to B\,\mathrm{Diff}(F; \partial F),$$

the homology of the base is independent of the genus and of the number of boundary components in a range, whereas the fibre grows in size with g and b. This would seem to prevent stabilization. The explanation is, however, that the fundamental group $\Gamma_{g,b} = \pi_1 B\,\mathrm{Diff}(F; \partial F)$ acts very non-trivially on the homology of the fibre.

The proof of Theorem 3.4 adapts and generalizes ideas from [39] about stability with twisted coefficients. The $\Gamma(F)$-module of twisted coefficients is

$$V_r(F) = H_r(\mathrm{Map}((F; \partial F), (X; x_0)); \mathbb{Z}).$$

It is of "finite degree" [40], [39], precisely when X is simply connected. This explains the unfortunate assumption in Theorem 3.4 that X be simply connected.

Theorem 3.5. *For simply connected X, there is a map*

$$\alpha_X \colon \mathbb{Z} \times \mathcal{S}_{\infty,b}(X; x_0) \to \Omega^\infty(\mathbb{C}P^\infty_{-1} \wedge X_+)$$

which induces isomorphism on integral homology.

Given Theorem 3.4, the proof of Theorem 3.5 can be deduced from section 7 of [47]. Alternatively, one can adopt the strategy of §2 above. The categories $\mathcal{C}_d$ and $\mathcal{C}_d^{\mathrm{red}}$ are replaced by the categories $\mathcal{C}_d(X)$ and $\mathcal{C}_d^{\mathrm{red}}(X)$ consisting of embedded cobordisms together with a map from the cobordism into X. Theorem 2.4 and Theorem 2.7 are valid for these categories,

$$B\mathcal{C}_d(X) \simeq B\mathcal{C}_d^{\mathrm{red}}(X) \simeq \Omega^{\infty-1}(\mathbb{G}_{-d} \wedge X_+). \tag{3.6}$$

For $d = 2$, we can apply Lemma 2.6 to complete the proof of Theorem 3.5.

For applications of Theorem 3.5, e.g. in string topology, one needs versions with marked points on the underlying surface. There are two cases: one in which the marked points are allowed to be permuted by the diffeomorphisms, and one in which the marked points are kept fixed. The first case is relevant to open-closed strings [3].

Here are some details. Given a surface $F^s = F^s_{g,b}$ with s interior marked points, let $\mathrm{Diff}(F^{(s)}; \partial F^{(s)})$ be the group of oriented diffeomorphisms that keeps ∂F^s pointwise fixed and permute the marked points. The associated moduli space,

$$\mathcal{S}^{(s)}_{g,b}(X; x_0) = \mathrm{Emb}^\infty_{g,b} \times_{\mathrm{Diff}(F^{(s)}; \partial F^{(s)})} \mathrm{Map}((F^s; \partial F^s); (X; x_0)),$$

fits into a fibration

$$\pi\colon \mathcal{S}^{(s)}_{g,b}(X;x_0) \to E\Sigma_s \times_{\Sigma_s} (X \times \mathbb{C}P^\infty)^s$$

with fibre $\mathcal{S}_{g,b+s}(X;x_0)$, cf. (1.4). Here Σ_s denotes the permutation group. There are stabilization maps

$$\mathcal{S}^{(s)}_{g,b}(X;x_0) \to \mathcal{S}^{(s+1)}_{g+1,b}(X;x_0) \tag{3.7}$$

that add $F^1_{1,2}$, a torus with two boundary circles and one marked point, to one of the boundary circles.

Infinite loop space theory tells us that the homotopy colimit or telescope of $E\Sigma_s \times_{\Sigma_s} (X \times \mathbb{C}P^\infty)^s$ as $s \to \infty$ is homology equivalent to $\Omega^\infty(\mathbb{S} \wedge (X \times \mathbb{C}P^\infty)_+) = \Omega^\infty S^\infty(X \times \mathbb{C}P^\infty_+)$.

For the moduli space $\mathcal{S}^s_{g,b}(X;x_0)$, where the marked points are kept fixed by the diffeomorphism group, the space $E\Sigma_s \times_{\Sigma_s} (X \times \mathbb{C}P^\infty)^s$ is replaced by $(X \times \mathbb{C}P^\infty)^s$, and $\Omega^\infty S^\infty(X \times \mathbb{C}P^\infty_+)$ by $\Omega S(X \times \mathbb{C}P^\infty_+)$, cf. [18].

Addendum 3.6. There are homology equivalences

(i) $\mathbb{Z} \times \mathbb{Z} \times \mathcal{S}^{(\infty)}_{\infty,b}(X;x_0) \to \Omega^\infty(\mathbb{C}P^\infty_{-1} \wedge X_+) \times \Omega^\infty S^\infty(X \times \mathbb{C}P^\infty_+)$,

(ii) $\mathbb{Z} \times \mathbb{Z} \times \mathcal{S}^\infty_{\infty,b}(X;x_0) \to \Omega^\infty(\mathbb{C}P^\infty_{-1} \wedge X_+) \times \Omega S(X \times \mathbb{C}P^\infty_+)$.

It was the Gromov–Witten moduli space and the string topology spaces of M. Chas and D. Sullivan [10], [68] that inspired us to consider the moduli spaces of Theorem 3.5 and Addendum 3.6. While our results are nice in their own right, the question remains if they could be useful for a better understanding of Gromov–Witten invariants and string topology.

The most obvious starting point would be to give a homotopical interpretation of the Batalin–Vilkovsky structure on the chain groups of $\bigsqcup \mathcal{S}_g(M)$, [68], somewhat similar to the homotopical definition in [11] of the Chas–Sullivan loop product.

4. Algebraic K-theory and trace invariants

Quillen's algebraic K-theory space $K(R)$ of a ring R [62], and Waldhausen's algebraic K-theory $A(X)$ of a topological space X [74] are two special cases of algebraic K-theory of "brave new rings". A brave new ring is a ring spectrum whose category of modules fits the axiomatic framework of K-theory laid down in [76]. There are several good choices for the category of brave new rings; one such is Bökstedt's Functors with Smash Products, a closely related one is the more convenient category of symmetric orthogonal spectra [49], [48]. In this category, both K-theory and its companion $\mathrm{TC}(-;p)$ (the topological cyclic homology at p) works well, and one has a good construction of the cyclotomic trace

$$\mathrm{tr}_p\colon K(E) \to \mathrm{TC}(E;p). \tag{4.1}$$

The topological cyclic homology and the trace map tr_p was introduced in joint work with M. Bökstedt and W.-C. Hsing in order to give information about the p-adic homotopy type of $K(E)$, cf. [7].

The Eilenberg–MacLane spectrum $H(R)$ of a ring R is a brave new ring; its K-theory is equivalent to Quillen's original $K(R)$. The K-theory of the brave new ring $\mathbb{S} \wedge \Omega X_+$ is Waldhausen's $A(X)$.

The product over all primes of the p-adic completion of $\mathrm{TC}(E;\, p)$ can be combined with a version of negative cyclic homology for $E \otimes \mathbb{Q}$ to define $\mathrm{TC}(E)$, [24]. There is a trace map from $K(E)$ to $\mathrm{TC}(E)$ whose p-adic completion is the p-adic completion of tr_p, and a map from $\mathrm{TC}(H(R))$ to the usual negative cyclic homology of $R \otimes \mathbb{Q}$.

4.1. $A(X)$ and diffeomorphisms. I begin with Waldhausen's definition of $A(\mathrm{pt})$. Let S_q be the category of length q "flags" of based, finite CW-complexes. An object consists of a string

$$X_1 \rightarrowtail X_2 \rightarrowtail \cdots \rightarrowtail X_q \ , \tag{4.2}$$

where the arrows are based cellular inclusions ($S_0 = *$). The morphisms in S_q are the based homotopy equivalences of flags. There are face operators

$$d_i \colon S_q \to S_{q-1}, \quad i = 0, \ldots, q,$$

where d_0 divides out X_1 in that it replaces (4.2) with the flag

$$X_2/X_1 \rightarrowtail \cdots \rightarrowtail X_q/X_1 \ ,$$

and d_i forgets X_i, when $i > 0$. This makes $S_\bullet$ into a simplicial category.

The classifying spaces BS_q with the induced d_i form a simplicial space $BS_\bullet$, and $A(\mathrm{pt})$ is the loop space of its topological realization,

$$A(\mathrm{pt}) = \Omega |BS_\bullet| = \Omega\big(\textstyle\bigsqcup \Delta^k \times BS_k/\!\sim\big). \tag{4.3}$$

(The definition of $A(X)$ is similar; S_q is replaced with the set of flags

$$X \rightarrowtail X_1 \rightarrowtail \cdots \rightarrowtail X_q \longrightarrow X,$$

whose composite is the identity map of X, and with $(X_i;\, X)$ a finite relative CW-complex). By definition,

$$BS_1 = \textstyle\bigsqcup B\,\mathrm{Aut}(Y)$$

where Y runs over finite CW-complexes and $\mathrm{Aut}(Y)$ denotes the monoid of pointed self-homotopy equivalences. The map from $\Delta^1 \times BS_1$ into $|BS_\bullet|$ induces a map

$$B\,\mathrm{Aut}(Y) \longrightarrow A(\mathrm{pt}), \tag{4.4}$$

and one may view $A(\mathrm{pt})$ as a kind of moduli space of finite CW-complexes.

Given the homotopy theoretic nature of the construction of $A(\mathrm{pt})$ and more generally of $A(X)$, the following theorem from [74] and [75] seems miraculous.

Theorem 4.1 ([74]). *There are homotopy equivalences*

(i) $A(\mathrm{pt}) \simeq \mathrm{hocolim}\, \Omega^n(\mathrm{Top}_{n+1} / \mathrm{Top}_n)$,

(ii) $A(X) \simeq \Omega^\infty S^\infty(X_+) \times \mathrm{Wh}^{\mathrm{Diff}}(X)$,

(iii) $\Omega^2 \mathrm{Wh}^{\mathrm{Diff}}(X) \simeq \mathrm{hocolim}_k \mathrm{Diff}(X \times I^{k+1}; X \times I^k)$, *provided X is a smooth manifold.*

In (i), Top_{n+1} denotes the topological group of homeomorphisms of $\mathbb{R}^{n+1}$, and $\mathrm{Top}_{n+1} / \mathrm{Top}_n$ is the associated homogenous space. The right-hand side of (iii) is the homotopy colimit of the space of diffeomorphisms of $X \times I^{k+1}$ that induces the identity on the submanifold $X \times I^k$ of the boundary, the so called stable pseudo-isotopy space of X. There is a stability range for pseudo-isotopy spaces in terms of $\dim(X)$ due to K. Igusa [36], namely

$$\mathrm{Diff}(X \times I; X \times 0) \to \mathrm{hocolim}_k \mathrm{Diff}(X \times I^{k+1}, X \times I^k) \tag{4.5}$$

induces isomorphism on homotopy groups in degree i if $3i < \dim X - 7$.

Theorem 4.1 is the conclusion of a long development in geometric topology. See the references in [75], where its proof was sketched out. The final details are due to appear in [77].

4.2. Topological cyclic homology. There is a trace map, due to K. Dennis, from $K(R)$ into a space $\mathrm{HH}(R)$, whose homotopy groups are the Hochschild homology groups of R with coefficients in the bimodule R itself, cf. [43, 8.4]. This was generalized to brave new rings by M. Bökstedt who constructed the topological Hochschild homology space $\mathrm{THH}(E)$ and a trace map from $K(E)$ into it. $\mathrm{THH}(E)$ is a cyclic space in the sense of Connes [43], so it comes equipped with a continuous action of the circle group $\mathbb{T}$. (Actually, $\mathrm{THH}(E)$ is a brave new ring with a $\mathbb{T}$-action.) Topological cyclic homology $\mathrm{TC}(E; p)$ is made out of the fixed sets $\mathrm{THH}(E)^{C_{p^n}}$ of the cyclic subgroups of $\mathbb{T}$.

The invariant (4.1) is the key tool for our present understanding of $A(X)$ and more generally $K(E)$. Consider a homomorphism $\varphi\colon E \to F$ of brave new rings and the induced diagram

$$\begin{array}{ccc} K(E) & \longrightarrow & \mathrm{TC}(E; p) \\ \downarrow & & \downarrow \\ K(F) & \longrightarrow & \mathrm{TC}(F; p). \end{array} \tag{4.6}$$

The following theorem of B. Dundas contains a basic relationship between K and TC. The theorem was conjectured by T. Goodwillie in [24], and proved in a special case by R. McCarthy in [50].

Theorem 4.2 ([14]). *Suppose $\pi_0 E \to \pi_0 F$ is a surjective ring homomorphism with nilpotent kernel. Then* (4.6) *becomes homotopy Cartesian after p-adic completion.*

I will now turn to the calculation of $\mathrm{TC}(X;\, p)$, the topological cyclic homology of the brave new ring $\mathbb{S} \wedge \Omega X_+$. There is a commutative diagram

$$\begin{array}{ccc} \mathrm{TC}(X;\, p) & \longrightarrow & \Omega^{\infty-1} S^\infty (E\mathbb{T} \times_{\mathbb{T}} LX_+) \\ \downarrow & & \downarrow \mathrm{trf} \\ \Omega^\infty S^\infty (LX_+) & \xrightarrow{1-\Delta_p} & \Omega^\infty S^\infty (LX_+), \end{array} \tag{4.7}$$

where $\Delta_p \colon LX \to LX$ sends a loop $\lambda(z)$ to $\lambda(z^p)$, $z \in S^1$, and trf is the $\mathbb{T}$-transfer map (a fibrewise Pontryagin–Thom collapse map).

Theorem 4.3 ([7]). *The diagram* (4.7) *becomes homotopy Cartesian after p-adic completion.*

When X is a single point, the theorem reduces to the statement

$$\mathrm{TC}(\mathrm{pt};\, p) \simeq_p \Omega^\infty S^\infty \times \Omega^{\infty-1} \mathbb{C}P^\infty_{-1}, \tag{4.8}$$

with $\simeq_p$ indicating that the two sides become homotopy equivalent after p-adic completion. In particular the two sides have the same mod p homotopy groups.

Theorem 4.2, applied to the case in which E is the sphere spectrum and F is the Eilenberg–Maclane spectrum of the integers, tells us that the homotopy fibres of $A(\mathrm{pt}) \to K(\mathbb{Z})$ and $\mathrm{TC}(\mathrm{pt};\, p) \to \mathrm{TC}(\mathbb{Z};\, p)$ have the same p-adic completions. This reduces the understanding of $A(\mathrm{pt})$ to the understanding of $K(\mathbb{Z})$ and the fibre of $\mathrm{TC}(\mathrm{pt};\, p) \to \mathrm{TC}(\mathbb{Z};\, p)$. The structure of $\mathrm{TC}(\mathbb{Z};\, p)$ is given in [8], [63].

If the ring R is finitely generated as an abelian group, then

$$\mathrm{TC}(R;\, p) \simeq_p \mathrm{TC}(R \otimes \mathbb{Z}_p;\, p).$$

The corresponding statement for K-theory is false, so the absolute invariant (4.1) is effective mostly for p-complete rings. There is an extensive theory surrounding the functor $\mathrm{TC}(R;\, p)$, developed in joint work with L. Hesselholt in [33], [34]. See also [32]. The p-adic completion of $\mathrm{TC}(R;\, p)$ is explicitly known when R is the ring of integers in a finite field extension of $\mathbb{Q}$, and in this case (4.1) induces an equivalence

$$K(R \otimes \mathbb{Z}_p) \simeq_p \mathrm{TC}(R;\, p).$$

For global rings, the motivic theory is the basic tool for calculations of $K(R)$; see F. Morel's article in these proceedings.

In view of Theorem 4.2 and Theorem 4.3, it is of obvious interest to examine the map from $\mathrm{TC}(X;\, p)$ to $\mathrm{TC}(\mathbb{Z}[\pi_1 X];\, p)$, but essentially nothing is known about this problem. Two special cases are of particular interest. The case $X = \mathrm{pt}$ is required for the homotopical control of the fibre of $A(\mathrm{pt}) \to K(\mathbb{Z})$. The case $X = S^1$ is, by theorems of T. Farrell and L. Jones, related to the homotopical structure of the group of homeomorphisms of negatively curved closed manifolds, cf. [45].

Let $\mathbb{K}$ be the periodic spectrum whose $2n$'th space is $\mathbb{Z} \times BU$ and with structure maps induced from Bott periodicity. It is believed that $A(\mathbb{K})$ will be important in the study of field theories, so one would like to understand the homotopy type of $\mathrm{TC}(\mathbb{K}; p)$. There are helpful partial results from [2], [1], but the problem seems to be a very difficult one.

Finally, and maybe most important, there are reasons to believe that the moduli space of Riemann surfaces is related to $\mathrm{TC}(\mathrm{pt}; p)$, possibly via field theories. The spectrum $\mathbb{C}P^{\infty}_{-1}$ occurs in both theories. It is a challenge to understand why.

References

[1] Ausoni, C., Topological Hochschild homology of connective complex K-theory. *Amer. J. Math.* **127** (6) (2005), 1261–1313.

[2] Ausoni, C., and Rognes, J., Algebraic K-theory of topological K-theory. *Acta Math.* **188** (1) (2002), 1–39.

[3] Baas, N., Cohen, R. L., and Ramirez, A., The topology of the category of open and closed strings. *Contemp. Math.* **407** (2006), 11–26.

[4] Barratt, M., and Priddy, S., On the homology of non-connected monoids and their associated groups. *Comment. Math. Helv.* **47** (1972), 1–14.

[5] Berrick, A. J., *An approach to algebraic K-theory*. Res. Notes in Math. 56, Pitman (Advanced Publishing Program), Boston, Mass., 1982.

[6] Bödigheimer, C.-F., and Tillmann, U., Stripping and splitting decorated mapping class groups. In *Cohomological methods in homotopy theory* (Bellaterra, 1998), Progr. Math. 196, Birkhäuser, Basel 2001, 47–57.

[7] Bökstedt, M., Hsiang, W. C., and Madsen, I., The cyclotomic trace and algebraic K-theory of spaces. *Invent. Math.* **111** (3) (1993), 465–539.

[8] Bökstedt, M., and Madsen, I., Algebraic K-theory of local number fields: the unramified case. In *Prospects in topology* (Princeton, NJ, 1994), Ann. of Math. Stud. 138, Princeton University Press, Princeton, NJ, 1995, 28–57.

[9] Borel, A., Stable real cohomology of arithmetic groups. *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 235–272.

[10] Chas, M., and Sullivan, D., String topology. Preprint, 1999; arXiv:math.GT/9911159v1.

[11] Cohen, R. L., and Jones, J. D. S., A homotopy theoretic realization of string topology. *Math. Ann.* **324** (4) (2002), 773–798.

[12] Cohen, R. L., and Madsen, I., Surfaces in a background space and the homology of mapping class groups. Preprint, 2006; arXiv:math.GT/0601750.

[13] Culler, M., and Vogtmann, K., Moduli of graphs and automorphisms of free groups. *Invent. Math.* **84** (1) (1986), 91–119.

[14] Dundas, B. I., Relative K-theory and topological cyclic homology. *Acta Math.* **179** (2) (1997), 223–242.

[15] Earle, C. J., and Eells, J., A fibre bundle description of Teichmüller theory. *J. Differential Geometry* **3** (1969), 19–43.

[16] Earle, C. J., and Schatz, A., Teichmüller theory for surfaces with boundary. *J. Differential Geometry* **4** (1970), 169–185.

[17] Eliashberg, Y., Galatius, S., and Mishachev, N., The Madsen-Weiss theorem for geometrically minded topologists. In preparation.

[18] Fiedorowicz, Z., Classifying spaces of topological monoids and categories. *Amer. J. Math.* **106** (2) (1984), 301–350.

[19] Galatius, S., private communication.

[20] Galatius, S., Mod p homology of the stable mapping class group. *Topology* **43** (5) (2004), 1105–1132.

[21] Galatius, S., Mod 2 homology of the stable spin mapping class group. *Math. Ann.* **334** (2006), 439–455.

[22] S. Galatius, Madsen, I., U. Tillmann, and M. Weiss. The homotopy type of the cobordism category. Preprint, 2006; arXiv:math.AT/0605249.

[23] Galatius, S., Madsen, I., and Tillmann, U., Divisibility of the stable Miller-Morita-Mumford classes. *J. Amer. Math. Soc.* **19** (4) (2006), 759–779.

[24] Goodwillie, T. G., The differential calculus of homotopy functors. In *Proceedings of the International Congress of Mathematicians* (Kyoto, 1990), Vol. I, The Mathematical Society of Japan, Tokyo, Springer-Verlag, Tokyo, 1991, 621–630.

[25] Gromov, M., *Partial differential relations*. Ergeb. Math. Grenzgeb (3) 9, Springer-Verlag, Berlin 1986.

[26] Handel, D., Some homotopy properties of spaces of finite subsets of topological spaces. *Houston J. Math.* **26** (4) (2000), 747–764.

[27] Harer, J. L., Stability of the homology of the mapping class groups of orientable surfaces. *Ann. of Math.* (2) **121** (2) (1985), 215–249.

[28] Harris, J., and Morrison, I., *Moduli of curves*. Grad. Texts in Math. 187, Springer-Verlag, New York 1998.

[29] Hatcher, A., Homological stability for automorphism groups of free groups. *Comment. Math. Helv.* **70** (1) (1995), 39–62.

[30] Hatcher, A., and Vogtmann, K., Homological stability for outer automorphism groups of free groups. *Algebr. Geom. Topol.* **4** (2004), 1253–1272.

[31] Hatcher, A., Vogtmann, K., and Wahl, N., Erratum to: Homological stability for automorphism groups of free groups. *Algebr. Geom. Topol.* **6** (2006), 573–579.

[32] Hesselholt, L., Algebraic K-theory and trace invariants. *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. II, Higher Ed. Press, Beijing 2002, 415–425.

[33] Hesselholt, L., and Madsen, I., On the K-theory of local fields. *Ann. of Math.* (2) **158** (1) (2003), 1–113.

[34] Hesselholt, L., and Madsen, I., On the De Rham-Witt complex in mixed characteristic. *Ann. Sci. École Norm. Sup.* (4) **37** (1) (2004), 1–43.

[35] Hopkins, M. J., Algebraic topology and modular forms. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. I, Higher Ed. Press, Beijing 2002, 291–317.

[36] Igusa, K., The stability theorem for smooth pseudoisotopies. *K-Theory* **2** (1–2) (1988), 1–355.

[37] Igusa, K., *Higher Franz-Reidemeister torsion*. AMS/IP Stud. in Adv. Math. 31, Amer. Math. Soc., Providence, RI, 2002.

[38] Ivanov, N. V., Stabilization of the homology of Teichmüller modular groups. *Leningrad Math. J.* **1** (1990), 675–691.

[39] Ivanov, N. V., On the homology stability for Teichmüller modular groups: closed surfaces and twisted coefficients. In *Mapping class groups and moduli spaces of Riemann surfaces* (Göttingen, 1991/Seattle, WA, 1991), Contemp. Math. 150, Amer. Math. Soc., Providence, RI, 1993, 149–194.

[40] van der Kallen, W., Homology stability for linear groups. *Invent. Math.* **60** (3) (1980), 269–295.

[41] Kirwan, F., Cohomology of moduli spaces. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. I, Higher Ed. Press, Beijing 2002, 363–382.

[42] Kriegl, A., and Michor, P. W., *The convenient setting of global analysis*. Math. Surveys Monogr. 53, Amer. Math. Soc., Providence, RI, 1997.

[43] Loday, J.-L., *Cyclic homology*. Appendix E by María O. Ronco, Grundlehren Math. Wiss. 301, Springer-Verlag, Berlin 1992.

[44] Looijenga, E., Cohomology of $\mathcal{M}_3$ and $\mathcal{M}_3^1$. In *Mapping class groups and moduli spaces of Riemann surfaces* (Göttingen, 1991/Seattle, WA, 1991), Contemp. Math. 150, Amer. Math. Soc., Providence, RI, 1993, 205–228.

[45] Madsen, I., The cyclotomic trace in algebraic K-theory. In *First European Congress of Mathematics* (Paris, 1992), Vol. II, Progr. Math. 120, Birkhäuser, Basel 1994, 213–241.

[46] Madsen, I., and Tillmann, U., The stable mapping class group and $Q(\mathbb{C}P^\infty_+)$. *Invent. Math.* **145** (3) (2001), 509–544.

[47] Madsen, I., and Weiss, M., The stable moduli space of Riemann surfaces: Mumford's conjecture. *Ann. of Math.* **165** (3) (2007), to appear; Preprint 2004; arXiv:math.AT/0212321.

[48] Mandell, M. A., and May, J. P., Equivariant orthogonal spectra and S-modules. *Mem. Amer. Math. Soc.* **159** (755) (2002), x + 108.

[49] Mandell, M. A., May, J. P., Schwede, S., and Shipley, B., Model categories of diagram spectra. *Proc. London Math. Soc.* (3) **82** (2) (2001), 441–512.

[50] McCarthy, R., Relative algebraic K-theory and topological cyclic homology. *Acta Math.* **179** (2) (1997), 197–222.

[51] McDuff, D., and Segal, G., Homology fibrations and the "group-completion" theorem. *Invent. Math.* **31** (3) (1975/76), 279–284.

[52] Miller, E. Y., The homology of the mapping class group. *J. Differential Geom.* **24** (1) (1986), 1–14.

[53] Milnor, J., Construction of universal bundles. II. *Ann. of Math.* (2) **63** (1956), 430–436.

[54] Milnor, J., On axiomatic homology theory. *Pacific J. Math.* **12** (1962), 337–341.

[55] Milnor, J. W., and Moore, J. C., On the structure of Hopf algebras. *Ann. of Math.* (2) **81** (1965), 211–264.

[56] Morita, S., Characteristic classes of surface bundles. *Invent. Math.* **90** (3) (1987), 551–577.

[57] Mumford, D., Towards an enumerative geometry of the moduli space of curves. In *Arithmetic and geometry*, Vol. II, Progr. Math. 36, Birkhäuser, Boston, MA, 1983, 271–328.

[58] Phillips, A., Submersions of open manifolds. *Topology* **6** (1967), 171–206.

[59] Pontrjagin, L. S., A classification of continuous transformations of a complex into a sphere. I. *Doklady Akad. Nauk SSSR* (*N.S.*) **19** (1938), 147–149.

[60] Pontrjagin, L. S., A classification of continuous transformations of a complex into a sphere. II. *Doklady Akad. Nauk SSSR* (*N.S.*) **19** (1938), 361–363.

[61] Quillen, D., On the cohomology and K-theory of the general linear groups over a finite field. *Ann. of Math.* (2) **96** (1972), 552–586.

[62] Quillen, D., Higher algebraic K-theory. I. In *Algebraic K-theory, I: Higher K-theories* (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), Lecture Notes in Math. 341, Springer-Verlag, Berlin 1973, 85–147.

[63] Rognes, J., Topological cyclic homology of the integers at two. *J. Pure Appl. Algebra* **134** (3) (1999), 219–286.

[64] Segal, G., Classifying spaces and spectral sequences. *Inst. Hautes Études Sci. Publ. Math.* **34** (1968), 105–112.

[65] Segal, G., Geometric aspects of quantum field theory. In *Proceedings of the International Congress of Mathematicians* (Kyoto, 1990), Vol. II, The Mathematical Society of Japan, Tokyo, Springer-Verlag, Tokyo 1991, 1387–1396.

[66] Segal, G., The definition of conformal field theory. In *Topology, geometry and quantum field theory*, London Math. Soc. Lecture Note Ser. 308, Cambridge University Press, Cambridge 2004, 421–577.

[67] Serre, J.-P., Groupes d'homotopie et classes de groupes abéliens. *Ann. of Math.* (2) **58** (1953), 258–294.

[68] Sullivan, D., Sigma models and string topology. In *Graphs and patterns in mathematics and theoretical physics*, Proc. Sympos. Pure Math. 73, Amer. Math. Soc., Providence, RI, 2005, 1–11.

[69] Thom, R., Espaces fibrés en sphères et carrés de Steenrod. *Ann. Sci. Ecole Norm. Sup.* (3) **69** (1952), 109–182.

[70] Thom, R., Quelques propriétés globales des variétés différentiables. *Comment. Math. Helv.* **28** (1954), 17–86.

[71] Tillmann, U., On the homotopy of the stable mapping class group. *Invent. Math.* **130** (2) (1997), 257–275.

[72] Tommasi, O., Rational cohomology of the moduli space of genus 4 curves. *Compositio Math.* **141** (2) (2005), 359–384.

[73] Wahl, N., Homological stability for the mapping class groups of non-orientable surfaces. Preprint, 2006; arXiv:math.GT/0601310.

[74] Waldhausen, F., Algebraic K-theory of topological spaces. I. In *Algebraic and geometric topology* (Stanford University, Stanford, Calif., 1976), Part 1, Proc. Sympos. Pure Math. 32, Amer. Math. Soc., Providence, RI, 1978, 35–60.

[75] Waldhausen, F., Algebraic K-theory of spaces, a manifold approach. In *Current trends in algebraic topology* (London, Ont., 1981), Part 1, CMS Conf. Proc. 2, Amer. Math. Soc., Providence, RI, 1982, 141–184.

[76] Waldhausen, F., Algebraic K-theory of spaces. In *Algebraic and geometric topology* (New Brunswick, N.J., 1983), Lecture Notes in Math. 1126, Springer-Verlag, Berlin 1985, 318–419.

[77] Waldhausen, F., Jahren, B., and Rognes, J., Spaces of PL manifolds and categories of simple maps. In preparation.

[78] Wall, C. T. C., Determination of the cobordism ring. *Ann. of Math.* (2) **72** (1960), 292–311.

[79] Weiss, M., What does the classifying space of a category classify? *Homology Homotopy Appl.* **7** (1) (2005), 185–195.

[80] Whitney, H., Differentiable manifolds. *Ann. of Math.* (2) **37** (3) (1936), 645–680.

Department of Mathematical Sciences, University of Aarhus, Denmark.
E-mail: imadsen@imf.au.dk

Advances in convex optimization: conic programming

Arkadi Nemirovski

Abstract. During the last two decades, major developments in convex optimization were focusing on *conic programming*, primarily, on linear, conic quadratic and semidefinite optimization. Conic programming allows to reveal rich structure which usually is possessed by a convex program and to exploit this structure in order to process the program efficiently. In the paper, we overview the major components of the resulting theory (conic duality and primal-dual interior point polynomial time algorithms), outline the extremely rich "expressive abilities" of conic quadratic and semidefinite programming and discuss a number of instructive applications.

Mathematics Subject Classification (2000). Primary 90C22,90C25,90C51,90C90; Secondary 49N15.

Keywords. Convex, conic and semidefinite programming, duality, polynomial time algorithms.

1. Conic programming – motivation

1.1. Efficiency issues in mathematical programming. Mathematical programming is about solving *optimization programs* of the form

$$\mathrm{Opt} = \min_{x\in\mathbb{R}^n} \{f_0(x) : f_i(x) \le 0,\ i = 1,\dots,m\}, \tag{1}$$

where the *objective* $f_0(\cdot)$ and the *constraints* $f_i(\cdot)$ are given functions on $\mathbb{R}^n$, usually assumed to be smooth (at least C^1). The corresponding body of knowledge, in its mathematical aspects (that is, aside of modelling and implementation issues), focuses on characterization of optimal solutions (necessary/sufficient optimality conditions), their sensitivity to program's data and on developing and theoretical investigation of computational algorithms aimed at building approximate solutions. It should be stressed that the ultimate goal is to *find* a solution rather than to *prove* its existence, uniqueness, etc. As a matter of fact, the situations where a "closed analytic form solution" is available are rare exceptions, this is why the focus is on algorithms capable to approximate optimal solutions within (any) desired accuracy. Moreover, what matters is not just the convergence of an algorithm, but its *efficiency* – a "reasonable" dependence of the computational effort on the required accuracy. The emphasis on the algorithmic and efficiency aspects is what makes the major difference between mathematical programming (MP) and its "pure" counterparts, like calculus of variations, and gives the MP theory its specific flavour.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

Mathematical programming arose in early 1950s as a natural extension of linear programming (LP). The latter, invented around 1947 by George Dantzig, focuses on optimization programs with linear objective and constraints. Significant post-war demand on techniques for modelling and processing logistic and planning problems, nice duality theory allowing, among other things, for far-reaching interpretations in Economics, excellent practical performance of the famous LP simplex algorithm (Dantzig 1947), availability of new computational devices – computers – all these factors were crucial for emerging and rapid development of theory and algorithms for LP and MP. Eventually, in these developments the problem of *theoretically efficient solvability* of various classes of MP programs was addressed. This problem was posed first for linear programming, and the corresponding story is an excellent example of the "specific flavour" of MP we have mentioned. At the first glance, the problem of finding a solution to a system of m linear inequalities with n real unknowns (this is what LP is about) seems completely trivial – invoking the standard characterization of extreme points of polyhedral sets, it reduces to solving at most $\binom{m}{n}$ systems of linear equations. The difficulty is that the number of systems blows up exponentially with the sizes m, n of the system, which makes this naive approach completely impractical already with m, n like few tens. Dantzig's simplex algorithm inspects the systems in a "smart" order, which in practice allows to arrive at a solution pretty fast; however, in the worst case, exponentially many systems should be inspected, so that the simplex method is *not* theoretically efficient. Developing theoretically efficient algorithms for LP is an extremely challenging and deep problem, and it took over 20 years to find the first such algorithm (Khachiyan, 1978). Note that all known efficient LP algorithms do something completely different from inspecting the above systems of linear equations.

Informally, the question we are interested in is: given a class of MP programs, does it admit an efficient solution algorithm, and the first issue here is what does efficiency mean. In combinatorial complexity theory (CCT), there are good reasons to qualify a "fully finite" algorithm (e.g., Turing machine) converting finite binary words – data of instances of a discrete problem – into solutions to the instances as *efficient*, if the conversion time is polynomial in the bit length of the input (see, e.g., [21]). For problems with continuous data and decision variables, similar reasons lead to the concept of a real arithmetic polynomial time algorithm as follows ([8]; cf. [12]). Consider a *generic* MP problem $\mathcal{P}$ – a family of instances of the form (1), with instance p specified within $\mathcal{P}$ by its *data vector* $\mathrm{Data}(p) \in \mathbb{R}^{N(p)}$.

E.g., LP can be naturally considered as a generic problem, with the data vector $\mathrm{Data}(p)$ of an LP program p defined as follows: the first 2 entries are the numbers $m = m(p)$ of constraints and $n = n(p)$ of variables, and the remaining $(m(p) + 1)(n(p) + 1) - 1$ entries are the vectors of coefficients of the objective and constraints stacked atop each other into a single column.

A *solution algorithm* $\mathcal{B}$ for $\mathcal{P}$ is a code for an idealized real arithmetic computer capable to store real numbers and to perform exact real arithmetic operations (a.o.) – four arithmetic operations, comparisons and computations of univariate elementary

functions, like $\sqrt{\cdot}$, $\exp\{\cdot\}$, etc. Loaded with this code and an input comprised of $\mathrm{Data}(p)$, $p \in \mathcal{P}$, and $\varepsilon > 0$, the computer should terminate in a finite number $N(p, \varepsilon)$ of operations and output either an ε-solution to p – a vector $x_\varepsilon \in \mathbb{R}^{n(p)}$ such that $f_i^{(p)}(x_\varepsilon) \le \varepsilon$, $i = 1, \ldots, m(p)$, and

$$f_0^{(p)}(x_\varepsilon) \le \varepsilon + \mathrm{Opt}(p), \quad \mathrm{Opt}(p) = \inf_x \{f_0^{(p)}(x) : f_i^{(p)}(x) \le 0,\ i = 1, \ldots, m(p)\}$$

(here $n(p)$ is number of variables in p, $f_0^{(p)}, \ldots, f_{m(p)}^{(p)}$ are the objective and the constraints of p), or a correct claim that p is infeasible (i.e., $\mathrm{Opt}(p) = +\infty$), or a correct claim that p is unbounded (i.e., $\mathrm{Opt}(p) = -\infty$). A solution method $\mathcal{B}$ is *polynomial time* ("computationally efficient"), if $N(p, \varepsilon)$ is bounded by a polynomial in the *size* $\mathrm{Size}(p) = \dim \mathrm{Data}(p)$ of the instance and the *number of accuracy digits* in an ε-solution defined as

$$\mathrm{Digits}(p, \varepsilon) = \log\left([\mathrm{Size}(p) + \|\mathrm{Data}(p)\|_1 + \varepsilon^2]/\varepsilon\right) = (1+o(1))\log(1/\varepsilon),\ \varepsilon \to 0.$$

Finally, generic problem $\mathcal{P}$ is called *polynomially solvable* ("computationally tractable"), if it admits a polynomial time solution algorithm.

The standard informal interpretation of polynomiality is that with solution time fixed, a 10-fold progress in computer's performance allows for both (a) a *constant factor* progress in the sizes of instances which can be solved to a given accuracy, and (b) a *constant factor* progress in the number of accuracy digits to which an instance of a given size can be solved. (a), (b) compare favourably polynomial time algorithms with methods suffering from "curse of dimensionality" ($N(p, \varepsilon)$ can grow with $\mathrm{Size}(p)$ as $\exp\{\mathrm{Size}(p)\}$), same as with sublinearly converging methods ($N(p, \varepsilon)$ can grow as $1/\varepsilon^c$, $c > 0$, when $\varepsilon \to 0$).

1.2. Convex programming – solvable case of MP. At the early 1980s it became clear that what forms the "efficiently solvable case" in MP, is *convex programming* – programs (1) with convex objective and constraints. Specifically, it was proved that *generic convex problems, under mild computability and boundedness assumptions, are polynomially solvable.* In contrast to this, *no efficient algorithms for typical generic non-convex problems are known, and there are strong reasons to believe that no such algorithms exist* (e.g., programs with quadratic objective and constraints are not polynomially solvable unless P = NP).

Here is a basic example of a "convex programming solvability statement" (cf. [8, Theorem 5.3.1]):

Theorem 1.1. *A generic MP problem $\mathcal{P}$ with convex instances is polynomially solvable, provided it possesses the following properties:*

(i) (Polynomial computability) *There exists an algorithm $\mathcal{O}$ which, given on input* $\mathrm{Data}(p)$*, a point $x \in \mathbb{R}^{n(p)}$ and a tolerance $\delta > 0$, computes in polynomial in* $\mathrm{Size}(p)$ *and* $\mathrm{Digits}(p, \delta)$ *number of a.o. δ-accurate approximations to the values and subgradients of the objective and the constraints of p at x.*

(ii) (Polynomial growth)

$$\max_{0\le i\le m(p)} |f_i^{(p)}(x)| \le \left(\chi[\mathrm{Size}(p) + \|\mathrm{Data}(p)\|_1 + \|x\|_1]\right)^{\chi\,\mathrm{Size}^\chi(p)}$$

for all x (here and below χ is an instance-independent constant).

(iii) (Polynomial boundedness of feasible sets) *If x is feasible for an instance p, then $\|x\|_1 \le (\chi[\mathrm{Size}(p) + \|\mathrm{Data}(p)\|_1])^{\chi\,\mathrm{Size}^\chi(p)}$.*

Note that in fact (i) can be weakened to the possibility to compute in polynomial in $\mathrm{Size}(p)$ and $\mathrm{Digits}(p,\delta)$ time δ-approximations solely to the values of the objective and the constraints at x.

Polynomial time solvability results like the one stated by Theorem 1.1 are based upon existence of linearly converging *black box oriented* methods for solving general-type convex programs, i.e., methods which work solely with local information on the program – the values and the subgradients of $f_0, f_1, \ldots, f_m$ at successively generated *search points*, with no direct access to program's data. Historically, the first method of this type was the ellipsoid algorithm proposed independently in [43] and [65] (for detailed study of the algorithm and its theoretical consequences, see [26]), and the corresponding result is as follows.

Theorem 1.2. *Let* (1) *be a convex program with n variables, and let the feasible set $X = \{x : f_i(x) \le 0,\ i \ge 1\}$ be contained in the ball $B = \{x : \|x\|_2 \le R\}$ and contain a ball of radius $r > 0$, with R, r known. Assume that we have an access to*

- *a first order oracle $\mathcal{O}$ capable to compute the value $f_0(x)$ and a subgradient $f_0'(x)$ at every given point $x \in B$;*
- *a separation oracle $\mathcal{S}$ which, given on input a point $x \in B$, reports whether $x \in X$, and if it is not the case, returns a linear form which separates x and X.*

In this environment, certain explicit algorithm (the ellipsoid method) finds, for every accuracy $\varepsilon > 0$, a feasible ε-solution to (1) *at the cost of no more than*

$$N(\varepsilon) \le \mathrm{Ceil}\left(2n^2\left[\log(R/r) + \ln\left(1 + \mathrm{Var}_B(f_0)/\varepsilon\right)\right]\right) + 1,$$

$$\mathrm{Var}_B(f_0) = \max_B f_0 - \min_B f_0$$

subsequent calls to $\mathcal{O}$ and $\mathcal{S}$ plus $O(1)n^2$ a.o. per call to process oracle's answer.

In spite of their crucial role in demonstrating polynomial solvability of convex programming, black-box-oriented techniques like the ellipsoid method are too slow to be of actual practical interest; indeed, for all known methods of this type, the computational effort per accuracy digit grows with the design dimension n *at least* as $O(n^4)$, which, in reality, makes it problematic to process already medium-scale (few hundreds of variables) convex programs. This contrast between theoretical properties and practical performance is especially sharp in LP: on the theoretical side, the ellipsoid method allowed to resolve affirmatively the long-standing problem of whether

LP with rational data admits a CCT-polynomial time solution algorithm (Khachiyan [34], 1979), while practical performance of the method in LP is incomparably worse than the one of the "theoretically bad" (with exponential in the size of an LP program worst-case complexity) simplex method. Comparing extremely powerful in practice simplex method with its black-box-oriented rivals, it is easy to guess from where the weakness of the rivals comes: the simplex method fully utilizes the rich structure of an LP program and works directly on program's data, which is not the case with "nearly blind" black-box-oriented algorithms. Note, however, that while in reality a convex program usually has a lot of structure (otherwise, how could we know that the program is convex?), the standard way to think about nonlinear convex programs, suggested by representation (1), made it extremely difficult to reveal and to utilize this structure. In retrospect, tremendous developments in convex programming during what is called "Interior Point Revolution" (started in 1984 when Karmarkar [33] invented his famous practically efficient polynomial time algorithm for LP) were mainly focused on finding and utilizing novel "structure revealing" representations of convex programs, most notably, in the form of *conic programs*.

Remark 1.3. A "classically oriented" mathematician might be surprised by the attention we pay to representation issues. Indeed, finally an optimization problem is to minimize a function over a set; why should we bother about representations of these, completely transparent by themselves, entities? The answer is, that an algorithm cannot work with abstract entities, it can work only with their representations, and different representations of the same entities may be of completely different "algorithmic value".

1.3. Conic programs. When passing from a linear programming program

$$\min_x \left\{c^T x : Ax - b \geq 0\right\} \tag{2}$$

to its nonlinear extensions, the most natural way is the one used in MP – to replace the linear objective $c^T x$ and left hand sides $[Ax - b]_i$ in the constraints with nonlinear ones, thus arriving at (1). As far as convex programming is concerned, there is an equivalent, less trivial and, as it turns out, much more convenient way to introduce nonlinearity, namely, replacing the standard coordinate-wise vector inequality

$$a \geq b \Longleftrightarrow a - b \geq 0 \Longleftrightarrow a - b \in \mathbb{R}^m_+ = \{y \in \mathbb{R}^m : y_i \geq 0,\ i = 1, \ldots, m\}$$

with another "good" vector inequality given by a subset $K \subset \mathbb{R}^n$ according to

$$a \geq_K b \Longleftrightarrow a - b \geq_K 0 \Longleftrightarrow a - b \in K.$$

The evident necessary and sufficient condition for the resulting binary relation to be a partial order compatible with linear operations on $\mathbb{R}^m$ is for $K \subset \mathbb{R}^m$ to be a nonempty convex pointed ($K \cap (-K) = \{0\}$) cone. From the analytical perspective, it makes sense also to require from K to be closed with a nonempty interior. Given a *regular*

(convex, pointed, closed and with a nonempty interior) cone K, we define a *conic program on* K as the optimization program

$$\min_x \left\{ c^T x : \underbrace{Ax - b \geq_K 0}_{\Leftrightarrow Ax-b\in K} \right\} \tag{CP}$$

Preliminary observations about this representation are that (a) in (CP), it is easy to distinguish between the "structure" (given by the cone K) and the data (c, A, b), and (b) independently of values of the data, (CP) is a problem of optimizing a linear objective over a convex set, and thus is a convex problem (thus, the convexity in (CP) is "built in", while in (1) it should be "added from outside"). At the same time, it is easily seen that every convex program can be represented in the form of (CP). By themselves, (a), (b) do not say much in favour of conic representation of a convex program as compared to its MP form – a general-type convex cone is not a "better structured" entity than a general-type convex function. The crucial advantage of conic representation is that it possesses outstanding "unifying abilities" – as a matter of fact, just 3 families of cones allow to represent an extremely wide spectrum of convex programs. These 3 families are

$\mathcal{LP}$: nonnegative orthants $\mathbb{R}^m_+$ giving rise to LP programs (2),

$\mathcal{CQP}$: finite direct products of Lorentz cones $\boldsymbol{L}^{k+1} = \{(y, t) \in \mathbb{R}^{k+1} = \mathbb{R}^k \times \mathbb{R} : t \geq \|y\|_2\}$; the MP form (1) of the resulting *conic quadratic* programs is

$$\min_x \left\{ c^T x : \|A_i x - b_i\|_2 \leq c_i^T x - d_i,\ i = 1, \ldots, m \right\}, \tag{3}$$

where A_i, b_i, c_i, d_i are matrices and vectors of appropriate dimensions. A constraint $\|Ax - b\|_2 \leq c^T x - d$ is called a CQI (Conic Quadratic Inequality);

$\mathcal{SDP}$: direct products of semidefinite cones $\boldsymbol{S}^m_+$. $\boldsymbol{S}^m_+$ is the cone of positive semidefinite (psd) matrices in the Euclidean space $\boldsymbol{S}^m$ of real symmetric $m \times m$ matrices equipped with the Frobenius inner product $\langle A, B\rangle = \mathrm{Tr}(AB)$. The resulting *semidefinite* programs (sdp's) are of the form

$$\min_x \left\{ c^T x : \mathcal{A}_i x - B^i \equiv x_1 A^i_1 + \cdots + x_n A^i_n - B^i \succeq 0,\ i = 1, \ldots, m \right\}, \tag{4}$$

where A^i_j, $B^i \in \boldsymbol{S}^{k_i}$ and $A \succeq B$ means that $A - B$ is psd. A constraint $\sum_i x_i A_i - B \succeq 0$ is called LMI (Linear Matrix Inequality).

It is immediately seen that $\mathcal{LP} \subset \mathcal{CQP} \subset \mathcal{SDP}$; indeed, a linear inequality is a particular case of CQI, which, in turn, is a particular case of LMI due to $(y, t) \in \boldsymbol{L}^{k+1}$ iff $\begin{bmatrix} t & y^T \\ y & tI_k \end{bmatrix} \succeq 0$.

In the sequel, we intend to overview the main elements of the theory of conic programming, specifically, (1) duality, (2) interior point polynomial time algorithms, and (3) "expressive abilities" and applications.

2. Conic duality

Duality in optimization stems from the desire to find a systematic way to bound from below the optimal value of a minimization problem; it turns out that a good answer to this question is crucial for building optimality conditions, solution algorithms, etc. As applied to MP, the standard *Lagrangian duality* associates with (1) the Lagrange function $L(x,\lambda) = f_0(x) + \sum_{i=1}^m \lambda_i f_i(x)$ and observes that whenever $\lambda \geq 0$, one has $L_*(\lambda) = \inf_x L(x,\lambda) \leq \mathrm{Opt}$; thus, we get a family $L_*(\lambda)$, $\lambda \geq 0$, of (computable under favourable circumstances) lower bounds on Opt and can now associate with (1) the *dual problem* $\max_{\lambda\geq 0} L_*(\lambda)$ of finding the best lower bound available from the outlined mechanism. *When* (1) *is convex* and satisfies mild additional assumptions[1)], the dual problem is solvable with the optimal value Opt ("strong duality"). In the case of (CP), essentially the same Lagrange recipe results in the dual problem of the form

$$\max_{\lambda} \left\{ b^T\lambda : A^T\lambda = c, \lambda \geq_{K_*} 0 \right\}, \tag{D}$$

where $K_* = \{\lambda : \lambda^T\xi \geq 0 \text{ for all } \xi \in K\}$ is the cone dual to K (and thus regular along with K). (D) again is a conic problem, and in fact the duality is fully symmetric. Indeed, assuming the columns of A to be linearly independent (which in fact does not restrict generality), we can pass in (CP) from original variables x to *primal slack* $\xi = Ax - b$, ending up with equivalent *primal* reformulation

$$\min_{\xi} \left\{ d^T\xi : \xi \in [\mathcal{L} - b] \cap K \right\} \quad \left[\mathcal{L} = \mathrm{Im}A,\ d : A^Td = c \right] \tag{Pr}$$

of (CP) as a problem of minimizing a linear objective over the intersection of a cone and an affine plane. Observe that the linear constraints in (D) read $A^T\lambda = c = A^Td$, or, equivalently, $\lambda \in \mathrm{Ker}\, A^T + d = \mathcal{L}^\perp + d$. Thus, (D) is the problem

$$\max_{\lambda} \left\{ b^T\lambda : \lambda \in [\mathcal{L}^\perp + c] \cap K_* \right\} \tag{Dl}$$

of the geometry completely similar to the one of (Pr). Moreover, $(\mathcal{L}^\perp)^\perp = \mathcal{L}$ and $(K_*)_* = K$, so that the problem dual to (Dl) is exactly (Pr) – the duality indeed is symmetric. The "notational difference" between (CP) and (D) comes from the fact that in (CP) we represent a geometric entity (affine subspace $\mathcal{L} - b$) as the image of an affine embedding, while in (D) a similar entity is represented as the solution set of a system of linear equations. The relations between the primal and the dual problem are summarized in the following theorem (see, e.g., [45], [1], [46]):

Theorem 2.1. *Assuming A in* (CP) *is of full column rank, the following is true:*

(i) *The duality is symmetric:* (D) *is a conic problem, and the conic dual to* (D) *is* (*equivalent to*) (CP).

[1)] The standard assumptions are the existence of a feasible solution where all nonlinear constraints are satisfied as strict inequalities and below boundedness of the objective on the feasible set.

(ii) (Weak duality) $\mathrm{Opt(D)} \leq \mathrm{Opt(CP)}$.

(iii) (Strong duality) *If one of the programs* (CP), (D) *is bounded and strictly feasible* (i.e., the corresponding affine plane intersects the interior of the associated cone)*, then the other is solvable and* $\mathrm{Opt(CP)} = \mathrm{Opt(D)}$. *If both* (CP), (D) *are strictly feasible, then both programs are solvable and* $\mathrm{Opt(CP)} = \mathrm{Opt(D)}$.

(iv) (Optimality conditions) *Assume that both* (CP), (D) *are strictly feasible. Then a pair* (x, λ) *of feasible solutions to the problems is comprised of optimal solutions iff* $c^T x = b^T \lambda$ (*"zero duality gap"*)*, same as iff* $\lambda^T [Ax - b] = 0$ (*"complementary slackness"*).

It is highly instructive to compare Lagrange duality with its "particular case" – conic duality. The general Lagrange duality is "asymmetric" (in general, $\mathcal{L}_*(\cdot)$ "does not remember" the underlying program (1)) and usually results in *implicitly given* dual problem. In contrast to this, conic duality is "fully algorithmic" – building a dual problem is a simple purely mechanical process – and completely symmetric. As it turns out, these advantages make conic duality an extremely useful tool in processing, analytical as well as computational, of conic programs.

Finally, conic duality looks completely similar to the standard LP duality, with the only exception that in the LP case strong duality is ensured by mere feasibility and not a strict one. For "good" cones, like those associated with $\mathcal{CQP}$ and $\mathcal{SDP}$, there exist more advanced (still "fully algorithmic", although non-symmetric) version of duality [59] which is free of this shortcoming – whenever the primal optimal value is finite, the dual is solvable with the same optimal value.

While conic programming and conic duality as "well-established" research subjects arose in early 1990s, initially due to the desire to extend Karmarkar's polynomial time LP algorithm to the non-polyhedral case, there are wonderful earlier examples of using what is now called semidefinite duality (by Lovasz [40] in connection with his famous θ-function, by A. Shapiro [64] in connection with certain statistical problems, and perhaps more…)

In hindsight, Conic Duality Theorem can be traced to at least as early as 1958, namely, to written by L. Hurwicz chapter 4 of [5] (see [5], Corollary IV.3). Unfortunately, this paper, aimed at infinite-dimensional extensions of the optimality conditions in the "usual" (finite-dimensional) convex programming, overlooks the symmetric conic duality itself – the latter is, essentially, a finite-dimensional phenomenon. To the best of our knowledge, the remarkable paper in question made no "observable" impact on the development of mathematical programming and now is nearly completely forgotten.

3. Interior point polynomial time methods in conic programming

Conic programs are convex, and thus the issue of their polynomial time solvability can be resolved via the general results presented in Section 1.2; modulo minor

technicalities, in order to ensure polynomial time solvability of a generic conic problem, it suffices for the associated cones to be "computationally tractable" (to admit polynomial time membership/separation oracles), and for the instances – to include upper bounds on the norms of candidate solutions. For example, $\mathcal{LP}/\mathcal{CQP}/\mathcal{SDP}$ problems *with bounds* $\|x\|_\infty \equiv \max_i |x_i| \leq R$ *on variables* [2)], are polynomially solvable. The point, however, is that *conic programs associated with "good" cones admit much faster polynomial time algorithms than those coming from black-box-oriented techniques like the ellipsoid method.* The first "really fast" (and completely non-traditional) polynomial time algorithm for LP was discovered by Karmarkar in 1984 [33]; the subsequent intensive research in the emerging area of *interior point* (IP) *polynomial time algorithms* for LP resulted, among other things, in developing much more transparent (and theoretically even more efficient) than Karmarkar's method polynomial time algorithms for LP (Renegar, 1986 [60]; Gonzaga [24]) and brought the area in a position where non-polyhedral extensions became possible. These extensions, primarily due to Yu. Nesterov, led to a general theory of polynomial time IP methods in convex programming [46]. We start with outlining the basic elements of the theory and then will overview briefly the current state of this area.

3.1. Basics on IP methods. The starting point in all IP constructions is a well-known *interior penalty scheme* for solving a convex program

$$\min_{x \in X} c^T x \tag{P}$$

where $X \subset \mathbb{R}^n$, $\operatorname{int} X \neq \emptyset$, is closed and convex. The scheme, going back to Fiacco and McCormic [19], is to equip X with an *interior penalty* – a smooth and strictly convex function $F(x)\colon \operatorname{int} X \to \mathbb{R}$ which blows up to ∞ along every sequence $x_i \in \operatorname{int} X$ converging to a boundary point of X – and to associate with (P) a parametric optimization problem

$$x_*(t) = \operatorname{argmin}_{x \in \operatorname{int} X} F_t(x), \quad F_t(x) = tc^T x + F(x).$$

Under mild assumptions, the *central path* $x_*(t)$ is well-defined for $t > 0$ and converges to the optimal set of (P) as $t \to \infty$. In the interior penalty scheme, one "traces" this path by generating iterates (x_i, t_i) such that $x_i - x_*(t_i) \to 0$ and $t_i \to \infty$ as $i \to \infty$. Specifically, given (x_i, t_i) with x_i "close" to $x_*(t_i)$, one increases somehow t_i, thus getting t_{i+1}, and then applies a whatever method of unconstrained minimization to the function $t_{i+1}c^T x + F(x)$, starting the method at x_i, to get a "tight" approximation x_{i+1} to the minimizer $x_*(t_{i+1})$ of this function. A standard "working horse" here is the Newton method, commonly believed to be the fastest method for unconstrained minimization.

Self-concordance. The traditional theory of the Newton method (and all other methods of unconstrained minimization, for this matter) did not suggest polynomiality of

[2)] These bounds clearly do not affect the possibility to represent a problem as an $\mathcal{LP}/\mathcal{CQP}/\mathcal{SDP}$.

the outlined path-following scheme, vice versa, it predicted inevitable slowing down of the path-tracing process. It turned out that there exist interior penalty functions – *self-concordant barriers* – which do allow for polynomial time path-tracing, and that the associated *self-concordant-based* theory of IP methods [46] allows to explain all IP methods previously developed for LP and to extend them onto non-polyhedral convex case. Specifically, an interior penalty function F is called a *ϑ-self-concordant barrier* (ϑ-s.c.b.) for X, if F is C^3 and convex on int X and satisfies, for all $x \in \operatorname{int} X$, $h \in \mathbb{R}^n$, the differential inequalities

$$|D^3F(x)[h,h,h]| \le 2\left(D^2F(x)[h,h]\right)^{3/2} \qquad \text{(self-concordance)} \tag{5a}$$

$$|DF(x)[h]| \le \sqrt{\vartheta}\left(D^2F(x)[h,h]\right)^{1/2} \qquad \text{(barrier quantification)} \tag{5b}$$

which can be interpreted as follows: the convex function F at a point defines a "local" Euclidean norm $\|h\|_{x,F} = \sqrt{D^2F(x)[h,h]}$ on $\mathbb{R}^n$; self-concordance (5a) means that the Hessian of F is Lipschitz continuous, with constant 2, w.r.t. to the corresponding local metric, while (5b) says that F itself is Lipschitz continuous, with constant $\sqrt{\vartheta}$, in this metric.

Self-concordance-based path-tracing. It turns out that self-concordant functions – those satisfying (5a) alone – are extremely well suited for Newton minimization, which ensures nice properties of the "centering" $x_i \mapsto x_{i+1}$ in the path-tracing, while (5b) is responsible for the possibility to increase penalty parameter t at a constant rate, thus avoiding slowing down. The bottom line is as follows: assume that X does not contain lines, the level sets $\{x \in X : c^Tx \le a\}$ are bounded, and that F is ϑ-s.c.b. Then $x_*(t)$ is well-defined and $\nabla^2F(x) \succ 0$ on int X, so that the *Newton decrement* $\lambda(x,t) = \sqrt{\nabla F_t^T(x)[\nabla^2F_t(x)]^{-1}\nabla F_t(x)}$ *of* F_t *at* $x \in \operatorname{int} X$ is well-defined; note that $x_*(t)$ is characterized by $\lambda(x,t) = 0$. Let us say that x is close to $x_*(t)$, if $\lambda(x,t) \le 0.1$. Given a starting point (x_0,t_0) with $t_0 > 0$ and x_0 close to $x_*(t_0)$, consider the path-tracing scheme

$$\begin{bmatrix} t_i \\ x_i \end{bmatrix} \mapsto \begin{bmatrix} t_{i+1} = (1+0.1\vartheta^{-1/2})t_i \\ x_{i+1} = x_i - \frac{1}{1+\lambda(x_i,t_{i+1})}[\nabla^2F_{t_{i+1}}(x_i)]^{-1}\nabla F_{t_{i+1}}(x_i) \end{bmatrix}. \tag{6}$$

Then the process is well-defined, ensures closeness of x_i and $x_*(t_i)$ and the relation

$$c^Tx_i - \min_X c^Tx \le 2\vartheta/t_i \le 2\exp\left\{-0.05i\vartheta^{-1/2}\right\}\vartheta t_0^{-1}.$$

Thus, the path-tracing scheme (6) with a *single* Newton-like step per updating the penalty converges linearly, and it takes $O(\sqrt{\theta})$ iterations to get an extra accuracy digit. Of course, to run the outlined scheme, we should once come close to the central path; this can be done by applying the same path-tracing technique to an appropriate auxiliary problem. It follows that *if we are smart enough to equip the feasible domains*

of instances (written in the form of (P)) *of a generic convex problem $\mathcal{P}$ with self-concordant barriers computable, along with their first and second order derivatives, in time polynomial in the size of an instance, and the parameters ϑ of these barriers are bounded by a polynomial of instance's size, then the outlined path-tracing scheme provides a polynomial time algorithm for $\mathcal{P}$.*

As about being "smart enough" to equip generic convex problems with "good" s.c.b.'s, the situation is as follows. *In principle*, every closed convex set $X \subset \mathbb{R}^n$, $\operatorname{int} X \neq \emptyset$, admits an $O(1)n$-s.c.b.; assuming w.l.o.g. that X does not contain lines, this *universal barrier* is $F(x) = O(1) \ln \operatorname{mes}_n(P_x)$, where $P_x = \{y : y^T(z - x) \leq 1 \text{ for all } z \in X\}$ is the polar of X w.r.t. x [46]. In the case when X is a cone, this construction results in the logarithm of the *characteristic function* $F(x) = \int_{K_*} \exp\{-x^T y\} dy$ of the cone K_* [27]. This existence theorem has restricted algorithmic content, since the universal barrier rare is efficiently computable. There exists, however, a simple "calculus" of s.c.b.'s [46] which shows that basic convexity-preserving operations with sets, e.g., taking intersections, direct products, affine images and inverse affine images (as well as taking inverse images under specific non-linear mappings, most notably a kind of Siegel domain construction) can be equipped with simple rules which allow to combine s.c.b.'s for the operands into an s.c.b. for the resulting set. E.g., summing up ϑ_i-s.c.b.'s for sets X_i, $i = 1, \ldots, m$, we get a $\left(\sum_i \vartheta_i\right)$-s.c.b. for the intersection of the sets; superposition $F(Ax + b)$ of a ϑ-s.c.b. F with affine mapping is ϑ-s.c.b. for the inverse image of the domain of F under the mapping, etc. These and more advanced "calculus rules" allow to build "from scratch" (from the only observation that the function $-\ln t$ is 1-s.c.b. for $\mathbb{R}_+$) explicit efficiently computable s.c.b.'s with moderate values of the parameter for a wide variety of interesting convex sets. This family includes the cones underlying $\mathcal{LP}$, $\mathcal{CQP}$, $\mathcal{SDP}$, $\|\cdot\|_p$-cones $\{(x, t) : \|x\|_p \leq t\}$, feasible sets of geometric programming programs, intersections, direct products, affine and inverse affine images of the above, and much more. The related *empirical* observation is that all generic polynomially solvable convex problems arising in applications admit "good" explicit s.c.b.'s, and that the outlined scheme is the source of the best known so far complexity bounds and polynomial time algorithms for these generic problems.

Aside of their role in constructing polynomial time algorithms, s.c.b.'s seem to be pretty interesting entities by their own right – their properties are closely related to the geometry of their domains. E.g., a closed convex domain X not containing lines is bounded if and only if (any, and then all) s.c.b. F for X attains it minimum on $\operatorname{int} X$, let the (automatically unique) minimizer be $\bar{x}$. When it is the case, the *Dikin ellipsoid* $D_{\bar{x}} = \{x : \|x - \bar{x}\|_{\bar{x},F} \leq 1\}$ of F gives an $O(\vartheta)$-*rounding* of X: $D_{\bar{x}} \subset X \subset \{x : \|x - \bar{x}\|_{\bar{x},F} \leq \vartheta + 2\sqrt{\vartheta}\}$ ([46], [32]; note that $D_{\bar{x}} \subset X$ for all $\bar{x} \in \operatorname{int} X$, not only when $\bar{x}$ is a minimizer of F [46]). This combines with elementary facts of barrier calculus to imply, e.g., the following: *if the intersection of m ellipsoids in $\mathbb{R}^n$ has a nonempty interior, it is in-between two efficiently computable concentric similar ellipsoids with similarity ratio not exceeding $m + 2\sqrt{m}$.* We are not aware of a direct proof of this, useful in some applications, geometric fact.

Path-tracing and Riemannian geometry. An s.c.b. F defines a Riemannian structure on its domain $X^o = \{x : F(x) < \infty\}$, the metric tensor being $\nabla^2 F(x)$. Various *short step* interior point methods associated with F can be described as follows: in order to solve (P), the method generates a sequence of points $x_i \in X^o$ such that (a) the Riemannian distance from x_i to x_{i+1} does not exceed an absolute constant, say, 0.2, and (b) the shift $x_{i+1} - x_i$ is defined solely in the "local" terms – in terms of the objective c and the quantities $F(x_j)$, $\nabla F(x_j)$, $\nabla^2 F(x_j)$, $0 \le j \le i$ (cf. (6)). The complexity of such a method is quantified by the number of steps required to reach the set $X^o_\varepsilon = \{x \in X^o : c^T x - \inf_{x' \in X^o} c^T x' \le \varepsilon\}$ of ε-solutions to (P). Clearly, the complexity of a short step method is below bounded by the Riemannian distance from x_0 to X^o_ε. Ideally, we would like to have the complexity within an absolute constant factor of this "ultimate" lower bound; it, however, is unclear how to build such a method – how to describe the shortest path from x_0 to X^o_ε in local terms? (cf. climbing a mountain in a fog and without map). It can be proved [55] that the short step path-following method (6) is not that far from being ideal: its performance is within the factor $O(1)\vartheta^{1/4}$ of the lower bound, provided that X^o is bounded and x_0 is close to argmin F.

3.2. Interior point methods in conic programming. Barriers especially well-suited for conic problems are *ϑ-logarithmically homogeneous* s.c.b.'s, that is, C^3 convex functions F: int $K \to \mathbb{R}$, K being a regular cone, satisfying (5a) and the identity $F(tx) = F(x) - \vartheta \ln t$, $t > 0$. This implies that F is a ϑ-s.c.b. for K and that the *conjugate barrier* $F_*(y) = \max_x \left[-y^T x - F(x)\right]$ is a ϑ-logarithmically homogeneous s.c.b. for K_*; the mappings $x \mapsto -\nabla F(x)$, $y \mapsto -\nabla F_*(y)$ turn out to be inverse to each other one-to-one correspondences between int K and int K_*. Given a pair of strictly feasible primal-dual conic problems (Pr), (Dl) and a pair of conjugate to each other ϑ-logarithmically homogeneous s.c.b.'s F, F_* for the cones K, K_*, one can develop *primal-dual* interior point methods simultaneously solving (Pr), (Dl). The most popular *primal-dual path-following scheme* is as follows. When both (Pr) and (Dl) are strictly feasible, the corresponding primal and dual central paths $\xi_*(t) = \text{argmin}\left[td^T\xi + F(\xi) : \xi \in \mathcal{L} - b\right]$ and $\lambda_*(t) = \text{argmin}\left[-tb^T\lambda + F_*(\lambda) : \lambda \in \mathcal{L}^\perp + d\right]$ are well-defined and linked to each other: $\lambda_*(t) = -t^{-1}\nabla F(\xi_*(t))$, $\xi_*(t) = -t^{-1}\nabla F_*(\lambda_*(t))$, and one can apply Newton-based path-tracing to the *primal-dual* central path $(\xi_*(t), \lambda_*(t))$, thus solving (Pr) and (Dl) simultaneously. It turns out that processing both problems together has a lot of advantages, allowing, e.g., for

• on-line adjustable "long step" policies [47] which are less conservative than the worst-case-oriented policy (6) and thus exhibit much better practical performance, while still ensuring the theoretical complexity bounds,

• an elegant way ("self-dual embedding", see, e.g., [72], [77], [4], [42], [35], [58]) to initialize the path-tracing even in the case when no feasible solutions to (Pr) and (Dl) are available in advance,

• building certificates of strict (i.e., preserved by small perturbations of the data) primal or dual infeasibility [51] when it is the case, etc.

It should be added that the primal-dual central path $(\xi_*(\cdot), \lambda_*(\cdot))$ is "nearly geodesic" w.r.t. the Riemannian structure on the primal-dual feasible set given by the metric tensor $\nabla^2(F(\xi) + F_*(\lambda))$: the Riemannian length of every segment of the path is within factor $\sqrt{2}$ of the Riemannian distance between the endpoints of the segment [54].

3.3. The case of symmetric cones: LP/CQP/SDP. Interior point constructions achieve maximal flexibility for cones with a lot of symmetries, most notably for *symmetric cones* – those which are homogeneous (i.e., the group of linear automorphisms of the cone acts transitively on its interior) and self-dual w.r.t. an appropriate Euclidean structure on the embedding space. Classification theory due to Vinberg [71] says that all symmetric cones are direct products of irreducible ones, specifically, Lorentz cones, real semidefinite cones (in particular, nonnegative rays), the cones of Hermitian psd complex matrices, the cones of Hermitian psd quaternion matrices, and, finally, copies of exceptional 27-dimensional octonian cone. The latter 3 cones are cross-sections of the semidefinite cone of "the same" (within factor 4) real dimension and therefore do not add much, as far as the associated families of conic problems are concerned; therefore we lose nearly nothing when focusing on the cones which are direct products of Lorentz and semidefinite cones, thus arriving at problems of minimizing linear objective under a mixture of conic quadratic and LMI constraints (the latter include also linear constraints which are merely 1-dimensional LMI's). Now, we can equip a direct product $K = K_1 \times \cdots \times K_m$ of Lorentz and semidefinite cones with the *canonical* logarithmically homogeneous s.c.b. $F(x^1, \ldots, x^m) = \sum_i F_i(x^i)$, the barriers for the Lorentz factors $K_i = \{x^i = (u_i, s_i) : s_i \geq \|u_i\|_2\}$ being $F_i(x^i) = -\ln(s_i^2 - u_i^T u_i)$ ($\vartheta = 2$) and the barriers for the semidefinite factors $K_i = \boldsymbol{S}_+^{m_i}$ being $F_i(x^i) = -\ln\det x^i$ ($\vartheta = m_i$). The parameter of the resulting barrier is the sum of those of the components, i.e., it is twice the number of Lorentz factors plus the total row size of the semidefinite ones. The canonical barrier F respects the symmetries $x \mapsto Ax$ of the underlying cone ($F(Ax) = F(x) + \text{const}(A)$) and its self-duality ($F_*(x) = F(x) + \text{const}$) and possesses a number of advanced properties which can be utilized in the interior point algorithms, e.g., in developing long-step policies. Discovery of these properties and the ways to utilize them in the IP context by Nesterov and Todd [48], [49] was one of the most important breakthroughs in developing of IP theory and algorithms.

It should be noted that the theory of IP methods on symmetric cones is one of few (alas!) "avenues of contact" of convex optimization and modern mathematics, specifically, the theory of Euclidean Jordan algebras; the latter turned out to be a natural way to treat the IP methods on symmetric cones, see [62], [63], [17], [18], [29] and references therein. Another such avenue is the theory of hyperbolic polynomials originating from PDEs. Recall that a real homogeneous, of a degree m, polynomial $p(\cdot)$ on $\mathbb{R}^n$ is called *hyperbolic* in a direction d, $p(d) > 0$, if the univariate polynomial $\phi(t) = p(x + td)$ has all its roots real whenever $x \in \mathbb{R}^n$. It is well known that the component of d in the set $p(\cdot) > 0$ is the interior of a closed convex cone K – the

hyperbolicity cone of p. As discovered in [28], $-\ln\det p(x)$ is an m-logarithmically homogeneous s.c.b. for K with a number of useful properties mimicking those of canonical barriers (the latter are built from logs of specific hyperbolic polynomials $\det(x)\colon \boldsymbol{S}^m \to \mathbb{R}$ and $x_{k+1}^2 - \sum_{i=1}^k x_i^2 \colon \mathbb{R}^{k+1} \to \mathbb{R}$). For further links between convex optimization and hyperbolic polynomials, see [6], [31] and references therein.

We conclude this section with complexity bounds for generic LP/CQP/SDP problems with bounds on variables. For all these problems, the complexity of building ε-solution, measured both in the number of IP iterations and in the total number of a.o., is proportional to the required number of accuracy digits $\mathrm{Digits}(\cdot, \varepsilon)$, so that we can speak about "number of iterations/a.o. per accuracy digit"; these are the complexity characteristics to be indicated below.

LP: for an LP program $\min_{x\in\mathbb{R}^n}\{c^T x : Ax \geq b \in \mathbb{R}^m, \|x\|_\infty \leq R\}$, the size is $O(mn)$, and the complexity is $O(1)\sqrt{m+n}$ IP iterations and $O(1)(m+n)^{3/2}n^2$ a.o. per accuracy digit. With smart implementation of subsequent Newton steps ("Karmarkar acceleration"), the # of a.o. per accuracy digit can be reduced to $O(1)[(m+n)n^2 + m^{1.5}n]$ (see [60]); thus, to find an ε-solution to an LP with $m \leq O(n^2)$ is, up to factor $\ln(1/\varepsilon)$, not more difficult than to find the least squares solution to a system of $m+n$ linear equations with n unknowns;

CQP: for a CQP $\min_{x\in\mathbb{R}^n}\{c^T x : \|A_i x - b_i\|_2 \leq c_i^T x - d_i,\ i \leq m,\ \|x\|_2 \leq R\}$ with $k_i \times n$ matrices A_i, the size is $O(n\sum_i k_i)$, and the complexity is $O(1)\sqrt{m}$ IP iterations and $O(1)m^{1/2}n\left(mn + n^2 + \sum_i k_i\right)$ a.o. per accuracy digit (provided the matrices $A_i^T A_i$ are computed in advance).

SDP: for an sdp $\min_{x\in\mathbb{R}^n}\{c^T x : \sum_j x_j A_j^i - B^i \succeq 0,\ i \leq m, \|x\|_2 \leq R\}$ with $k_i \times k_i$ matrices A_j^i, the size is $O(n\sum_i k_i^2)$, and the complexity is $O(1)\sqrt{\sum_i k_i}$ IP iterations and $O(1)\sqrt{\sum_i k_i}\,n(n^2 + n\sum_i k_i + \sum_i k_i^3)$ a.o. per accuracy digit.

Empirical behaviour of well-implemented IP methods is better than the one predicted by the worst-case theoretical analysis. Theoretically, iteration count in LP and SDP should be $O(\sqrt{m})$, where m is the number of linear constraints in LP and is the total row size of LMIs in SDP. In reality, no essential growth of the iteration count with m is observed, and a high accuracy solutions are found in something like 30–50 iterations. What limits the practical scope of IP methods is the complexity of a single iteration where a Newton-type system of n linear equations with n unknowns is formed and solved, n being the design dimension of the program. With $n \sim 10^4$ and more, solving Newton system in reasonable time is possible only when it is highly sparse; the latter is usually the case with real-world LP's, but typically is not the case with sdp's.

4. Expressive abilities and applications of LP/CQP/ SDP

As we have already mentioned, the IP machinery is especially well suited for solving conic problems on symmetric cones, which makes it natural to ask: when a convex

program can be reformulated as a conic program on such a cone, specifically, as an LP/CQP/SDP program? Usually, the original formulation of a convex program is in (or can be immediately converted to) the form

$$\min_{x\in X} c^T x, \quad X = \bigcap_{i=1}^{m} X_i, \tag{7}$$

where X_i are convex sets, most typically given as the level sets of convex functions: $X_i = \{x : f_i(x) \le 0\}$. What we need are tools to recognize that (7) can be reformulated as, say, an sdp, and to build such a reformulation when possible, and we start with an overview of the corresponding "toolkit".

4.1. Calculus of LP/CQP/SDP-representable sets and functions. Let $\mathcal{K}$ be a family of regular cones closed w.r.t. passing from a cone to its dual and closed w.r.t. taking direct products; note that these properties are shared by the families $\mathcal{LP}/\mathcal{CQP}/\mathcal{SDP}$. Let us ask ourselves when program (7) can be reformulated as a *$\mathcal{K}$-program* – a conic program on a cone from $\mathcal{K}$. A natural (and somehow tautological) answer is: *it suffices for X to be a $\mathcal{K}$-representable set* ("$\mathcal{K}$-s." for short), meaning that there exists a *$\mathcal{K}$-representation* ("$\mathcal{K}$-r.") of X:

$$X = \{x \in \mathbb{R}^n : \text{ there exists } u \in \mathbb{R}^m \text{ such that } A(x,u) \succeq_K 0\}, \tag{8}$$

where $K \in \mathcal{K}$ and $A(\cdot)$ is an affine mapping; in other words, X is the projection of the inverse image of K under appropriate affine mapping. Indeed, given representation (8) of X, we can pose (7) as the $\mathcal{K}$-program $\min_{x,u}\{c^T x : A(x,u) \succeq_K 0\}$.

It turns out that $\mathcal{K}$-sets admit a kind of simple calculus comprised of "raw materials" (list of "basic" $\mathcal{K}$-s.'s) and "calculus rules" (list of operations preserving $\mathcal{K}$-representability). This calculus is the "toolkit" we are looking for: whenever we see that the set X in question is obtained from "raw materials" via calculus rules, we can be sure that X is a $\mathcal{K}$-s. (and in fact, as we shall see, can point out an explicit $\mathcal{K}$-r. of X, thus converting (7) to an explicit $\mathcal{K}$-program).

Since a convex set often arise as a level set of a convex function, it makes sense to define a *$\mathcal{K}$-representable function* ("$\mathcal{K}$-f." for short) $f : \mathbb{R}^n \to \mathbb{R} \cup \{+\infty\}$ as a function with $\mathcal{K}$-representable epigraph $\mathrm{Epi}\{f\}$. An immediate observation is that *a $\mathcal{K}$-r. of* $\mathrm{Epi}\{f\}$ *induces $\mathcal{K}$-r.'s of all level sets of f*. Indeed,

$$\begin{gathered}\big(f(x) \le t \Leftrightarrow \text{there exists } u \text{ such that } A(x,t,u) \succeq_K 0\big)\\ \Longrightarrow\\ \big(f(x) \le a \Leftrightarrow B(x,u) \equiv A(x,a,u) \succeq_K 0\big).\end{gathered}$$

4.1.1. "Calculus rules". It turns out (see, e.g., [8]) that all basic convexity-preserving operations with functions/sets preserve $\mathcal{K}$-representability. E.g.,

- A polyhedral set is $\mathcal{K}$-s.
- Finite intersections, arithmetic sums and direct products of $\mathcal{K}$-s.'s are $\mathcal{K}$-s.'s.

While the above statement looks as an existence theorem, it in fact is "fully algorithmic": given $\mathcal{K}$-r.'s for the operands X_i, we can efficiently build a $\mathcal{K}$-r. for the resulting set. E.g., if $X_i = \{x : \text{ there exists } u^i \text{ such that } A_i(x, u^i) \succeq_{K_i} 0\}$, $i = 1, \ldots, m$, then $\bigcap_{i=1}^m X_i = \{x : \text{ there exists } u = (u^1, \ldots, u^m) \text{ such that } A(x, u) \equiv (A_1(x, u^1), \ldots, A_m(x, u^m)) \succeq_{K_1 \times \cdots \times K_m} 0\}$, and the cone $K = K_1 \times \cdots \times K_m$ is in $\mathcal{K}$, since this family is closed w.r.t. taking direct products. It should be stressed that *all* calculus rules to follow are equally simple and algorithmic.

• The image and the inverse image of a $\mathcal{K}$-s. under an *affine* mapping is a $\mathcal{K}$-s.

• The *polar cone* $X_* = \{(y, t) : y^T x \le t \text{ for all } x \in X\}$ of a $\mathcal{K}$-s. X given by *strictly feasible* $\mathcal{K}$-r. is a $\mathcal{K}$-s. In other words, the support function of X (its epigraph is exactly X_*) is $\mathcal{K}$-f., and thus the polar of $X \ni 0$ (which is the 1-level set of the support function) is $\mathcal{K}$-s.

As an instructive example, let us build a $\mathcal{K}$-r. of X_*. If $X = \{x : Ax + Bu + c \succeq_K 0 \text{ for some } u\}$ is a strictly feasible $\mathcal{K}$-r. for X, then $X_* = \{(y, t) : \sup_{x,u}\{y^T x : Ax + Bu + c \succeq_K 0\} \le t\} = \{(y, t) : \min_v\{c^T v : A^T v = -y, B^T v = 0, v \succeq_{K_*} 0\} \le t\} = \{(y, t) : \text{ there exists } v \text{ such that } A^T v = -y, B^T v = 0, v \succeq_{K_*} 0, c^T v \le t\}$, with the second "=" in the chain given by conic duality. We see that X_* is the projection onto the (y, t)-space of the set $Y = \{(y, t, v) : A^T v = -y, B^T v = 0, v \succeq_{K_*} 0, c^T v \le t\}$. Y is a $\mathcal{K}$-s. Indeed, K_* is $\mathcal{K}$-s. since $\mathcal{K}$ is closed w.r.t. passing to dual cones, and Y is the direct product of K_* and a polyhedral set (the space of (y, t)) intersected with another polyhedral set; all these operations preserve $\mathcal{K}$-representability. The same is true for projection, thus X_* is $\mathcal{K}$-s. along with Y.

• Two useful operations with sets – taking closed conic hull $\mathrm{cl}\{(t, x) : t > 0, t^{-1}x \in X\}$ of X and taking the closed convex hull of the union of finitely many convex sets X_i – "nearly preserve" $\mathcal{K}$-representability, meaning that $\mathcal{K}$-r.'s of the operands readily provide a $\mathcal{K}$-r. of a convex set $\hat{Y}$ which is in-between the "true" result Y of the operation and the closure of Y (in particular, we end up with $\mathcal{K}$-r. of *exactly* Y when Y is closed). As far as the possibility of conic reformulation of a program $\min_{y \in Y} c^T y$ is concerned, a $\mathcal{K}$-r. of a convex set $\hat{Y}$ which is in-between the true set Y and its closure is, essentially, as good as a $\mathcal{K}$-r. of Y itself.

• Sometimes, getting a $\mathcal{K}$-r. of a result of an operation requires mild regularity assumptions on the $\mathcal{K}$-r.'s of operands. E.g., let $\{x : Ax + Bu + c \succeq_K 0 \text{ for some } u\}$ be a $\mathcal{K}$-r. of a convex set X such that $Bu \in K$ implies that $u = 0$. Then the closed conic hull of X and the recessive cone of X are $\mathcal{K}$-s.'s with representations, respectively, $\{x : \text{ there exists } (u, t \ge 0) \text{ such that } Ax + Bu + tc \succeq_K 0\}$ and $\{x : \text{ there exists } u \text{ such that } Ax + Bu \succeq_K 0\}$.

"Functional analogies" of the outlined calculus rules are as follows:

• The maximum, a linear combination with nonnegative coefficients, and a direct sum of finitely many $\mathcal{K}$-f.'s is again a $\mathcal{K}$-f.

• If $f(\cdot)$ is a $\mathcal{K}$-f., then so is $g(y) = f(Ay + b)$.

• If $f(\xi, \eta)$ is a $\mathcal{K}$-f. and the infimum $\phi(\xi) = \inf_\eta f(\xi, \eta)$ is achieved for every ξ for which this infimum is $< +\infty$, then ϕ is a $\mathcal{K}$-f.

• The Legendre transformation ("the conjugate") $f_*(\xi) = \sup_x[\xi^T x - f(x)]$ of a function f with $\mathrm{Epi}\{f\}$ given by a strictly feasible $\mathcal{K}$-r. is a $\mathcal{K}$-f.

• Let $f_i, i = 1, \ldots, m$, be $\mathcal{K}$-f.'s on $\mathbb{R}^m$ and g be a nondecreasing, w.r.t. the usual partial order $\leq$, $\mathcal{K}$-f. on $\mathbb{R}^m$. Then the superposition $g(f_1(x), \ldots, f_m(x))$ is again a $\mathcal{K}$-f.

A good news expressed by the above facts is that *with $\mathcal{K}$-r.'s of the involved entities in use, all basic constructions of Convex Analysis* (including "advanced ones", like taking polar, support function, Legendre transformation, etc.) *become "explicitly representable" and thus much better suited for analytical/algorithmic processing than in their original abstract form.*

Equipped with "calculus" of $\mathcal{K}$-representable sets and functions, we are in a position to investigate the "expressive abilities" of LP/CQP/SDP. The situation with LP seems to be clear: $\mathcal{LP}$-s.'s are exactly the polyhedral sets, and $\mathcal{LP}$-f.'s are finite maxima of affine functions. To understand what can be expressed via CQP and SDP, we need to know what are the corresponding "raw materials". These are the issues we are about to address in the next two sections.

4.2. Expressive abilities and applications of CQP. Basic $\mathcal{CQP}$-representable sets and functions include, along with trivial examples, like affine function or the Euclidean norm $f(x) = \|x\|_2$, several less trivial examples, e.g.:

• Convex quadratic forms $f(x) = x^T A^T Ax + b^T x + c$: $\{t \geq f(x) \Leftrightarrow (2(Ax)^T, t - b^T x - c + 1, t - b^T x - c + 1)^T \succeq_{\boldsymbol{L}} 0\}$;

• Univariate power functions $(\max[0, x])^p$, $|x|^p$ and p-norms $\|\cdot\|_p$ on $\mathbb{R}^n$, provided $p \geq 1$ is rational,

• Power monomials $(-\prod_{i=1}^m x_i^{p_i})$ with $x_i \geq 0$ and rational exponentials $p_i \geq 0$ such that $\sum_i p_i \leq 1$ (the latter is necessary and sufficient for the convexity of the monomial), same as monomials $\prod_{i=1}^m x_i^{-p_i}$ with $x_i > 0$ and rational $p_i \geq 0$.

In view of calculus rules, already these "raw materials" allow for CQP reformulations of a wide variety of convex programs, including (but by far not restricted to) convex quadratic quadratically constrained programs.

Example (Truss topology design.) A nontrivial example of a $\mathcal{CQP}$-f. is given by $\mathrm{Compl}(t) = \min\{\tau : \begin{bmatrix} 2\tau & f^T \\ f & A^T \mathrm{Diag}\{t\} A \end{bmatrix} \succeq 0\}$ of *nonnegative* vector variable t. This function is associated with an important application of CQP – *truss topology design*, see [73, Chapter 15] and references therein. In the TTD problem, one is looking for a construction comprised of elastic bars (like railway bridge, electric mast, or Eiffel Tower) most rigid w.r.t. a given set of (non-simultaneous) loading scenarios. The data are given by a finite 2D or 3D mesh of nodes, where the would-be bars can be linked to each other, boundary conditions restricting virtual displacements of the nodes to given linear subspaces in the embedding physical space, *k loads* – collections of external forces acting at the nodes, and the total weight w of the construction. A design is specified by a collection $t \in \mathbb{R}^n$ of weights of the bars, and its rigidity w.r.t. a load is measured by the *compliance* – the energy capacitated by the construction in the static

equilibrium under the load (the less is the compliance, the better). With properly defined matrix A (readily given by the nodal mesh and the boundary conditions) and vector f representing the load, the compliance is exactly Compl$(\cdot)$, so that the TTD problem, in its simplest form, reads

$$\min_{t,\tau}\left\{\tau : \left[\begin{array}{cc} 2\tau & f_i^T \\ f_i & A^T \mathrm{Diag}\{t\}A \end{array}\right] \succeq 0,\ i=1,\dots,k,\ t\geq 0,\ \textstyle\sum_j t_j \leq w\right\}. \tag{9}$$

The applied importance of this problem stems from the fact that it allows to optimize not only the sizing, but also the topology of truss. To this end one starts with a fine nodal mesh where all pairs of nodes can be linked by bars; in the optimal solution just few of the bars get positive weights, and the solution recovers the (nearly) optimal topology.

As it arises, (9) is an sdp. However, passing to the SDP dual of (9) and more or less straightforwardly processing it, one concludes that the dual is *equivalent* to a CQP program, whence, again applying duality, one gets an equivalent CQP reformulation of (9) and recovers a $\mathcal{CQP}$-r. of the compliance:

$$\begin{aligned}\tau \geq \mathrm{Compl}(t) \Longleftrightarrow \text{there exists } (q,r) \text{ such that } & A^T q = f,\ r\geq 0,\\ & \sum_i r_i \leq 2\tau,\ (2q_i, r_i - t_i, r_i + t_i)^T \in \boldsymbol{L}^3 \quad \text{for all } i.\end{aligned} \tag{10}$$

This example is very instructive. After the $\mathcal{CQP}$-r. (10) of compliance is guessed, its validity can be easily proved directly. The power of conic programming machinery is that there is no necessity to guess (and to the best of our knowledge, (10) never was guessed, in spite of its a posteriori transparent mechanical interpretation) – it can be *computed* in a purely mechanical way. Besides this, the CQP equivalent of the dual to (9) – which again is given by a mechanical computation – is of incomparably smaller design dimension than the original problem. Indeed, to capture the topology design, the mesh cardinality N already in the 2D case should be of order of thousands; when all pair connections are allowed, this results in the design dimension n of (9) of about $N^2/2$, i.e., in the range of millions, which is too much for actual computations. In contrast, the design dimension of the CQP reformulation of the dual to (9) is of order of $kN \ll N^2$, and this is how the TTD problem is actually solved. This example, among many others, shows that conic programming is not just a good framework for number crunching; it is a good framework for instructive analytical processing of convex programs.

Example (Robust linear programming). In reality, the data c, A, b in an LP program $\min_x\{c^T x : Ax \geq b\}$ usually are *uncertain* – not known exactly when the program is solved. It turns out that even pretty small from practical viewpoint perturbations of the data, like 0.01%, can make the nominal optimal solution (one corresponding to the nominal data) heavily infeasible and thus practically meaningless. One way to "immunize" solutions against data uncertainty is to assume that the data (c, A, b) are "uncertain-but-bounded", i.e., belong to a given in advance *uncertainty set* $\mathcal{U}$, and to

require from candidate solutions to be *robust feasible*, i.e., to satisfy the constraints whatever be a realization of the data from $\mathcal{U}$. Treating in the same worst-case-oriented fashion the objective, one associates with uncertain LP its *Robust Counterpart* (RC) – the problem $\min_{x,t}\{t : c^T x \le t, Ax - b \ge 0 \text{ for all } (c, A, b) \in \mathcal{U}\}$ of minimizing the worst-case value of the objective over robust feasible solutions. While improving significantly "reliability" of resulting decisions in the face of data uncertainty, the RC, as an optimization program, has a drawback: when $\mathcal{U}$ is infinite (which is typical), the RC is a *semi-infinite* (that is, with infinitely many linear constraints) program; programs of this type not necessarily are computationally tractable. Fortunately, in this respect uncertain LP (in contrast to uncertain CQP/SDP) is simple – the RC of an uncertain LP problem is computationally tractable, provided that the (convex) uncertainty set is so. For example, if $\mathcal{K}$ is a family of regular cones closed w.r.t. taking direct product and passing from a cone to its dual, and $\mathcal{U}$ is given by a strictly feasible $\mathcal{K}$-r., the RC can be straightforwardly reformulated as an explicit $\mathcal{K}$-program (an immediate corollary of $\mathcal{K}$-representability of the polar cone of a $\mathcal{K}$-s., see Section 4.1). Now, typical uncertainty sets in uncertain LP are $\mathcal{CQP}$-representable, most notably – intersections of boxes (coming from upper and lower bounds on uncertain coefficients) and ellipsoids (which allow to model reasonably well random uncertainty). As a result, RC's of uncertain LP programs are CQP's.

For other applications of CQP, see [39], [2], [14].

The above suggests that "expressive abilities" of CQP are much stronger, and applications are much wider than those of LP. Surprisingly, the "gap" here is smaller than one could think – *conic quadratic programs with bounds on variables are polynomially reducible to linear programs.* The reduction is given by *fast polyhedral approximation* of Lorentz cones [9]. Specifically, given m-dimensional Lorentz cone $\boldsymbol{L}^{m+1} = \{(x, t) \in \mathbb{R}^m \times \mathbb{R} : t \ge \|x\|_2\}$ and $\varepsilon \in (0, 1/2)$, one can point out an explicit system of $O(m \ln(1/\varepsilon))$ linear inequalities $Px + tp + Qu \ge 0$ in original variables x, t and $O(m \ln(1/\varepsilon))$ additional variables u such that the projection $\boldsymbol{P}^m$ of the cone $\{(x, t, u) : Px + tp + Qu \ge 0\}$ onto the space of x, t-variables satisfies $\boldsymbol{L}^m \subset \boldsymbol{P}^m \subset \{(x, t) : \|x\|_2 \le (1 + \varepsilon)t\}$. Exaggerating, we could say that CQP does not exist as an independent entity. It is interesting whether the same is true for SDP; to the best of our knowledge, this question is completely open.

4.3. Expressive abilities and applications of SDP.

4.3.1. Basic $\mathcal{SDP}$-representable sets and functions. As it was already mentioned, the Lorentz cone is a cross-section of the semidefinite one, so that all $\mathcal{CQP}$-representable functions and sets are $\mathcal{SDP}$-representable as well. In fact the expressive abilities of SDP are much wider than those (already pretty rich) of CQP. The essentially new functions/sets we can handle are as follows [8, Section 4.2]:

• *Functions of eigenvalues of symmetric matrices.* For $X \in \boldsymbol{S}^n$, let $\lambda(X) = (\lambda_1(X), \ldots, \lambda_n(X))^T$ be the vector of eigenvalues of X taken with their multiplicities in the non-ascending order. We start with observation (see, e.g., [46]) that *the sum of*

k largest eigenvalues of a symmetric matrix X is an $\mathcal{SDP}$-f.:

$$t \geq \lambda_1(X) + \cdots + \lambda_k(X) \Leftrightarrow 0 \preceq Z,\ X \preceq Z + sI,\ t \geq \mathrm{Tr}(Z) + ks \text{ for some } (Z, s).$$

As a result, *whenever $f(\cdot)\colon \mathbb{R}^n \to \mathbb{R} \cup \{+\infty\}$ is a symmetric w.r.t. permutations of arguments $\mathcal{SDP}$-f., the function $f(\lambda(X))\colon \boldsymbol{S}^n \to \mathbb{R} \cup \{+\infty\}$ is an $\mathcal{SDP}$-f. with $\mathcal{SDP}$-r. readily given by an $\mathcal{SDP}$-r. of f*. In particular, the following functions on $\boldsymbol{S}^n$ admit explicit $\mathcal{SDP}$-r.'s: (a) $\sum_{i=1}^k \lambda_i(X)$; (b) $\|X\| = \max_i |\lambda_i(X)|$; (c) $-\det^q(X)$, $X \succeq 0$, $q \leq \frac{1}{n}$ is rational; (d) $\det^{-q}(X)$, $X \succ 0$, $q > 0$ is rational; (e) $\|X\|_p = \left(\sum_{i=1}^m |\lambda_i(X)|^p\right)^{1/p}$, $p \geq 1$ is rational; (f) $\left(\sum_{i=1}^m \max^p[\lambda_i(X), 0]\right)^{1/p}$, $p \geq 1$ is rational.

• *Functions of singular values.* Singular values $\sigma_1(X) \geq \sigma_2(X) \geq \cdots \geq \sigma_m(X)$ of a rectangular $m \times n$, $m \leq n$, matrix X are closely related to the eigenvalues of the linearly depending on X $(n+m) \times (n+m)$ symmetric matrix $\hat{X} = \begin{bmatrix} & X \\ X^T & \end{bmatrix}$: eigenvalues of $\hat{X}$ are $\pm\sigma_i(X)$, $i = 1, \ldots, m$, and $n - m$ zeros. Therefore $\mathcal{SDP}$-r.'s of functions of eigenvalues of symmetric matrices admit "singular value counterparts". E.g., *if $f\colon \mathbb{R}^m_+ \to \mathbb{R} \cup \{+\infty\}$ is a nondecreasing symmetric w.r.t. permutations of arguments $\mathcal{SDP}$-f., then the function $f(\sigma(X))\colon \mathbb{R}^{m\times n} \to \mathbb{R} \cup \{+\infty\}$ is an $\mathcal{SDP}$-f. with $\mathcal{SDP}$-r. readily given by one of f*. In particular, the following functions on $\mathbb{R}^{m\times n}$ admit explicit $\mathcal{SDP}$-r.'s: (a) $\sum_{i=1}^k \sigma_i(X)$; (b) $\|X\| = \max_i \sigma_i(X)$; (c) $\|X\|_p = \left(\sum_{i=1}^m \sigma_i^p(X)\right)^{1/p}$, $p \geq 1$ is rational.

• *Sets of the form $\{X \in \boldsymbol{S}^n : \lambda(X) \in A\}$, where A is a symmetric w.r.t. permutations of coordinates $\mathcal{SDP}$-s. in $\mathbb{R}^n$*, and their "singular value" analogies $\{X \in \mathbb{R}^{m\times n} : \sigma(X) \in A\}$ with symmetric and monotone $(0 \leq x' \leq x \in A \Rightarrow x' \in A)$ $\mathcal{SDP}$-s. A.

• *The set $\{(A, a, \alpha) \in \boldsymbol{S}^n \times \mathbb{R}^n \times \mathbb{R} : x^T Ax + 2a^T + \alpha \geq 0$ for all $(x : x^T Bx + 2b^T x + \beta \geq 0)\}$ of quadratic forms nonnegative on the level set of a given quadratic form which is positive somewhere: there is $\bar{x}$ with $\bar{x}^T B\bar{x} + 2b^T\bar{x} + \beta > 0$.* By the famous $\mathcal{S}$-Lemma, an $\mathcal{SDP}$-r. of the set in question is

$$\left\{(A, a, \alpha) : \begin{bmatrix} \alpha & a^T \\ a & A \end{bmatrix} \succeq \lambda \begin{bmatrix} \beta & b^T \\ b & B \end{bmatrix} \text{ for some } \lambda \geq 0\right\}.$$

• *Sets $\mathcal{P}_n(\mathbb{R})$ of (vectors of coefficients of) real algebraic polynomials of degree $\leq n$ which are nonnegative on the entire axis*, same as sets of algebraic polynomials of degree $\leq n$ nonnegative on a given segment or ray, and sets of trigonometric polynomials of degree $\leq n$ nonnegative on a given segment. The same is true for the cones of psd on a given segment matrix-valued univariate algebraic/trigonometric polynomials of degree $\leq n$.

$\mathcal{SDP}$-r. of $\mathcal{P}_n(\mathbb{R})$ is readily given by the following observation [53]: *if $\phi_i(z)$, $1 \leq i \leq m$ are functions on a given set Z, L is the linear space in $\mathbb{R}^Z$ spanned by the functions $\phi_i(\cdot)\phi_j(\cdot)$ and $K \subset L$ is the cone of sums-of-squares (i.e., functions which are sums of squares of linear combinations of ϕ_i), then K is an $\mathcal{SDP}$-s., specifically, the image of $\boldsymbol{S}^m_+$ under the linear mapping $[X_{ij}]_{i,j=1}^m \mapsto \sum_{i,j} X_{ij}\phi_i(z)\phi_j(z)\colon \boldsymbol{S}^m \to L$.*

This simple observation underlies recent techniques for testing nonnegativity of a multivariate polynomial on a given domain, see [22], [57], [38] and references therein.

• Some sets given by nonlinear matrix inequalities can be represented by LMI's as well. E.g., $\mathrm{cl}\{X, Y, Z : Y \succ 0, X^T Y^{-1} X \preceq Z\} = \left\{X, Y, Z : \left[\begin{smallmatrix} Z & X^T \\ X & Y \end{smallmatrix}\right] \succeq 0\right\}$, and $\mathrm{cl}\{(X, Y) : X \succ 0, Y \preceq (C^T X^{-1} C)^{-1}\} = \{(X, Y) : Y \preceq Z,\ Z \succeq 0,\ X \geq CZC^T \text{ for some } Z\}$, provided C is of full column rank.

A seemingly interesting question is to *characterize* $\mathcal{SDP}$-representable sets. Clearly, such a set is convex and semi-algebraic. Is the inverse also true? This question can be relaxed, e.g., to whether an epigraph of convex multivariate polynomial is an $\mathcal{SDP}$-s. (this indeed is true in the univariate case), or: whether the hyperbolicity cone of a hyperbolic polynomial is an $\mathcal{SDP}$-s. (due to recently proved Lax conjecture [41], this indeed is true for polynomials of 3 variables), etc. This question seems to be completely open.

4.3.2. Applications of SDP. Due to its tremendous expressive abilities and powerful computational tools, SDP has an extremely wide spectrum of applications, including those in combinatorics (SDP relaxations of difficult problems), engineering (robust control, design of mechanical structures, electrical circuits and arrays of antennae, communications), signal processing, design of statistical experiments, etc. Over the last decade, the spectrum of applications of SDP has been constantly growing, and we believe this tendency is to continue in the foreseen future. We are about to overview an instructive sample of SDP applications; for more examples, see [13], [69], [16], [14], [73, Part III].

SDP relaxations of difficult combinatorial problems. The simplest way to derive SDP relaxations of combinatorial problems goes back to N. Shor [66], [67] and is as follows: consider a quadratic quadratically constrained program

$$\mathrm{Opt} = \min_x \{f_0(x) : f_i(x) \leq 0, i = 1, \ldots, m\},\ f_i(x) = x^T A_i x + 2b_i^T x + c_i, i \geq 0; \tag{11}$$

note that quadratic constraints can easily express combinatorial restrictions (like $x_i^2 - x_i = 0 \Leftrightarrow x_i \in \{0, 1\}$), and let us try to bound the optimal value from below (this is important, e.g., for various branch-and-bound algorithms). To this end, setting $x_+ = (1, x^T)^T$, observe that the objective and the constraints in (11) are linear in the matrix $X(x) = x_+ x_+^T$: $f_i(x) = \mathrm{Tr}(Q_i X(x))$, $i = 0, \ldots, m$, where $Q_i = \left[\begin{smallmatrix} c_i & b_i^T \\ b_i & A_i \end{smallmatrix}\right]$. When x runs through $\mathbb{R}^n$, $X(x)$ runs through the set cut off the convex set $\{X \succeq 0, X_{11} = 1\}$ by the requirement $\mathrm{Rank}(X) = 1$. Removing this requirement (and thus extending problem's feasible set), we arrive at the sdp

$$\mathrm{Opt(SDP)} = \min_X \{\mathrm{Tr}(Q_0 X) : \mathrm{Tr}(Q_i X) \leq 0,\ i = 1, \ldots, m,\ X \succeq 0,\ X_{11} = 1\}; \tag{12}$$

due to the origin of this program, we have $\mathrm{Opt(SDP)} \leq \mathrm{Opt}$.

Another way to arrive at (12) is to use Lagrange relaxation: whenever $\lambda \geq 0$, the quantity $L_*(\lambda) \equiv \inf\limits_x \left\{ f_0(x) + \sum_{i=1}^m \lambda_i f_i(x) \right\}$ is a lower bound on Opt. Maximizing this bound over $\lambda \geq 0$, we again get a lower bound on Opt; at the same time, the fact that all f_i are quadratic makes the program $\max_{\lambda \geq 0} L_*(\lambda)$ an explicit sdp, which is nothing but the semidefinite dual of (12).

Seemingly the first application of SDP in building computable bounds on difficult combinatorial entities is the famous *Lovasz capacity number* $\theta(G)$ *of a graph* G – a computable upper bound on the stability number of G introduced in [40]. The bound is

$$\begin{aligned} \theta(G) &= \min_{\lambda, X} \{\lambda : \lambda I \succeq X,\ X_{ij} = 1 \text{ when } (i,\ j) \text{ is not an arc}\} \\ &= \max_Y \left\{ \textstyle\sum_{i,j} Y_{ij} : Y \succeq 0, \mathrm{Tr}(Y) = 1,\ Y_{ij} = 0 \text{ when } (i,\ j) \text{ is an arc} \right\}. \end{aligned} \tag{13}$$

$\theta(G)$ is in-between the stability number $\alpha(G)$ of G and the chromatic number $\xi(\overline{G})$ of the complementary graph: $\alpha(G) \leq \theta(G) \leq \xi(\overline{G})$ ("Lovasz sandwich theorem"); it coincides with $\alpha(G)$ for perfect graphs, and possesses a number of other interesting and important properties. In hindsight, $\theta(G)$ can be obtained by Lagrange relaxation from the representation $\alpha(G) = \max_x \left\{ \sum_i x_i : x_i^2 - x_i = 0,\ x_i x_j = 0 \text{ whenever } (i,\ j) \text{ is an arc} \right\}$. Lovasz capacity is one of the earliest precursors to SDP, and the second equality in (13) found in [40] seems to be the first example of SDP duality.

Yet another way to think about the relaxation (this way *in hindsight* can be traced back to Grothendieck [25], 1953) is to imagine that we are looking for a random vector ξ which *at average* satisfies the constraints of the original problem and minimizes under this restriction the expected value of the objective; X in (12) can be thought of as the covariance matrix $\boldsymbol{E}\{(1, \xi^T)^T (1, \xi^T)\}$. The advantage of the latter interpretation is that it suggests a way to produce suboptimal solutions to (11) from the optimal solution X_* to (12). Specifically, given X_*, we can point out (in fact, in many ways) a random vector ξ such that $\mathrm{Cov}(\xi) = X_*$, thus getting a random solution to (11) which *at average* is feasible with expected value of the objective Opt(SDP), i.e., better than the true optimal value Opt. In favourable circumstances it is possible to convert, at a controllable cost in terms of the objective, the "feasible at average" random solution into an actually feasible solution; whenever it is the case, SDP relaxation yields a suboptimal solution to the problem of interest with *known* level of non-optimality. Examples include:

• The famous MAXCUT-related result of Goemans and Williamson [23] stating that SDP relaxation bound in the MAXCUT problem is tight up to factor 1.1382 ....

In the MAXCUT problem, one is given a graph with arcs assigned nonnegative weights and is looking for a cut (coloring of nodes into two colors) of maximal weight (the total weight of arcs linking nodes of different colors). MAXCUT can be posed in the form of (11), specifically, as

$$\mathrm{Opt} = \max_x \left\{ x^T L x : x_i^2 \leq 1,\ i = 1, \ldots, n \right\} \tag{14}$$

where $L \in \boldsymbol{S}^n$ is the Laplace matrix of the graph (and thus satisfying $L \succeq 0$, $L_{ij} \leq 0$ when $i \neq j$ and $\sum_j L_{ij} = 0$) and n is the number of nodes in the graph. MAXCUT is an NP-complete combinatorial problem; it is known [30] that it is NP-hard to approximate Opt within 4%-accuracy, even when randomized algorithms are allowed. In spite of this "severe computational intractability" of MAXCUT, Goemans and Williamson show that the SDP relaxation of (14) yields a surprisingly tight bound Opt(SDP) on Opt: $1 \leq \text{Opt(SDP)}/\text{Opt} \leq 1.1382\ldots$. The proof goes as follows: the optimal solution X_* to the SDP relaxation, which is the problem $\max_X \{\text{Tr}(LX) : X \succeq 0, X_{ii} = 1 \text{ for all } i\}$, is treated as the covariance matrix of a Gaussian random vector ξ with zero mean; this "feasible at average" random solution ξ is corrected to $(\text{sign}(\xi_1), \ldots, \text{sign}(\xi_n))$, thus yielding a feasible solution with the expected value of the objective at least $\text{Opt(SDP)}/1.1382\ldots$. For extensions and modifications of this result, see [73, Chapter 12] and references therein.

• Nesterov's $\frac{\pi}{2}$ theorem [52] stating that for an *arbitrary* matrix $L \succeq 0$ in (14), the SDP relaxation yields a $\frac{\pi}{2}$-tight upper bound on Opt, and that this remains true when the constraints $x_i^2 \leq 1$ in (14) are replaced with an arbitrary system of linear equality and inequality constraints on x_i^2 (for extensions and applications, see [75], [73, Chapter 13]).

One of far-reaching consequences of this fact is a tight efficiently computable upper bound on the (p, r)-norm $\|A\|_{p,r} = \max_x\{\|Ax\|_r : \|x\|_p \leq 1\}$. Computing (p, r)-norm is known to be easy only in the cases $p = 1$, $r = \infty$ and $p = r = 2$, and is known to be NP-hard when $p > r$. Nesterov [73, Theorem 13.2.4] shows that when $\infty \geq p \geq 2 \geq r \geq 1$, the efficiently computable quantity

$$\Psi(A) = \frac{1}{2} \min_{\mu\in\mathbb{R}^n, \nu\in\mathbb{R}^m} \left\{ \|\mu\|_{\frac{p}{p-2}} + \|\nu\|_{\frac{r}{2-r}} : \left[\begin{array}{c|c} \text{Diag}\{\mu\} & A^T \\ \hline A & \text{Diag}\{\nu\} \end{array}\right] \succeq 0 \right\}$$

is an upper bound, tight within the factor $\frac{1}{\frac{2\sqrt{3}}{\pi} - \frac{2}{3}} = 2.2936\ldots$, on $\|A\|_{p,r}$. When $r = 2$ or $p = 2$, the tightness factor can be improved to $\sqrt{\pi/2} = 1.2533\ldots$. Finally, we clearly have $\|A\|_{\infty,1} = \frac{1}{2}\max_{\|z\|_\infty\leq 1} z^T \left[\begin{array}{c|c} & A \\ \hline A^T & \end{array}\right] z$; the fact that the sdp relaxation of the latter problem yields a tight, within an absolute constant factor, upper bound on $\|A\|_{\infty,1}$ is nothing but a rephrasing of the Grothendieck inequality discovered as early as in 1953 [25][3)]. In the case in question, the tightness factor of the sdp relaxation bound can be improved to $\frac{\pi}{2\ln(1+\sqrt{2})} \approx 1.7822\ldots$ [37], which is better than Nesterov's "universal" constant $2.2936\ldots$. For further results on efficient bounding of $\|A\|_{\infty,1}$, see [3].

• "Approximate $\mathcal{S}$-Lemma" [11] stating that the SDP relaxation of the problem $\text{Opt} = \max_x\{x^T Lx : x^T Q_i x \leq 1, i = 1, \ldots, m\}$ with $Q_i \succeq 0$ and possibly indefinite L results in an efficiently computable upper bound Opt(SDP) on Opt which is tight within the factor $O(1)\ln(m + 1)$ (and indeed can differ from Opt by factor

[3)] this paper implies, particular, that the absolute constant $\pi/2$ in Nesterov's $\pi/2$ theorem cannot be improved.

$O(\ln(m+1))$ even when $L \succeq 0$);

- "Matrix Cube Theorem" [10] to be discussed later.

Applications in structural design. We have already considered one of these applications – truss topology design, which can be reduced to CQP. SDP offers a natural way to treat structural design problems in more complicated settings, most notably in the free material optimization one, see [7], [73, Chapter 15] and references therein. In free material optimization, one seeks for a construction comprised of material distributed over a given 2D/3D domain with varying from point to point mechanical properties and capable to withstand best of all a number of external loads. After finite element discretization, the problem reads

$$\min_{\{t_i\}} \left\{ \max_{1\le\ell\le k} \mathrm{Compl}_\ell(t) = \max_{P_\ell v \le p_\ell} \left[f_\ell^t v - v^T A(t) v/2 \right] : t_i \succeq 0,\ \sum_i \mathrm{Tr}(t_i) \le w \right\}, \tag{15}$$

where $A(t) = \sum_{i,s} b_{is} t_i b_{is}^T$ is the *stiffness matrix*, $t_i \in \boldsymbol{S}^d$ are rigidity tensors of the material in the finite element cells ($d = 3$ for 2D and $d = 6$ for 3D constructions), $P_\ell v \le p_\ell$ are constraints on virtual displacements of the nodes of finite element cells given by rigid obstacles in ℓ-th loading scenario, f_ℓ represents the ℓ-th load, and $\mathrm{Compl}_\ell(t)$ is the corresponding compliance – potential energy capacitated in the construction in the static equilibrium under ℓ-th load. Same as in the TTD case, the main advantage of the FMO model is that it allows to find the topology of the optimal construction; this topology serves as a starting point in actual engineering design restricted to traditional materials and taking into account a lot of complicating details ignored in the FMO model.

Same as in truss design, compliance in (15) admits an $\mathcal{SDP}$-r., and (15) can be reformulated as the SDP program

$$\min_{t,\tau,\mu} \left\{ \tau : \begin{array}{l} \begin{bmatrix} 2\tau - 2p_\ell^T \mu_\ell & \mu_\ell^T P_\ell - f_\ell^T \\ P_\ell^T \mu_\ell - f_\ell & A(t) \end{bmatrix} \succeq 0 \text{ for all } \ell \le k \\ t_i \succeq 0 \text{ for all } i,\ \sum_i \mathrm{Tr}(t_i) \le w,\ \mu_\ell \ge 0 \text{ for all } \ell \le k \end{array} \right\}. \tag{16}$$

Same as in the TTD case, semidefinite duality admits for instructive and better suited for numerical processing equivalent reformulations of (16), in particular, those where the Newton systems to be solved in IP methods are sparse (a rare case in SDP!). As a result, when the number of loading scenarios is small (like 2 or 3), IP methods allow to solve real world FMO problems with design dimension as large as many tens of thousands [36].

Another application of SDP in structural design relates to ensuring dynamical stability of a construction, i.e., imposing a lower bound on its eigenfrequencies. This can be modelled by the constraint $A(t) \succeq \omega^2 M(t)$, where t is the vector of design parameters, $A(t)$, $M(t)$ are the stiffness and the mass matrices and ω is the desired lower bound. Whenever $A(t)$, $M(t)$ are affine in t (as it is the case for trusses and in FMO), the constraint in question is an LMI.

Control applications. For the time being, the most "mature" applications of SDP are those in control, where for the last decade or so LMI's became a kind of standard language to pose and to process various control-related problems (see, e.g., [13], [16], [73, Chapter 14] and references therein). To give a flavour of related constructions and results, consider the basic problem of Lyapunov stability analysis/synthesis. The analysis problem is: given an uncertain n-dimensional linear dynamical system

$$\dot{x}(t) = A(t)x(t), \quad t \geq 0, \tag{17}$$

where the only restriction on $A(t)$ is to belong, at any time t, to a given "uncertainty set" $\mathcal{U}$, certify systems's *robust stability* – the fact that all trajectories of (all realizations of) the system tend to 0 as $t \to \infty$. In the "certain" case of $A(t) \equiv A$, a necessary and sufficient stability condition is the existence of *Lyapunov Stability Certificate* (LSC) – a matrix $X \succeq I$ and $\alpha > 0$ such that $A^T X + XA \preceq -\alpha X$. For an uncertain system, the standard *sufficient* stability condition is the existence of a common LSC (X, α) for all realizations $A \in \mathcal{U}$ of system's matrix; such an LSC implies that $x^T(t)Xx(t) \leq \exp\{-\alpha t\}x^T(0)Xx(0)$ for all trajectories, and thus – "stability with the decay rate α". Thus, LSC's of uncertain system are described by the infinite system of matrix inequalities

$$A^T X + XA + \alpha X \preceq 0 \quad \text{for all } A \in \mathcal{U} \tag{18}$$

in variables $X \succeq I$, $\alpha > 0$. To simplify our presentation, we treat below the decay rate α as a given positive constant rather than a variable, which makes (18) an infinite system of LMI's in X. In some cases, this infinite system can be replaced with a finite one, thus allowing for efficient computation of an LSC or detecting that no one exists. The simplest cases of this type are *polytopic uncertainty* $\mathcal{U} = \mathrm{Conv}\{A_1, \ldots, A_N\}$ (the equivalent finite system of LMI's is merely $A_i^T X + XA_i + \alpha X \preceq 0$, $i = 1, \ldots, N$) and *norm-bounded uncertainty* $\mathcal{U} = \{A = \bar{A} + B\Delta C : \|\Delta\| \leq \rho\}$ (here the LSC's are exactly the X-components of the solutions (X, λ) of the LMI

$$\left[\begin{array}{c|c} \bar{A}^T X + X\bar{A} + \alpha X + \lambda C^T C & \rho XB \\ \hline \rho B^T X & -\lambda I \end{array}\right] \preceq 0,$$

see [13]). There are also cases where (18), while being NP-hard, admits provably tight tractable approximation, most notably, the case of "interval uncertainty of level $\rho > 0$":

$$\mathcal{U} = \mathcal{U}_\rho = \{A : |A_{ij} - \bar{A}_{ij}| \leq \rho\delta_{ij} \text{ for all } i, j\}. \tag{19}$$

In the case of (19), X solves (18) if and only if the image of the cube $\{\zeta \in \mathbb{R}^{n\times n} : \|\zeta\|_\infty \leq \rho\}$ under the affine mapping

$$\zeta \mapsto B[X] + \sum_{i,j} \zeta_{ij} B^{ij}[X],$$

$$B[X] = -\bar{A}^T X - X\bar{A} - \alpha X, \quad B^{ij}[X] = -\delta_{ij}[e_j e_i^T X + X e_i e_j^T],$$

e_i being the basic orths, belongs to the semidefinite cone. Now, the question whether a "matrix cube" $\mathcal{B}_\rho = \{B + \sum_{\nu=1}^N z_\nu B_\nu : \|z\|_\infty \le \rho\}$ belongs bo the semidefinite cone is NP-hard, unless all matrices B_ν are of rank 1 (already with Rank $B_\nu = 2$, this question is at least as difficult as the MAXCUT problem [10]). There is, however, an evident verifiable *sufficient* condition for the inclusion $\mathcal{B}_\rho \subset \boldsymbol{S}^n_+$, namely, the existence of matrices $\{X_\nu\}_{\nu=1}^N$ such that $X_\nu \succeq \pm B_\nu$ and $B_0 - \rho \sum_\nu X_\nu \succeq 0$. It turns out ("Matrix Cube Theorem" [10]) that this condition is tight, provided that all "edge matrices" B_ν are of low rank; specifically, if the condition is *not* satisfied for certain ρ, then $\mathcal{B}_{\vartheta\rho} \not\subset \boldsymbol{S}^n_+$, with $\vartheta = \vartheta(\mu) \le \sqrt{\pi\mu}/2$ depending solely on $\mu = \max_\nu \mathrm{Rank}\, B_\nu$; note that $\vartheta(1) = 1$ and $\vartheta(2) = \pi/2$. Thus, our verifiable sufficient condition for the inclusion $\mathcal{B}_\rho \subset \boldsymbol{S}^n_+$ allows to identify, within factor $\vartheta(\mu)$, the largest ρ for which the inclusion takes place. Now note that when building an LSC for interval uncertainty (19), we seek for X such that a specific matrix cube *with edge matrices* $B^{ij}[X]$ *of rank* 2, depending on X as on a parameter, belongs to $\boldsymbol{S}^n_+$. Replacing the latter constraint with the above verifiable sufficient condition with its validity, we end up with a system of LMI's

$$X^{ij} \succeq \pm B^{ij}[X], \quad i,j = 1,\ldots,n,\ B[X] - \rho \sum_{ij} X^{ij} \succeq 0 \tag{20}$$

in variables (X, X^{ij}) such that the X-part of a feasible solution to this system is feasible for the infinite system of LMI's (18)–(19). The resulting "safe approximation" of (by itself intractable) system (18)–(19) is "tight within the factor $\pi/2$" – whenever (20) is infeasible, so is the system of interest with increased by factor $\pi/2$ uncertainty level. In particular, we can find efficiently a tight, within the factor $\pi/2$, lower bound on the largest possible uncertainty level for which the stability still can be certified by an LSC.

From practical viewpoint, a shortcoming of (20) is large, although polynomial in n, design dimension of this system of LMI's; an $n \times n$ matrix variable per each uncertain entry in the matrix of the original dynamical system is too much…Well, applying semidefinite duality, one can convert (20) into an equivalent system of LMI's in X and just $\approx \frac{3}{2}n^2$ additional scalar variables. Here again we see how useful could be the conic programming machinery in analytical processing of optimization problems.

For the time being, we were focusing on the stability analysis. In the *Lyapunov stability synthesis* problem, one is given a controlled dynamical system

$$\dot{x}(t) = A(t)x(t) + B(t)u(t),\ y(t) = C(t)x(t) \tag{21}$$

where $(A(t), B(t), C(t))$ is known to belong to a given uncertainty set $\mathcal{U}$, and is looking for output-based linear feedback control $u(t) = Ky(t)$ which allows to equip the closed loop system with an LSC (and thus makes it stable). Thus, we look for both a stabilizing feedback *and* a LSC for the closed loop system. The synthesis problem admits a nice LMI-based solution *at least* when the state-based feedback is allowed, i.e., when $C(t) \equiv I$, which we assume from now on. The Lyapunov matrix inequality

(18) for the closed loop system reads

$$[A + BK]^T X + X[A + BK] + \alpha X \preceq 0 \quad \text{for all } [A, B] \in \mathcal{U}; \tag{22}$$

this is *not* a LMI in our new design variables anymore. However, passing from X, K to the variables $Y = X^{-1}$, $Z = KY$ and multiplying both sides in (22) by Y from the left and from the right, we rewrite (22) as the infinite system of LMI's

$$AY + YA^T + BZ + Z^T B^T + \alpha Y \preceq 0 \quad \text{for all } [A, B] \in \mathcal{U}.$$

Same as above, this infinite system of LMI's can be processed efficiently in the case of polytopic or norm-bounded uncertainty, admits tractable tight approximation in the case of interval uncertainty, etc.

Not only stability, but many other "desired properties" of a linear time-invariant dynamical system (passivity, contractiveness, positive realness, nonexpansiveness, etc.) are certified, in a necessary and sufficient fashion, by solutions to appropriate LMI's. Usually, existence of a *common* certificate of this type for all realizations of system's data from a given uncertainty set becomes *sufficient condition* for the associated uncertain system to possess the robust version of the property in question; this explains the unique role played by SDP in robust control.

Extremal ellipsoids. In many situations (see, e.g., [15] and references therein), it is natural to approximate convex sets by ellipsoids – the latter are especially easy-to-specify and easy-to-operate convex sets. There are several ways to build ellipsoidal approximations of a convex solid $A \subset \mathbb{R}^n$. When A is given by a membership oracle, one can find a $O(n^{3/2})$-rounding of A, i.e., a pair of concentric similar ellipsoids $E_* \subset A \subset E^*$ with the ratio of linear sizes $O(n^{3/2})$, by a kind of ellipsoid method [26]. When A admits an explicit ϑ-self-concordant barrier F, one can build a $(\vartheta + 2\sqrt{\vartheta})$-rounding of A by approximating the minimizer of F over A ([13], cf. the end of Section 3.1). SDP enters the game when we are interested to find the "largest" ellipsoid contained in A or the "smallest" ellipsoid containing A. Indeed, representing ellipsoids in $\mathbb{R}^n$ in the form of $E = E(y, Y) = \{x = y + Yu : u^T u \leq 1\}$ with $Y \in \boldsymbol{S}^n_+$, natural "sizes" of E, like $(\mathrm{mes}_n(E))^{1/n} = c_n(\det(Y))^{1/n}$, or the smallest half-axis $\lambda_{\min}(Y)$, or the sum of k smallest half-axes (i.e., the k smallest eigenvalues of Y), become $\mathcal{SDP}$-representable concave functions of the parameters y, Y of the ellipsoid, so that maximizing such a size over all ellipsoids contained in A becomes a sdp, *provided that the set of parameters y, Y of ellipsoids contained in A is an $\mathcal{SDP}$-s.* Similarly, representing ellipsoids in $\mathbb{R}^n$ in the form of $W = W(z, Z) = \{x : (x - Z^{-1}z)^T Z^2 (x - Z^{-1}z) \leq 1\}$ with $Z \succ 0$, the sizes of W like $(\mathrm{mes}_n(W))^{\frac{1}{2n}} = d_n(\det(Z))^{-1/n}$, or the largest half-axis of W (i.e., $1/\lambda_{\min}(Z)$), or the sum of k largest half-axes of W, become $\mathcal{SDP}$-representable functions of z, Z, so that minimizing such a size over all ellipsoids containing A again is an sdp, *provided that the set of parameters z, Z of ellipsoids $W(z, Z)$ containing A is an $\mathcal{SDP}$-s.* Thus, when seeking for an extremal ellipsoid inscribed into/circumscribed around a solid $A \subset \mathbb{R}^n$

reduces to finding an $\mathcal{SDP}$-r. for the parameters y, Y, respectively, z, Z of the ellipsoids contained into/containing A. The key positive result here is as follows [13, Section 3.7]: one has $E(y, Y) \subset W(z, Z)$ if and only if there exists λ such that

$$\left[\begin{array}{c|c|c} I & ZY & Zy - z \\ \hline YZ & \lambda I & \\ \hline y^T Z^T - z^T & & 1 - \lambda \end{array}\right] \succeq 0,$$

which is an LMI in (y, Y, λ) when z, Z are fixed, and is an LMI in (z, Z, λ) when y, Y are fixed. As a result, the problems of finding (a) the smallest outer ellipsoidal approximation of the union of finitely many ellipsoids, and (b) the largest inner ellipsoidal approximation of the intersection of finitely many ellipsoids can be posed as explicit sdp's. The same is true for the problems of finding the largest inner ellipsoidal approximation of a polytope given by a list of linear inequalities, and finding the smallest outer ellipsoidal approximation of the convex hull of finitely many points. In contrast to this, it is NP-hard to verify that a given ellipsoid is contained in the convex hull of a given finite set of points or contains a polytope given by a list of linear inequalities; thus, the problems of inner ellipsoidal approximation of a convex hull of finite set and outer ellipsoidal approximation of the set of solutions of a finite system of linear inequalities both seem to be computationally intractable.

Concluding remarks. We hope that the outlined constructions and results demonstrate that convex programming is not merely something about number crunching; its development, stimulated both by intrinsic reasons and by needs of applications, requires resolving challenging mathematical problems with a specific "operational" flavour (at the end of the day, we want to understand how to build something rather than how something is built) which is a nice complement to typical descriptive flavour of problems arising in purely theoretical areas of mathematics. The most famous, posed in 1960s and still open, challenge here is to understand whether LP admits a strongly polynomial algorithm (essentially, a real arithmetic algorithm solving LP's *exactly* in time polynomial in the dimension of the data). Simplex-type LP algorithms are finite, but no one of them is known to be polynomial (and most are known *not* to be so); all known exact polynomial algorithms for LP work with rational data only, with running time polynomial in the *bit length* of the data, not in the number of data entries. All known in this direction is the existence of a strongly polynomial algorithm for LP with integer *and varying in a once for ever fixed finite range* data in the constraint matrix and real data in the objective and the right hand side (Tardos [68], see also [70]).

The major, in our appreciation, recent challenge comes from the desire to process extremely large-scale (tens and hundreds of thousands of variables) conic quadratic and semidefinite programs arising in some of applications (relaxations of combinatorial problems, structural design, etc.). Problems of huge sizes are beyond the "practical scope" of interior point methods with their Newton-type, and therefore too time consuming in the large scale case, iterations and require essentially different

optimization techniques (cf. [56], [44]). Note that in the extremely large scale case utilizing problem's structure becomes really crucial, which increases the importance of "structure-revealing" conic programming formulations of convex programs.

References

[1] Alizadeh, F., Interior point methods in semidefinite programming with applications to combinatorial problems. *SIAM J. Optim.* **5** (1995), 13–51.

[2] Alizadeh, F., Goldfarb, D., Second-order cone programming. *Math. Program.* **95** (2003), 3–51.

[3] Alon, N., Naor, A., Approximating the Cut-Norm via Grothendieck's Inequality. *SIAM J. Comput.* **35** (4) (2006), 787–803.

[4] Andersen, E. D., Ye, Y., On a homogeneous algorithm for monotone complemntarity system. *Math. Program.* **84** (1999), 375–399.

[5] Arrow, K.J., Hurwicz, L., Uzawa, H., *Studies in linear and non-linear programming*. Stanford University Press, Stanford 1958.

[6] Bauschke, H., Güler, O., Lewis, A. S., Sendov, H. S., Hyperbolic polynomials and convex analysis. *Canad. J. Math.* **53** (2001), 470–488.

[7] Ben-Tal, A., Kočvara, M., Nemirovski, A., Zowe, J., Free material design via semidefinite programming. The multiload case with contact conditions. *SIAM J. Optim.* **9** (1999), 813–832.

[8] Ben-Tal, A., Nemirovski, A. *Lectures on Modern Convex Optimization: Analysis, Algorithms and Engineering Applications*. MPS/SIAM Ser. Optim., SIAM, Philadelphia, PA, 2001.

[9] Ben-Tal, A., and Nemirovski, A., On polyhedral approximations of the second-order cone. *Math. Oper. Res.* **26** (2001), 193–205.

[10] Ben-Tal, A., and Nemirovski, A., On tractable approximations of uncertain linear matrix inequalities affected by interval uncertainty. *SIAM J. Optim.* **12** (2002), 811–833.

[11] Ben-Tal, A., Nemirovski, A., and Roos, C., Robust solutions of uncertain quadratic and conic-quadratic problems. *SIAM J. Optim.* **13** (2002), 535–560.

[12] Blum, L., Cucker, F., Shub, M., Smale, S., *Complexity and Real Computation*. Springer-Verlag, New York 1997.

[13] Boyd, S., El Ghaoui, L., Feron, E., Balakrishnan, V., *Linear Matrix Inequalities in System and Control Theory*. SIAM, Philadelphia, PA, 1994.

[14] Boyd, S., Vandenberghe, L., *Convex Optimization*. Cambridge University Press, Cambridge 2004.

[15] Chernousko, F. L., *State estimation for dynamic systems*. CRC Press, 1994.

[16] El Ghaoui, L., Niculescu, S.-I. (eds.), *Advances on Linear Matrix Inequality Methods in Control*. SIAM, Philadelphia, PA, 1999.

[17] Faybusovich, L., Euclidean Jordan algebras and interior-point algorithms. *Positivity* **1** (1997), 331–357.

[18] Faybusovich, L., Linear system in Jordan algebras and primal-dal interior-point algorithms. *J. Comput. Appl. Math.* **86** (1997), 149–175.

[19] Fiacco, A., McCormic, G. P., *Nonlinear Programming: Sequential Unconstrained Minimization Techniques*. J. Wiley and Sons, New York, London, Sydney 1968.

[20] Fu, M., Luo, Z.-Q., Ye, Y., Approximation algorithms for quadratic programming. *J. Comb. Optim.* **2** (1998), 29–50.

[21] Garey, M. R., Johnson, D. S. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, San Francisco, CA, 1979.

[22] Gaterman, K., Parrilo, P. A., Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra* **192** (2004), 95–128.

[23] Goemans, M. X., Williamson, D. P., Improved approximation algorithms for maximum cut and satisfability problem using semidefinite programming. *J. Assoc. Comput. Mach.* **42** (1995), 1115–1145.

[24] Gonzaga, C. C., An algorithm for solving linear programming problems in $O(n^3L)$ operations. In: *Progress in mathematical programming. Interior point and related methods* (ed. by N. Megiddo). Springer-Verlag, New York 1989, 1–28.

[25] Grothendieck, A., Résumńe de la théorie ḿetrique des produits tensoriels topologiques. *Bol. Soc. Mat. Sao Paulo* **8** (1953), 1–79.

[26] Grötschel, M., Lovasz, L., Schrijver, A., *Geometric Algorithms and Combinatorial Optimization*. Algorithms Combin. 2, Springer-Verlag, Berlin 1987.

[27] Güler, O., On the self-concordance of the universal barrier function. *SIAM J. Optim.* **7** (1997), 295–303.

[28] Güler, O., Hyperbolic polynomials and interior point methods for convex programming. *Math. Oper. Res.* **22** (1997), 350–377.

[29] Güler, O., Tunçel, L., Characterization of the barrier parameter of homogeneous convex cones. *Math. Program.* **81** (1998), 55–76.

[30] Håstad, J., Some optimal inapproximability results. *J. ACM* **48** (2001), 798–859.

[31] Hildebrand, R., An LMI description for the cone of Lorentz-positive maps, http://www.optimization-online.org/DB_HTML/2005/12/1260.html

[32] Jarre, F., Optimal ellipsoidal approximations around the analytic center. *Appl. Math. Optim.* **30** (1994), 15–19.

[33] Karmarkar, N., A new polynomial-time algorithm for linear programming. *Combinatorica* **4** (1984), 373–395.

[34] Khachiyan, L. G., A Polynomial Algorithm in Linear Programming. *Dokl. Akad. Nauk SSSR* **244** (1979), 1093–1097; English transl. *Soviet Math. Dokl.* **20**, 191–194.

[35] de Klerk, E., Roos, C., Terlaky, T., Initialization in semidefinite programming via a self-dual skew-symmetric embedding. *Oper. Res. Letters* **20** (1997), 213–221.

[36] Koçvara, M., Stingl, M., PENNON – A Code for Convex Nonlinear and Semidefinite Programming. *Optim. Methods Softw.* **18** (2003), 317–333.

[37] Krivine, J. L., Sur la constante de Grothendieck. *C. R. Acad. Sci. Paris Ser. A-B* **284** (1977), 445–446.

[38] Lasserre, J. B., Global optimization with polynomials and the problem of moments. *SIAM J. Optim.* **11** (2001), 796–817.

[39] Lobo, M., Vandenberghe, L., Boyd, S., Lebret, H., Applications of second-order cone programming. *Linear Algebra Appl.* **284** (1998), 193–228.

[40] Lovasz, L., On the Shannon capacity of graphs. *IEEE Trans. Inform. Theory* **25** (1979), 1–7.

[41] Lewis, A. S., Parillo, P., Ramana, M., The Lax conjecture is true. *Proc. Amer. Math. Soc.* **133** (2005), 2495–2499.

[42] Luo, Z.-Q., Sturm, J. F., Zhang, S., Coinic convex programming and self-dual embedding. *Optim. Methods Softw.* **14** (2000), 169–218.

[43] Nemirovski, A., Yudin, D., Information-based complexity and efficient methods of convex optimization. *Èkonom. i Mat. Metody*; English transl. *Matekon* **12** (1976), 357–379.

[44] Nemirovski, A., Prox-method with rate of convergence $O(1/t)$ for variational inequalities with Lipschitz continuous monotone operators and smooth convex-concave saddle point problems. *SIOPT J. Optim.* **15** (2004), 229–251.

[45] Nesterov, Yu., Nemirovski, A., Conic duality and its applications in Convex Programming. *Optim. Methods Softw.* **1** (1992), 95–115.

[46] Nesterov, Yu., Nemirovski, A., *Interior Point Polynomial Time Methods in Convex Programming*. SIAM, Philadelphia, PA, 1994.

[47] Nesterov, Yu., Long-step strategies in interior-point primal-dual methods. *Math. Program.* **76** (1997), 47–94.

[48] Nesterov, Yu., Todd, M. J., Self-scaled barriers and interior-point methods for Convex Programming. *Math. Oper. Res.* **22** (1997), 1–42.

[49] Nesterov, Yu., Todd, M. J., Primal-dual interior-point methods for self-scaled cones. *SIAM J. Optim.* **8** (1998), 324–364.

[50] Nesterov, Yu., Nemirovski, A., Multiparameter surfaces of analytic centers and long-step path-following interior point methods. *Math. Oper. Res.* **23** (1998), 1–38.

[51] Nesterov, Yu., Todd, M. J., Ye, Y., Infeasible-start primal-dual methods and infeasibility detectors for nonlinear programming problems. *Math. Program.* **84** (1999), 227–267.

[52] Nesterov, Yu., Semidefinite relaxation and nonconvex quadratic optimization. *Optim. Methods Softw.* **9** (1998), 141–160.

[53] Nesterov, Yu., Squared functional systems and optimization problems. In *High Performance Optimization* (ed. by H. Frenk, T. Terlaky, Sh. Zhang). Kluwer Academic Publishers, Dordrecht 1999, 405–439.

[54] Nesterov, Yu., Todd, M. J., On the Riemannian geometry defined by self-concordant barriers and interior-point methods. *Found. Comput. Math.* **2** (2002), 333–361.

[55] Nesterov, Yu., Nemirovski, A., Central path and Riemannian distances. Discussion paper 2003/30, CORE, Louvain-la-Neuve, 2003.

[56] Nesterov, Yu., Smooth minimization of non-smooth functions. *Math. Program.* **103** (2005), 127–152.

[57] Parrilo, P. A., Semidefinite programming relaxations for semialgebraic problems. *Math. Program. Ser. B* **96** (2003), 293–320, 2003.

[58] Potra, F. A., Sheng, R., On homogeneous interior-point algorithms for semidefinite programming. *Optim. Methods Softw.* **9** (1998), 161–184.

[59] Ramana, M., An exact duality theory for semidefinite programming and its complexity implications. *Math. Program. Ser. B* **77** (1997), 129–162.

[60] Renegar, J., A polynomial-time algorithm, based on Newton's method, for linear programming. *Math. Program.* **40** (1988), 59–93.

[61] Renegar, J., *A Mathematical View of Interior-Point Methods in Convex Optimization*. MPS/SIAM Ser. Optim., SIAM, Philadelphia, PA, 2001.

[62] Schmieta, S. H., Alizadeh, F., Associative and Jordan Algebras, and Polynomial Time Interior-Point Algorithms for Symmetric Cones. *Math. Oper. Res.* **26** (2001), 543–564.

[63] Schmieta, S. H., Alizadeh, F., Extension of primal-dual interior point methods to symmetric cones. *Math. Program.* **96** (2003), 409–438.

[64] Shapiro, A., Extremal problems on the set of nonnegative definite matrices. *Linear Algebra Appl.* **67** (1985), 7–18.

[65] Shor, N. Z., Cut-off method with space extension in convex programming problems. *Cybernetics* **12** (1977), 94–96.

[66] Shor, N. Z., Class of global minimum bounds of polynomial functions. *Cybernetics* **23** (1987), 731–734.

[67] Shor, N. Z., *Nondifferentiable Optimization and Polynomial Problems*. Kluwer Academic Publishers, Dordrecht 1998.

[68] Tardos, E., A strongly polynomial minimum cost circulation algorithm. *Combinatorica* **5** (1985), 247–256.

[69] Vandenberghe, L., Boyd, S., Applications of semidefinite programming. *Appl. Numer. Math.* **29** (1999), 283–299.

[70] Vavasis, S., Ye, Y., A primal-dual interior point method whose running time depends only on the constraint matrix. *Math. Program.* **74** (1996), 79–120.

[71] Vinberg, E. B., The theory of homogeneous cones. *Trans. Moscow Math. Soc.* **12** (1965), 340–403.

[72] Ye, Y., Todd, M. J., Mizuno, S., An $O(\sqrt{nL})$-iteration homogeneous and self-dual linear programming algorithm. *Math. Oper. Res.* **19** (1994), 53–67.

[73] H. Wolkowicz, R. Saigal, L. Vandenberghe (eds.), *Handbook of Semidefinite Programming*. Kluwer Academic Publishers, 2000.

[74] Ye, Y., *Interior-Point Algorithms: Theory and Analysis*. Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley and Sons, New York 1997.

[75] Ye, Y., Approximating quadratic programming with bound and quadratic constraints. *Math. Program.* **84** (1999), 219–226.

[76] Ye, Y., Zhang, S., New results on quadratic minimization. *SIAM J. Optim.* **14** (2003), 245–267.

[77] Xu, X., Hung, P. F., Ye, Y., A simplified homogeneous self-dual linear programming algorithm and its implementation. *Ann. Oper. Res.* **62** (1996), 151–171.

ISYE, Georgia Institute of Technology, 765 Ferst Drive, Atlanta, GA 30332-0205, U.S.A.
E-mail: nemirovs@isye.gatech.edu

Deformation and rigidity for group actions and von Neumann algebras

Sorin Popa

Abstract. We present some recent rigidity results for von Neumann algebras (II_1 factors) and equivalence relations arising from measure preserving actions of groups on probability spaces which satisfy a combination of *deformation* and *rigidity* properties. This includes strong rigidity results for factors with calculation of their fundamental group and cocycle superrigidity for actions with applications to orbit equivalence ergodic theory.

Mathematics Subject Classification (2000). Primary 46L35; Secondary 37A20, 22D25, 28D15.

Keywords. von Neumann algebras, II_1 factors, amenability and property T for groups, measure preserving actions, Bernoulli actions, orbit equivalence, cocycles.

Introduction

A measure preserving action $\Gamma \curvearrowright X$ of a countable group Γ on a probability space (X, μ) gives rise in a natural way to a von Neumann algebra $L^\infty(X) \rtimes \Gamma$, through the *group measure space* (or *crossed product*) construction of Murray and von Neumann ([MvN36]). If Γ is infinite and the action is free and ergodic then $L^\infty(X) \rtimes \Gamma$ is a II_1 *factor*, a highly non-commutative infinite dimensional algebra with a positive trace. A central problem in the theory of von Neumann algebras is the classification up to isomorphisms of these factors in terms of their group/action data. Related to this, it was already shown in ([Si55]) that the isomorphism class of $L^\infty(X) \rtimes \Gamma$ only depends on the equivalence relation given by the orbits of $\Gamma \curvearrowright X$. This led to the study of actions of groups up to *orbit equivalence* ([D59]), an area in ergodic theory which since then developed in parallel but closely related to von Neumann algebras.

The early years concentrated on the amenable case, culminating with Connes' celebrated theorem that all II_1 factors arising from actions of amenable groups are isomorphic ([C76]). Also, all ergodic actions of amenable groups on the non-atomic probability space were shown orbit equivalent in ([OW80], [CFW81]). But non-amenable groups were used to produce large families of non-isomorphic factors in ([MvN43], [D63], [Sch63], [Mc70], [C75]), indicating the richness of the theory. Rigidity phenomena started to unveil in the work of Connes ([C80]), who discovered that factors arising from groups with property (T) of Kazhdan have countable outer

Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006

automorphism and fundamental groups ([C80]). On the OE side, Zimmer obtained a cocycle superrigidity result for actions of higher rank semisimple Lie groups, a dynamical generalization of Margulis superrigidity which enabled him to prove that free ergodic actions of lattices such as $\mathrm{SL}(n, \mathbb{Z})$ are non-OE for different n's ([Z80]). Surprising non-embeddability results for II_1 factors arising from certain lattices were then shown in ([CJ85], [CoH89]). More applications of all these ideas were derived in ([P86], [GoNe87], [GeGo88], [CoZ89]).

We present in this paper some recent progress made in these areas, triggered by the discovery in ([P01a], [P01b]) that if a group action $\Gamma \curvearrowright X$ satisfies both a *rigidity* condition (e.g. a weak form of property T) and a *deformability* property (e.g. Haagerup property on the group, or Bernoulli-like *malleability* on the action), then the overall rigidity of $L^\infty(X) \rtimes \Gamma$ is considerably enhanced. Two new techniques, *deformation/rigidity* and *intertwining subalgebras*, were developed to exploit this idea ([P01b], [P03], [P04a]). This led to the first *strong rigidity* results in von Neumann algebra theory, showing that any isomorphism between factors arising from Bernoulli actions of Kazhdan groups comes from conjugacy of actions and isomorphism of groups ([P03], [P04a]). When combined with work of Gaboriau in OE ergodic theory ([G00], [G01]), it also led to the solution in ([P01b], [P03]) of long standing open problems of Murray–von Neumann ([MvN43]) and Kadison ([Ka67]) on the fundamental group of factors.

The von Neumann algebra framework and deformation/rigidity techniques also allowed proving *cocycle superrigidity* with arbitrary discrete groups as targets for all Bernoulli actions $\Gamma \curvearrowright (X_0, \mu_0)^\Gamma$, first in the case Γ is Kazhdan ([P05]), then for Γ a product between a non-amenable and an infinite group ([P06]). When applied to cocycles coming from OE, this provided new *OE superrigidity* results, showing that if in addition Γ has no finite normal subgroups then any OE between a Bernoulli Γ-action and a free action $\Lambda \curvearrowright Y$ of an arbitrary countable group comes from a conjugacy. This added to the recent rigidity results obtained in OE ergodic theory using measure theoretic framework in ([Fu99a], [Fu99b], [G00], [G02], [MoS02]; see [S05] for a survey).

The presentation is organized as follows: In Sections 1, 2 we recall the basic definitions related to II_1 factor framework and its specific analysis tools (c.p. maps and Hilbert bimodules, Jones basic construction). In Section 3 we discuss the rigidity statements we aim to prove and review past progress. Section 4 explains the use of "separability arguments" in rigidity results while Sections 5, 6 describe the intertwining and resp. deformation/rigidity techniques. In Sections 7–10 we state the results obtained through these techniques in ([P01b], [P03], [P04a], [IPeP05], [P05]).

1. The II_1 factor framework

A *von Neumann algebra* is an algebra of linear bounded operators on a Hilbert space $\mathcal{H}$, containing $\mathrm{id}_\mathcal{H}$, closed under the adjoint $*$-operation and closed in the

weak operator topology given by the seminorms $|\langle T\xi, \eta\rangle|$, $T \in \mathcal{B}(\mathcal{H})$, $\xi, \eta \in \mathcal{H}$. These conditions ensure that once an operator T lies in the algebra so does its polar decomposition, and if in addition $T = T^*$ then the functional calculus of T with Borel functions belongs to it as well. The algebra $\mathcal{B}(\mathcal{H})$ of all linear bounded operators on $\mathcal{H}$ is an example of a von Neumann algebra. If $\mathcal{X} \subset \mathcal{B}(\mathcal{H})$ is a selfadjoint subset (for instance the range of a unitary representation of a group) then the set $\mathcal{X}'$ of operators $T \in \mathcal{B}(\mathcal{H})$ commuting with all elements in $\mathcal{X}$ is a von Neumann algebra. By a well known theorem of von Neumann, a $*$-algebra $M \subset \mathcal{B}(\mathcal{H})$ is a von Neumann algebra iff it is equal to its bicommutant $M'' = (M')'$.

1.1. von Neumann algebras from group actions. If (X, μ) is a standard probability space then the algebra of left multiplication operators by elements in $L^\infty(X)$ on the Hilbert space $L^2(X)$ is a von Neumann algebra. By the spectral theorem, any singly generated abelian von Neumann algebra A is in fact of this form. One identifies (functorially) a measure preserving isomorphism of probability spaces $\Delta\colon (X, \mu) \simeq (Y, \nu)$ (defined a.e.) with the integral preserving algebra isomorphism $\Delta\colon (L^\infty X, \int \cdot \mathrm{d}\mu) \simeq (L^\infty Y, \int \cdot \mathrm{d}\nu)$, via the relation $\Delta(x)(t) = x(\Delta^{-1}(t))$ for all $x \in L^\infty X$, $t \in X$. In particular, this gives a canonical identification of the groups $\mathrm{Aut}(X, \mu)$, $\mathrm{Aut}(L^\infty(X), \int \cdot \mathrm{d}\mu)$.

Let now Γ be a countable group and $\Gamma \curvearrowright X$ a *measure preserving* (*m.p.*) *action* of Γ on the probability space (X, μ), viewed also as an action of Γ on the algebra $L^\infty(X)$ preserving the integral, via the above identification. Consider the Hilbert space $\mathcal{H} = L^2(X) \mathbin{\overline{\otimes}} \ell^2\Gamma$ and let $L^\infty(X)$ acting on it by left multiplication on the $L^2(X)$-component. Let also Γ act on $\mathcal{H}$ as the multiple of the left regular representation λ, given by the unitary operators $u_g = \sigma_g \otimes \lambda_g$, $g \in \Gamma$, where σ denotes the representation of Γ on $L^2(X)$ extending $\Gamma \curvearrowright L^\infty(X)$. Let M_0 be the algebra generated by $L^\infty(X)$ and $\{u_g\}_g$ in $\mathcal{B}(\mathcal{H})$. The *group measure space von Neumann algebra* associated to $\Gamma \curvearrowright X$ is the weak closure of the algebra M_0 and is denoted $L^\infty(X) \rtimes \Gamma$.

It is convenient to view the dense subalgebra $M_0 \subset M = L^\infty X \rtimes \Gamma$ as the algebra of "polynomials" $\Sigma_g a_g u_g$ with "coefficients" a_g in $L^\infty(X)$, "indeterminates" (called *canonical unitaries*) u_g, $g \in \Gamma$, and multiplication rule $(a_g u_g)(a_h u_h) = a_g \sigma_g(a_h) u_{gh}$, and to view $\mathcal{H}$ as the Hilbert space $\oplus_g L^2(X) u_g$ of square summable formal "Fourier series" $\Sigma_g \xi_g u_g$ with coefficients ξ_g in $L^2(X)$. The same product formula gives an action of M_0 on $\mathcal{H}$ by left multiplication. In fact, if a series $x = \Sigma_g a_g u_g \in \mathcal{H}$ is so that its formal product with any element in $\Sigma_h \xi_h u_h \in \mathcal{H}$ remains in $\mathcal{H}$, then the left multiplication operator by x lies in $M = \bar{M}_0^{wo}$, and any element of M is of this form.

The particular case when X is reduced to a point (i.e. $L^\infty(X) = \mathbb{C}$) of this construction gives the *group von Neumann algebra* $L\Gamma$ associated with Γ ([MvN43]). It is naturally isomorphic to the von Neumann subalgebra of $L^\infty(X) \rtimes \Gamma$ generated by the canonical unitaries $\{u_g\}_g$.

If we view $L^\infty(X)$ as a subalgebra of M via the identification $a = au_e = a1$, then the integral $\int \cdot \mathrm{d}\mu$ extends to a functional τ on M, by $\tau(x) = \int x \mathrm{d}\mu = \langle x, 1\rangle_{\mathcal{H}} = \int a_e \mathrm{d}\mu$, where $x = \Sigma_g a_g u_g \in M$. The functional τ is *positive* (i.e. $\tau(x^*x) \geq 0$ for all $x \in M$), *faithful* (i.e. $\tau(x^*x) = 0$ iff $x = 0$) and satisfies $\tau(xy) = \tau(yx)$ for all $x, y \in M$, i.e. it is a *trace* on M. Moreover, like the integral on $L^\infty(X)$, τ is countably additive on mutually orthogonal projections, i.e. it is *normal* on M.

Like $L^\infty(X)$, which we view both as a subspace of $L^2(X)$ and as operators of left multiplication on $L^2(X)$, we view $x = \Sigma_g a_g u_g \in M$ both as an element in $\mathcal{H}$ and as operator of left multiplication on $\mathcal{H}$. The trace τ then recovers the Hilbert norm on $M \subset \mathcal{H}$ by $\|x\|_2 = \tau(x^*x)^{1/2}$ and $\mathcal{H}$ is the completion of M in this norm.

1.2. von Neumann algebras from equivalence relations. An action $\Gamma \curvearrowright X$ is *free* (i.e. $\mu(\{t \in X \mid gt = t\}) = 0$ for all $g \neq e$) iff $L^\infty(X)$ is maximal abelian in M. If this is the case, then one can give the following alternative description of the von Neumann algebra $M = L^\infty(X) \rtimes \Gamma$, which only depends on the equivalence relations $\mathcal{R}_\Gamma \stackrel{\text{def}}{=} \{(t, gt) \mid t \in X, g \in \Gamma\}$ (cf. [Si55]): Let m be the unique measure on $\mathcal{R} = \mathcal{R}_\Gamma$ satisfying $m(\{(t, gt) \mid t \in X_0\}) = \mu(X_0)$ for all $X_0 \subset X$ and $g \in \Gamma$. If one identifies $\mathcal{R}$ with $X \times \Gamma$ via $(t, gt) \mapsto (t, g)$, then m corresponds to the product measure on $X \times \Gamma$, so $L^2(\mathcal{R}, m)$ identifies naturally with $L^2(X) \otimes \ell^2\Gamma = \Sigma_g L^2(X) u_g$. Under this identification, if $x, y \in L^2(\mathcal{R}, m)$ then their formal product as elements in $\Sigma_g L^2 X u_g$ corresponds to "matrix multiplication" $xy(t, t') = \Sigma_{s \sim t} x(t, s) y(s, t')$ for all $(t, t') \in \mathcal{R}$. Then M is equal to the set $L(\mathcal{R})$ of operators on $L^2(\mathcal{R})$ for which there exists $x \in L^2(\mathcal{R})$ with (matrix) product xy lying in $L^2(\mathcal{R})$, for any $y \in L^2(\mathcal{R})$. Note that $L^\infty(X)$ then corresponds to "matrices" x that are supported on the diagonal $\{(t, t) \mid t \in X\} \subset \mathcal{R}$.

The above construction of the von Neumann algebra $L(\mathcal{R})$ works in fact for any equivalence relation $\mathcal{R}$ on (X, μ) that can be generated by a countable group $\Gamma \subset \mathrm{Aut}(X, \mu)$ (cf. [FM77]). Under this construction, $L^\infty(X)$ embeds in $L(\mathcal{R})$ as the subalgebra of "diagonal matrices" on $\mathcal{R}$, and is always maximal abelian in $L(\mathcal{R})$. Thus, unless Γ acts freely, the construction of $L(\mathcal{R}_\Gamma)$ and $L^\infty(X) \rtimes \Gamma$ are different. For instance if X is a one point set then $L^\infty(X) \rtimes \Gamma = L\Gamma$ while $L(\mathcal{R}_\Gamma) = \mathbb{C}$. The algebra $L(\mathcal{R})$ has a canonical trace, given by $\tau(x) = \langle x, 1\rangle = \int x_0 \mathrm{d}\mu$, where x_0 is the restriction of $x \in L^2(\mathcal{R})$ to the diagonal. Thus, τ is positive, normal, faithful and it extends $\int \cdot \mathrm{d}\mu$. If $\Gamma \curvearrowright X$ is not free then one still has a set of canonical unitaries $\{u_g \mid g \in \Gamma\}$ in $L(\mathcal{R}_\Gamma)$ which satisfy $u_g a u_g^* = g(a)$ for all $a \in L^\infty(X)$, and which together with $L^\infty(X)$ generate $L(\mathcal{R}_\Gamma)$, but with $\tau(u_g)$ being the measure of the set $\{t \in X \mid gt = t\}$ (thus possibly non-zero for $g \neq e$).

The maximal abelian subalgebra $A = L^\infty(X)$ in $M = L(\mathcal{R})$ has the property that the normalizer of A in M, $\mathcal{N}_M(A) = \{u \in \mathcal{U}(M) \mid uAu^* = A\}$, generates M as a von Neumann algebra, i.e. $\mathcal{N}_M(A)'' = M$ ([Di54]). Maximal abelian $*$-subalgebras $A \subset M$ in arbitrary II_1 factors which satisfy this property are called *Cartan subalgebras* ([Ve71], [FM77]). It is shown in ([FM77]) that if $A \subset M$ is a Cartan subalgebra

inclusion, then there exist a m.p. action $\Gamma \curvearrowright A = L^\infty(X,\mu)$ and a $\mathcal{U}(A)$-valued 2-cocycle v for the action such that $(A \subset M) = (L^\infty(X) \subset L(\mathcal{R}, v))$, where the von Neumann algebra $L(\mathcal{R}, v)$ is defined similarly with $L(\mathcal{R})$ but with the product of canonical unitaries being twisted by the cocycle.

1.3. Conjugacy, orbit equivalence and algebra isomorphism. A *conjugacy* of group actions $\Gamma \curvearrowright (X,\mu)$, $\Lambda \curvearrowright (Y,\nu)$ is an isomorphism of probability spaces $\Delta\colon (X,\mu) \simeq (Y,\nu)$ and a group isomorphism $\delta\colon \Gamma \simeq \Lambda$ such that $\delta(g)\circ\Delta = \Delta\circ g$ for all $g \in \Gamma$. If the actions are faithful (i.e. any $g \neq e$ implements a non-trivial automorphism) then the condition $\Delta\Gamma\Delta^{-1} = \Lambda$ is sufficient to ensure conjugacy. A conjugacy (Δ,δ) implements an algebra isomorphism $\theta = \theta^{\Delta,\delta}\colon L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$, by $\theta(\Sigma_g a_g u_g) = \Sigma_g \Delta(a_{\delta(g)}) v_{\delta(g)}$, where v_h are the canonical unitaries in $L^\infty(Y) \rtimes \Lambda$. Thus, θ extends $\Delta\colon L^\infty(X) \simeq L^\infty(Y)$.

By the construction in 1.2, an isomorphism $\Delta\colon (X,\mu) \simeq (Y,\nu)$, viewed as algebra isomorphism $\Delta\colon L^\infty(X) \simeq L^\infty(Y)$, extends to an isomorphism $L(\mathcal{R}_\Gamma) \simeq L(\mathcal{R}_\Lambda)$ iff Δ takes $\mathcal{R}_\Gamma$ onto $\mathcal{R}_\Lambda$, i.e. if it is an *orbit equivalence* (OE) of $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$ (cf. [Si55], [FM77]). In other words, an OE of actions $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$ is the same as an isomorphism of the associated von Neumann algebras $L(\mathcal{R}_\Gamma) \simeq L(\mathcal{R}_\Lambda)$ (or $L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$ when actions are free) that takes $L^\infty(X)$ onto $L^\infty(Y)$. A third point of view, adopted in ([D59]; cf. also [Si55]), is to consider the *full group* $[\Gamma]$ of an action $\Gamma \curvearrowright X$ as the set of automorphisms α of (X,μ) for which there exists a (countable) partition of X into measurable sets X_g^α, $g \in \Gamma$ such that α coincides with g on X_g^α. Equivalently, $\alpha \in [\Gamma]$ iff the graph of α is contained in $\mathcal{R}_\Gamma$. It is then immediate to see that $\Delta\colon X \simeq Y$ is an OE of $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$ iff $\Delta[\Gamma]\Delta^{-1} = [\Lambda]$, i.e. Δ conjugates the full groups.

Triggered this way by Murray–von Neumann group measure space construction, these observations led to the study of actions up to OE ([D59]), initiating what today is called *orbit equivalence ergodic theory*. The fact that OE of actions can be defined in both measure theoretic and von Neumann algebra terms allows a powerful dual approach to this subject. When adopting the point of view of studying group actions, an isomorphism of algebras $L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$ (or $L(\mathcal{R}_\Gamma) \simeq L(\mathcal{R}_\Lambda)$) is called a *von Neumann equivalence* (vNE) of $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$. Thus, "conjugacy $\Rightarrow$ OE $\Rightarrow$ vNE", but the reverse implications fail in general (cf. [D59], [CJ82]).

1.4. Ergodic actions and II_1 factors. A von Neumann algebra M having a faithful normal trace τ is called *finite*. Thus $L^\infty(X) \rtimes \Gamma$, $L(\mathcal{R}_\Gamma)$ and their von Neumann subalgebras are finite.

A von Neumann algebra M is a *factor* if its center, $\mathcal{Z}(M) = \{z \in M \mid zx = xz \text{ for all } x \in M\}$, is equal to $\mathbb{C}1_M$. A finite factor (M,τ) which has *atoms* (i.e. non-zero $p \in \mathcal{P}(M)$ with $pMp = \mathbb{C}p$) is of the form $M \simeq \mathrm{M}_{n\times n}(\mathbb{C})$, for some n. A finite factor M has no atoms (i.e. it is *diffuse*) iff it is infinite dimensional. M is then called a *type* II_1 *factor*. Like the algebra $\mathrm{M}_{n\times n}(\mathbb{C})$, a II_1 factor has a unique trace τ with $\tau(1) = 1$, and projections in M can be conjugated by a unitary element in M

iff they have same trace. In other words, τ is a "dimension function" on $\mathcal{P}(M)$, but while $\tau(\mathcal{P}(M)) = \{k/n \mid 0 \leq k \leq n\}$ when $M = \mathrm{M}_{n\times n}(\mathbb{C})$, for II_1 factors the range of τ on projections is all the interval $[0, 1]$.

The trace of a non-factorial finite von Neumann algebra M is not unique, but M does have a unique conditional expectation Ctr onto its center, called the *central trace* on M, which satisfies $\mathrm{Ctr}(xy) = \mathrm{Ctr}(yx)$ for all $x, y \in M$, is normal faithful and has the property that projections are unitary conjugate iff they have the same Ctr.

The algebra $L(\mathcal{R}_\Gamma)$ associated to an action $\Gamma \curvearrowright X$ is a factor iff Γ acts *ergodically* on (X, μ), i.e., if $Z \subset X$ measurable satisfies $g(Z) = Z$ for all $g \in \Gamma$, then $\mu(Z) = 0, 1$. If this is the case, then $L(\mathcal{R}_\Gamma)$ is II_1 iff X (or $L^\infty(X)$) has no atoms. In particular, if $\Gamma \curvearrowright X$ is free, then $L^\infty(X) \rtimes \Gamma$ is a factor iff $\Gamma \curvearrowright X$ is ergodic. It is a II_1 factor iff action is ergodic and X diffuse (or $|\Gamma| = \infty$).

Given any countable (infinite) group Γ, its action on the non-atomic probability space by Bernoulli shifts, $\Gamma \curvearrowright (X_0, \mu_0)^\Gamma \simeq (\mathbb{T}, \mu)$, is free and ergodic (even mixing). More generally, if Γ acts on a countable set I then the action $\Gamma \curvearrowright (X_0, \mu_0)^I$, given by $g(t_i)_i = (t_{g^{-1}i})_i$, is free whenever $\{i \mid gi \neq i\}$ is infinite for all $g \neq e$ and it is ergodic iff $|\Gamma i| = \infty$ for all $i \in I$, in which case it is even *weak mixing*, i.e. there exists $g_n \in \Gamma$ such that $\lim_n \mu(g_n(Z) \cap Z) = \mu(Z)^2$ for all $Z \subset X$. Such actions are called *generalized Bernoulli actions*.

If an action $\Gamma \curvearrowright X$ is not free, then a sufficient condition for $L^\infty(X) \rtimes \Gamma$ to be a II_1 factor is that the action be ergodic and Γ be *infinite conjugacy class* (ICC), i.e. $|\{ghg^{-1} \mid g \in \Gamma\}| = \infty$ for all $h \neq e$. In particular, $L\Gamma$ is a II_1 factor iff Γ is ICC. Examples of ICC groups are the infinite symmetric group S_∞, the free groups $\mathbb{F}_n, 2 \leq n \leq \infty$, the groups $\mathrm{PSL}(n, \mathbb{Z}), n \geq 2$.

In fact, given any finite von Neumann algebra (P, τ) and an action $\Gamma \curvearrowright (P, \tau)$ of a countable group Γ on it, one can construct the *crossed product* von Neumann algebra $P \rtimes \Gamma$ acting on the Hilbert space $\ell^2(\Gamma) \mathbin{\overline{\otimes}} L^2(P)$, exactly as in the case $(P, \tau) = (L^\infty(X), \int \cdot \mathrm{d}\mu)$. Freeness of the action means in this general context that if $g \in \Gamma$ and $v \in P$ satisfy $vx = g(x)v$ for all $x \in P$, then either $g = e$ or $v = 0$, and it is equivalent to the condition $P' \cap P \rtimes \Gamma = \mathcal{Z}(P)$. If the action is free ergodic then the crossed product algebra is a factor.

Other constructions of factors are the *tensor product* and the *free product* (possibly with amalgamation) of finite factors (P_i, τ_i), $i = 1, 2, \ldots$, which have self-explanatory definitions. A useful framework for analysis arguments is the *ultraproduct* construction of II_1 factors $\Pi_\omega M_n$, associated to a sequence of finite factors M_n, with $\dim M_n \to \infty$, and a free ultrafilter ω on $\mathbb{N}$ (e.g. [Mc70], [C76]).

1.5. Approximately finite dimensional II_1 factors. Murray–von Neumann showed that all group measure space II_1 factors arising from actions of locally finite groups, and more generally all *approximately finite dimensional* (AFD) II_1 factors, are mutually isomorphic ([MvN43]). The unique AFD II_1 factor, also called the *hyperfinite* II_1 factor and denoted R, can be realized as the group factor $L(S_\infty)$, or as the infinite tensor product $\overline{\otimes}_n(\mathrm{M}_{2\times 2}(\mathbb{C}), \mathrm{tr})_n$. Since the relative commutant $P_0' \cap M$ of any

finite dimensional subfactor P_0 of a II_1 factor M is also a II_1 factor, one can construct a copy of $R = \overline{\otimes}_n(\mathrm{M}_{2\times 2}, \mathrm{tr})_n$ inside any II_1 factor M. A remarkable theorem of Connes shows that all *amenable* II_1 factors are AFD and thus isomorphic to R ([C76]). In particular II_1 factors of the form $L^\infty(X) \rtimes \Gamma$ with Γ amenable, and all their subfactors, are isomorphic to R. Similarly, by ([OW80], [CFW81]), all free ergodic actions of infinite amenable groups are OE and any two Cartan subalgebras of R are conjugate by an automorphism of R. The outer automorphism group of R is huge, in fact any separable locally compact group Γ acts faithfully of R by outer automorphisms (e.g. if Γ is countable discrete then the "non-commutative" Bernoulli action $\Gamma \curvearrowright R = \overline{\otimes}_{g\in\Gamma}(\mathrm{M}_{2\times 2}(\mathbb{C}), \mathrm{tr})_g$ is properly outer) and the group of inner automorphisms $\mathrm{Int}(R) = \{\mathrm{Ad}(u) \mid u \in \mathcal{U}(R)\}$ is dense in $\mathrm{Aut}(R)$, when the latter is endowed with the natural Polish group structure given by pointwise convergence in $\|\cdot\|_2$.

1.6. Amplifications and the fundamental group. The "continuous dimension" phenomenon allows defining the algebra of "t by t matrices" over a II_1 factor M, or *amplification* of M by t, M^t, for any positive real numbers t: First note that if $p \in \mathcal{P}(M)$ then the algebra pMp, with normalized trace $\tau(\cdot)/\tau(p)$, is a II_1 factor. Similarly if $n \geq 1$ is an integer then $\mathrm{M}_{n\times n}(M) \simeq \mathrm{M}_{n\times n}(\mathbb{C}) \otimes M$ is a II_1 factor, with the normalized trace $\tau((x_{ij})_{i,j}) = \Sigma_i \tau(x_{ii})/n$. With this in mind, for $t > 0$ define M^t to be the (isomorphism class of the) algebra $p\mathrm{M}_{n\times n}(M)p$, where $n \geq t$ is an integer and $p \in \mathrm{M}_{n\times n}(M)$ is a projection of (normalized) trace t/n.

Rather than studying only isomorphisms between II_1 factors associated with actions, one considers *stable isomorphisms* (stable vNE) $L^\infty(X) \rtimes \Gamma \simeq (L^\infty(Y) \rtimes \Lambda)^t$ and respectively *stable orbit equivalence* $\mathcal{R}_\Gamma \simeq \mathcal{R}_\Lambda^t$ of actions $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$, where $\mathcal{R}_\Lambda^t$ is the equivalence relation on a subset Y_0 of measure t/n of $Y \times \{1, 2, \ldots, n\}$ obtained by restriction to Y_0 of the product between $\mathcal{R}_\Lambda$ and the transitive relation on the n-point set, for some $n \geq t$. It is easy to see that $\mathcal{R}_\Lambda^t$ is itself implementable by a countable $\Lambda' \subset \mathrm{Aut}(Y_0, \mu)$. We write $L^\infty(Y)^t$ for $L^\infty(Y_0)$.

Since both vNE and OE isomorphisms can be "amplified", stable vNE and OE are equivalence relations and $(M^s)^t = M^{st}$. The *fundamental group* of a II_1 factor M (resp. of an equivalence relation $\mathcal{R}_\Gamma$ implemented by an ergodic action $\Gamma \curvearrowright X$) is defined by $\mathcal{F}(M) \stackrel{\mathrm{def}}{=} \{t > 0 \mid M^t \simeq M\}$ (resp. $\mathcal{F}(\mathcal{R}_\Gamma) \stackrel{\mathrm{def}}{=} \{t > 0 \mid \mathcal{R}_\Gamma^t \simeq \mathcal{R}_\Gamma\}$).

An amplification of an AFD factor is clearly AFD. Thus, $\mathcal{F}(R) = \mathbb{R}_+^*$. Similarly, if $\mathcal{R}$ denotes the (unique) amenable equivalence relation implemented by any free ergodic action of an infinite amenable group, then $\mathcal{F}(\mathcal{R}) = \mathbb{R}_+^*$.

1.7. Representations of finite algebras (Hilbert modules). If (M, τ) is a finite von Neumann algebra then $L^2(M)$ denotes the completion of M in the norm $\|\cdot\|_2$ given by the trace, then M can be represented on $L^2(M)$ by left multiplication operators, as a von Neumann algebra. This is the *standard representation* of M.

If $(M, \tau) = (L^\infty X, \int \cdot \mathrm{d}\mu)$ then $L^2(M)$ coincides with $L^2(X)$, and each $\xi \in L^2(M) = L^2(X)$ can be viewed as the closed (densely defined) operator of (left)

multiplication by ξ, with the spectral resolution of $|\xi|$ and the partial isometry $u = \xi|\xi|^{-1}$ all lying in $L^\infty(X)$. For arbitrary (M, τ), $L^2(M)$ can be similarly identified with the (densely defined) closed linear operators ξ on $L^2(M)$, containing M in their domain, with $|\xi| = (\xi^*\xi)^{1/2}$ having spectral resolution $e_t, t \geq 0$, in M and $u = \xi|\xi|^{-1}$ in M as well. The fact that the vector 1 is in the domain of ξ is equivalent to ξ being "square integrable", i.e. $\int t^2 \mathrm{d}\tau(e_s) < \infty$. Similarly, the completion of M in the norm $\|x\|_1 = \tau(|x|)$, denoted $L^1(M)$, can be identified with the space of closed linear operators ξ on M with polar decomposition $\xi = u|\xi|$ satisfying $u \in M$, $|\xi|^{1/2} \in L^2(M)$. One has $(L^1(M))^* = M$, i.e. $L^1(M)$ is the predual of M.

In fact, M acts on $L^2(M)$ by right multiplication as well, giving this way the standard representation of M^{op} (the "opposite" of the algebra M). The left-right multiplication algebras M, M^{op} commute, one being the commutant of the other. If one extends the antilinear isometric map $J_M(x) = x^*$ from M to $L^2(M)$ by density, then $J_M^2 = \mathrm{id}$ and for each $x \in M$, viewed as left multiplication operator on $L^2(M)$, $J_M x J_M$ gives the operator of right multiplication by x^*. Thus, $M^{\mathrm{op}} = J_M M J_M = M'$.

Any other (separable) representation $M \subset \mathcal{B}(\mathcal{H})$ of M as a von Neumann algebra (or *left Hilbert M-module* $\mathcal{H}$) is of the form $\mathcal{H} \simeq \oplus_n L^2(M)p_n$, for some $\{p_n\}_n \subset \mathcal{P}(M)$, with the action of M by left multiplication. If M is a factor, the number $\dim_M \mathcal{H} \stackrel{\mathrm{def}}{=} \Sigma_n \tau(p_n) \in [0, \infty]$ characterizes the isomorphism class of $\mathcal{H}$. The M-module $\mathcal{H}$ can then be alternatively described as the (left) M-module $e_{11}L^2(\mathrm{M}_{n\times n}(M))p$, where $n \geq \dim \mathcal{H}$, $e_{11} \in \mathrm{M}_{n\times n}(\mathbb{C})$ is a one dimensional projection and $p \in \mathcal{P}(\mathrm{M}_{n\times n}(M))$ has (normalized) trace equal to $\dim \mathcal{H}/n$. Thus, the commutant M' of M in $\mathcal{B}(\mathcal{H})$ is a II_1 factor iff $\dim_M \mathcal{H} < \infty$ and if this is the case then $M' \simeq (M^t)^{\mathrm{op}}$, where $t = \dim_M \mathcal{H}$. For general finite von Neumann algebra M, M' is finite iff $\Sigma_n \mathrm{Ctr}(p_n)$ is a densely defined operator in $\mathcal{Z}(M)$.

2. Some II_1 factor tools

Thus, a free ergodic m.p. action $\Gamma \curvearrowright X$ of an infinite group on a non-atomic probability space gives rise to a II_1 factor $M = L^\infty(X) \rtimes \Gamma$ with trace extending the integral on $L^\infty(X)$ and a natural pre-Hilbert space structure. Elements $x \in M$ have Fourier-like expansion, $x = \Sigma_g a_g u_g$, with coefficients in $L^\infty(X)$ and "basis" $\{u_g\}_g$ made out of unitary elements that satisfy $u_g u_h = u_{gh}$ and implement the Γ-action on $L^\infty(X)$, by $u_g a u_g^* = g(a)$. Spectral analysis and distribution behavior of elements in M already reveal the dynamical properties of the group action. But in order to get proper insight into the structure of a II_1 factor, for instance to recapture from the isomorphism class of $M = L^\infty(X) \rtimes \Gamma$ the initial building data $\Gamma \curvearrowright X$ (or part of it), we need to complement such *local von Neumann algebra analysis* tools with more *global* ones, some of which we briefly explain in this section.

2.1. Hilbert bimodules and c.p. maps. While the Hilbert modules of a II_1 factor M reflect so nicely the continuous dimension phenomenon, they do not provide any actual insight into specific properties of M, the way a "good" representation theory should do. It was Connes who discovered, in the early 80s, that the appropriate representation theory for a II_1 factor M is given by the *Hilbert M-bimodules*, i.e. Hilbert spaces $\mathcal{H}$ with commuting von Neumann algebra representations $M, M^{\mathrm{op}} \subset \mathcal{B}(\mathcal{H})$ ([C82]). Moreover, the same way the GNS construction provides an equivalence between unitary representations of a group and its positive definite functions, Hilbert M-bimodules can be "encoded" into a *completely positive* (c.p.) *map* $\phi\colon M \to M$, i.e. a linear map with all amplifications $\phi^n = \phi \otimes \mathrm{id}$ on $\mathrm{M}_{n\times n}(M) \simeq M \otimes \mathrm{M}_{n\times n}(\mathbb{C})$, $n \geq 1$, positive.

This proved to be a deep, important idea at the conceptual level. Thus, Connes–Jones used this point of view in ([CJ85]) to define the property (T) for abstract II_1 factors M, by requiring: there is a finite $F \subset M$ and $\varepsilon > 0$ such that if $\mathcal{H}$ has a unit vector with $\|y\xi - \xi y\| \leq \varepsilon$ for all $y \in F$, then $\mathcal{H}$ contains a non-zero central vector ξ_0, i.e. $x\xi_0 = \xi_0 x$ for all $x \in M$. They proved that this is equivalent to the following condition for c.p. maps: for all ε_0 there is a finite $F \subset M$ and $\delta > 0$ such that if a subunital subtracial c.p. map $\phi\colon M \to M$ satisfies $\|\phi(y) - y\|_2 \leq \delta$ for all $y \in F$, then $\|\phi(x) - x\|_2 \leq \varepsilon$ for all x in the unit ball $(M)_1$ of M. Moreover, they pointed out that all the representation theory of a group Γ is reflected into the "representation theory" of a II_1 factor $L^\infty(X) \rtimes \Gamma$ of the group action $\Gamma \curvearrowright X$, since any positive definite function φ on Γ gives rise to a c.p. map $\phi = \phi_\varphi$, by $\phi(\Sigma a_g u_g) = \Sigma_g \varphi(a_g) u_g$. This led to a notion of Haagerup property for abstract II_1 factors and the proof that property (T) II_1 factors cannot be embedded into factors having this property ([CJ85]). It also led to several generalizations of all these notions in ([P86], [P01b]), as also explained in Section 6, and more recently to the construction of new cohomology theories for II_1 factors ([CSh04], [Pe04]).

Note that any automorphism of M, and more generally endomorphism $\theta\colon M \to M$ (not necessarily unital), is subunital subtracial c.p. map. Thus, c.p. maps can be viewed as "generalized symmetries" of M, or as a very general notion of *morphisms* of M into itself. This latter point of view was also present in work of Effros–Lance ([EL77]) and Haagerup ([H79], [CaH85], [CoH89]), and is now central to the theory of operator spaces. Altogether, c.p. maps, or equivalently Hilbert bimodules (also called *correspondences* by Connes [C82]) provide a key "global tool" in the study of II_1 factors.

2.2. Subalgebras and the basic construction. The study of subalgebras of a II_1 factor M is an important part of the theory of von Neumann algebras, one of the most interesting aspects of which is Jones far reaching theory of subfactors ([J83], [J90]). For us here, the consideration of subalgebras of M is mostly in relation to recovering the initial construction of M. For instance, if $\theta\colon L^\infty(X)\rtimes\Gamma \simeq L^\infty(Y)\rtimes\Lambda$ is an isomorphism, then we need to relate the positions of $P = \theta(L^\infty(X))$ (resp. $P = \theta(L\Gamma)$) and $N = L^\infty(Y)$ (resp. $N = L\Lambda$) inside $M = L^\infty(Y) \rtimes \Lambda$.

If (M, τ) is a finite von Neumann algebra then any von Neumann subalgebra N of M is finite, with $\tau_{|N}$ its faithful normal trace. The closure of N in the Hilbert space $L^2(M)$ is clearly isomorphic to $L^2(N)$ and a Radon–Nikodym type theorem shows that the orthogonal projection e_N of $L^2(M)$ onto $L^2(N) \subset L^2(M)$ takes M (as a subspace of $L^2(M)$) onto N. The restriction of e_N to M, denoted E_N, gives a τ-preserving projection of M onto N. Moreover $E_N(M_+) = N_+$ and E_N is N-bilinear, i.e. E_N is a conditional expectation of M onto N. Moreover, E_N is the unique expectation which preserves τ.

When viewed as operators on the Hilbert space $L^2(M)$, $x \in M$ and e_N satisfy the relations: (a) $e_N x e_N = E_N(x)e_N$; (b) $x \in N$ iff $[x, e_N] = 0$. Let $\langle M, e_N\rangle$ denote the von Neumann algebra generated in $\mathcal{B}(L^2(M))$ by M and e_N. Since we have $\vee\{x(e_N(L^2(M))) \mid x \in M\} = L^2(M)$, from (a), (b) it follows that $\mathrm{span} M e_N M$ is a *-algebra with support equal to 1 in $\mathcal{B}(L^2(M))$. Thus, $\langle M, e_N\rangle = \overline{\mathrm{sp}}^{\mathrm{w}}\{x e_N y \mid x, y \in M\}$. Also, $\langle M, e_N\rangle = (J_M N J_M)'$, $e_N\langle M, e_N\rangle e_N = N e_N$, implying that there are projections $p_n \nearrow 1$ in $\langle M, e_N\rangle$ such that $p_n\langle M, e_N\rangle p_n$ is a finite von Neumann algebra. Thus, $\langle M, e_N\rangle$ is a *semifinite von Neumann algebra* and it is finite iff $\dim_N L^2(M) < \infty$ (in the sense explained in 1.6). This is the *Jones basic construction* for $P \subset M$ ([J83]). The algebra $\langle M, e_N\rangle$ is endowed with a densely defined trace Tr by $\mathrm{Tr}(\Sigma_i x_i e_N y_i) = \Sigma_i \tau(x_i y_i)$, for x_i, y_i finite sets of elements in M. One denotes $L^2(\langle M, e_N\rangle, \mathrm{Tr})$ the completion of $\mathrm{sp} M e_N M$ in the norm $\|x\|_{2,\mathrm{Tr}} = \mathrm{Tr}(x^*x)^{1/2}$, $x \in \mathrm{sp} M e_N M$.

Any Hilbert subspace of $L^2(M)$ which is invariant under multiplication to the right by elements in N is a right Hilbert N-module (i.e. a left N^{op} module). If $\mathcal{H} \subset L^2(M)$ is a Hilbert subspace and f is the orthogonal projection onto $\mathcal{H}$ then $\mathcal{H}N = \mathcal{H}$ (i.e. $\mathcal{H}$ is a right N-module) iff f lies in $\langle M, e_N\rangle$. The right Hilbert N-module $\mathcal{H} \subset L^2(M)$ is invariant to multiplication from the left by a von Neumann subalgebra $P \subset M$, i.e. $P\mathcal{H} \subset \mathcal{H}$, iff $f \in P' \cap \langle M, e_N\rangle$. Although all subalgebras we consider have infinite Jones index, the idea of viewing $L^2(M)$, as well as subspaces $\mathcal{H} \subset L^2(M)$ with $P\mathcal{H}N = \mathcal{H}$, as $P - N$ Hilbert bimodules, and the use of the basic construction as framework, came from developments in the theory of subfactors (e.g. [PiP86], [P86], [P94], [P97]).

3. Prototype vNE and OE rigidity statements

While all II_1 factors (resp. equivalence relations) arising from ergodic actions of amenable groups look alike, in the non-amenable case the situation is very complex and rigidity phenomena were already detected at early stages of the subject ([MvN43], [D63], [Mc70], [C75], etc). Our aim in the rest of the paper is to investigate more "extreme" such rigidity phenomena, where for certain "small classes" of group actions the reverse of the implications "conjugacy $\Rightarrow$ OE $\Rightarrow$ vNE" hold true as well. Typically, we fix a class of *source* group actions $\Gamma \curvearrowright (X, \mu)$ and a class of *target* actions $\Lambda \curvearrowright (Y, \nu)$, each of them characterized by a set of suitable assumptions, then attempt

to show that the isomorphism of their group measure space algebras (vNE) entails isomorphism of the groups, or orbit equivalence of the actions (OE) or, ideally, the following type of statement:

(3.1). *Under the given conditions on the source* $\Gamma \curvearrowright X$ *and target* $\Lambda \curvearrowright Y$*, if* $\theta\colon L^\infty(X) \rtimes \Gamma \simeq (L^\infty(Y) \rtimes \Lambda)^t$*, then* $t = 1$ *and there exist a unitary element* $u \in \mathcal{U}(L^\infty(Y) \rtimes \Lambda)$*,* $\gamma \in \mathrm{Hom}(\Lambda, \mathbb{T})$ *and isomorphisms* $\Delta\colon X \simeq Y$*,* $\delta\colon \Gamma \simeq \Lambda$ *implementing a conjugacy of the actions, such that* $\theta = \mathrm{Ad}(u) \circ \theta^\gamma \circ \theta^{\Delta,\delta}$*, where* θ^γ *is the automorphism of* $L^\infty(Y) \rtimes \Lambda$ *implemented by* γ *and* $\theta^{\Delta,\delta}\colon L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$ *the algebra isomorphism implemented by the conjugacy.*

When the context concerns free ergodic actions, we call (3.1) a *vNE strong rigidity* statement. While we do indeed obtain such results, other results will only go as far as showing that there exists a unitary element in the target algebra $u \in (L^\infty(Y) \rtimes \Lambda)^t$ such that $\mathrm{Ad}(u) \circ \theta$ takes $L^\infty(X)$ onto $L^\infty(Y)^t$, a type of result we call *vNE/OE rigidity*.

Note that this latter statement is stronger than just showing vNE $\Rightarrow$ OE for the specific classes of group actions involved. Indeed, this implication would only require proving there exists an automorphism θ_0 of the target factor such that $\theta_0 \circ \theta$ takes $L^\infty(X)$ onto $L^\infty(Y)$. While the vNE/OE version of (3.1) requires the θ_0 to be inner! If the groups Γ, Λ in (3.1) are amenable, when by ([C76]) the resulting group measure space factors are all isomorphic to R, there always exists an automorphism θ_0 taking $L^\infty(X)$ onto $L^\infty(Y)$, by ([CFW81]), but there are uncountably many ways of decomposing R as $L^\infty(X_i) \rtimes \mathbb{Z}$, with $\mathbb{Z} \curvearrowright X_i$ isomorphic actions, without the Cartan subalgebras $L^\infty(X_i) \subset R$ being unitarily conjugated in R (cf. [FM77]).

The vNE/OE rigidity results can be further complemented with OE rigidity results from ergodic theory (e.g. [G01], [Fu99a], [MoSh02]), to recuperate the isomorphism class of the group, or derive that $t = 1$. Taking the same action $\Gamma \curvearrowright X$ as source and target gives information about $\mathrm{Out}(M) = \mathrm{Aut}(M)/\mathrm{Int}(M)$ and $\mathcal{F}(M)$ for $M = L^\infty(X) \rtimes \Gamma$.

If from the hypothesis of (3.1) we can only derive $\Gamma \simeq \Lambda$, then one calls it a *vNE rigidity* result. The group algebra case of such a rigidity statement, with the assumptions on both groups to have property (T), corresponds to *Connes Rigidity Conjecture* ([C82]):

(3.2). *If* Γ, Λ *are ICC property* (T) *groups and* $L\Gamma \simeq L\Lambda$ *then* $\Gamma \simeq \Lambda$

The case when X is a single point set of (3.1) then becomes the following stronger form of Connes's conjecture (see [J00]):

(3.2′). *If* Γ *is a property* (T) *group,* Λ *an arbitrary ICC group and* $\theta\colon L\Gamma \simeq (L\Lambda)^t$*, then* $t = 1$ *and there exist a unitary* $u \in \mathcal{U}(L\Lambda)$*), an isomorphism* $\delta\colon \Gamma \simeq \Lambda$ *and* $\gamma \in \mathrm{Hom}(\Lambda, \mathbb{T})$ *such that* $\theta = \mathrm{Ad}(u) \circ \theta^\gamma \circ \theta^\delta$*, where* θ^γ *is the automorphism of* $L\Lambda$ *implemented by* γ *and* $\theta^\delta\colon L\Gamma \simeq L\Lambda$ *the isomorphism implemented by* δ*.*

Note that although (3.2′) assumes property (T) only on the source group Γ, giving the statement a "superrigidity" flavor, the property (T) for Λ is automatic from the

isomorphism $L\Gamma \simeq (L\Lambda)^t$, due to results in ([CJ85]). The case $\Gamma = \Lambda$ in $(3.2')$ amounts to showing that $\mathrm{Out}(L\Gamma) \simeq \mathrm{Hom}(\Gamma, \mathbb{T}) \rtimes \mathrm{Out}(\Gamma)$ and $\mathcal{F}(L\Gamma) = \{1\}$. Connes' breakthrough rigidity result ([C80]), leading to his conjecture (3.2), shows that both groups are countable, being a verification "up to countable classes" of the formulas. To this date, the only other insight into Connes rigidity conjecture are the results of Connes–Jones, showing that $L(\mathrm{SL}(n, \mathbb{Z}))$, $n \geq 3$, cannot be embedded into $L(\mathrm{SL}(2, \mathbb{Z}))$ ([CJ85]), and of Cowling–Haagerup, showing that if Γ_n are lattices in $\mathrm{Sp}(n, 1)$ and $L(\Gamma_n) \subset L(\Gamma_m)$ then $n \leq m$ ([CoH89]).

If the isomorphism θ in (3.1) comes from a stable OE of free ergodic actions (so $\theta(L^\infty(X)) = (L^\infty(Y))^t$ by hypothesis), then (3.1) amounts to deriving conjugacy from OE, a statement labeled *OE strong rigidity* in ([Fu99b], [MoSh02]). The "ideal" such statement is when there are no restrictions at all on the "target" side, in which case it qualifies as *OE superrigidity* result. If only the isomorphism of the groups is derived, it is called *OE rigidity*. This type of result already appeared in early 80s, in pioneering work of Zimmer ([Z80], [Z84]). Thus, using his celebrated cocycle superrigidity theorem, itself a generalization of Margulis Superrigidity, he proved that free ergodic m.p. actions of the groups $\mathrm{SL}(n, \mathbb{Z})$, $n = 2, 3, \ldots$, are orbit inequivalent for different n's. Other OE rigidity results followed ([M82], [GeGo88]). By late 90s OE superrigidity phenomena started to unveil in the work of Furman, who added new ideas to the approach in ([Z91]) to derive that, more than just being rigid, actions of higher rank lattices such as $\mathrm{SL}(n, \mathbb{Z}) \curvearrowright \mathbb{T}^n$, $n \geq 3$, are in fact *OE superrigid*, i.e. any orbit equivalence between such an action and an arbitrary free m.p. action of a discrete group Λ comes from a conjugacy ([Fu99a, Fu99b]). Another important development on the OE side came with the work of Gaboriau who introduced a series of OE numerical-invariants for equivalence relations, allowing him to show that free m.p. actions of the free groups $\mathbb{F}_n$ are OE inequivalent for different $n \geq 1$ ([G00, G01]). A new set of OE superrigidity results was then established by Monod–Shalom, for doubly ergodic actions of products of word-hyperbolic groups ([MoS02]; see [Mo06], [S05] for survey articles).

These OE rigidity results were obtained by using a multitude of techniques, but all in measure theoretic framework. By 2001, vNE/OE rigidity started to emerge as well ([P01b]). Combined with ([G00]), they led to the first vNE rigidity results, where isomorphism of groups could be deduced from isomorphism of group measure space algebras, and factors with trivial fundamental group could be exhibited ([P01b]; see Section 7). Shortly after, vNE strong rigidity results of the form (3.1) were proved by using exclusively II_1 factor framework ([P03], [P04a]; see Section 8). They provided completely new OE superrigidity results as well, obtained this time with von Neumann algebra methods ([P04a], [P05]; see Section 9; also [V06] for a combined presentation of these vNE and OE results).

4. Proving rigidity "up to countable classes"

Before discussing the "precise" rigidity results mentioned above, we explain a method for deriving vNE and OE rigidity statements "up to countable classes", which grew out of Connes' initial rigidity paper ([C80]). Thus, by using the separability of the Hilbert space $L^2(M)$ of a II_1 factor M and the observation that two copies of the left regular representation λ_1, λ_2 of Γ into M that are sufficiently close on a set of generators of Γ can be intertwined in M, it was shown in ([P86]) that in fact all II_1 factors of the form $M = L^\infty(X) \rtimes \Gamma$, with Γ a property (T) group, have countable fundamental group. Moreover, if the generators of a property (T) II_1 subfactor N_1 of a separable II_1 factor M are almost contained into another subfactor $N_2 \subset M$, then a "corner" of N_1 can be unitarily conjugated into N_2. By separability of M this showed that M contains at most countably many property (T) subfactors up to stable isomorphism ([P86]).

These are typical examples of what we call *separability arguments*, leading to rigidity statements "up to countable classes". They perfectly illustrate the power of the II_1 factor framework. Such arguments were revived a few years ago, leading to new applications ([P01b], [Hj02], [Oz02], [GP03]). Thus, Hjorth proved that an infinite property (T) group Γ has uncountably many non-OE actions ([Hj02]). Since by ([CW80], [Sc81]) any non-amenable, non(T) group has at least two non-OE free ergodic m.p. actions, this shows that any non-amenable group has at least two non-OE actions (in fact even non-vNE). His proof starts by noticing that a property (T) group Γ has uncountably many non-conjugate actions σ_i (using Gaussian actions to produce the family). If there exist only countably many equivalence relations, then there must be uncountably many σ_i with same OE class $\mathcal{R}_\Gamma$. The σ_i's give copies λ_i of the left regular representations in the normalizer of $L^\infty(X)$ in $L(\mathcal{R}_\Gamma)$. As in ([P86]), by separability there exist $i \neq j$ such that λ_i and λ_j can be intertwined by some $b \neq 0$ in $M = L(\mathcal{R}_\Gamma)$. Additional work shows that b can be "pushed" into the normalizer of $L^\infty(X)$, implying that σ_i, σ_j are conjugate, contradiction.

Another illustration is Ozawa's proof ([Oz02]) that there exists no separable II_1 factor M containing isomorphic copies of any separable II_1 factor (not-necessarily with same unit as M): By a theorem of Gromov there exists a property (T) group Γ with uncountably many non-isomorphic simple quotients Γ_i. Assuming there exists a separable II_1 factor M with $L(\Gamma_i) \subset M$ for all i, by the same separability argument as above for λ_i's the left regular representation of Γ_i, but all viewed as representations of the group Γ, one gets an intertwiner between λ_i, λ_j for some $i \neq j$. This implies $\Gamma_i \simeq \Gamma_j$, contradiction.

In this same vein, let us note that by using a theorem of Shalom in ([Sh00]), showing that any property (T) group is a quotient of a finitely presented property (T) group (only countably many of which exist), separability arguments as above show that Connes rigidity conjecture (3.2) does hold true "up to countable classes", i.e. the functor $\Gamma \mapsto L\Gamma$ on ICC property (T) groups is (at most) countable to 1. Indeed, because if $M = L\Gamma_i$ for uncountably many non-isomorphic groups Γ_i, then

by ([Sh00]) we may assume they are all quotients of the same property (T) group Γ, and the previous separability argument gives a contradiction. Similarly one can prove that the strong rigidity conjecture (3.2′) holds true "modulo countable classes".

On the OE side, the same argument shows that there are at most countably many mutually measure equivalent (ME) property (T) groups (recall from [Fu1] that Γ is ME to Λ if there exist free ergodic m.p. actions $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$ which are stably OE). In other words, the following holds true "modulo countable classes": *If two property* (T) *groups are measure equivalent then they are virtually isomorphic*.

A separability argument was also used to prove that free groups have uncountably many OE inequivalent actions, in ([GP03]): One starts by showing that for all $\mathbb{F}_n \curvearrowright X$ free, with one generator acting ergodically, there exists an increasing "continuous" family of sub-equivalence relations $\mathcal{R}_{\mathbb{F}_n,t} \subset \mathcal{R}_{\mathbb{F}_n}$, $0 < t \leq 1$, each one implemented by a free ergodic m.p. action of $\mathbb{F}_n$. Taking the initial $\mathbb{F}_n$-action to be the restriction to $\mathbb{F}_n \subset \mathrm{SL}(2,\mathbb{Z})$ of the natural action $\mathrm{SL}(2,\mathbb{Z}) \curvearrowright \mathbb{T}^2 = \hat{\mathbb{Z}}^2$ and using the rigidity of this action (see 5.3), it follows from ([P01b]) that $\mathcal{R}_{\mathbb{F}_n,t}$ are rigid for $t \geq c$, for some $c < 1$. Then a separability argument is used to show that $\mathcal{R}_{\mathbb{F}_n,t}$, $t \in [c, 1]$ (in fact even the II_1 factors $L(\mathcal{R}_{\mathbb{F}_n,t})$) are mutually non-isomorphic modulo countable classes.

Thus, separability arguments can be used to prove rigidity results in many situations, often without too much work, but they give the answer only "up to countable classes". However, such arguments brought up the following simple fact, specific to II_1 factor framework, which is useful in proving "precise" rigidity results as well: If a group Γ has property (T), then *all* its representations into a II_1 factor are isolated. More precisely, if M is a II_1 factor, (F, ε) gives the critical neighborhood of the trivial representation of Γ and $\pi_i : \Gamma \to \mathcal{U}(p_i M p_i)$, $i = 1, 2$, satisfy $\|\pi_1(h) - \pi_2(h)\|_2 < \varepsilon \|p_1 p_2\|_2$ for all $h \in F$, then there exists a non-zero partial isometry v in M such that $\pi_1(g)v = v\pi_2(g)$ for all $g \in \Gamma$.

5. Techniques for intertwining subalgebras

Let $\theta : L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$ be an isomorphism of II_1 factors associated with free ergodic m.p. actions $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$, as in (3.1). Denote by M the target factor $L^\infty(Y) \rtimes \Lambda$, with $\{v_h\}_h$ its canonical unitaries, while u_g denotes the canonical unitaries in the source factor $L^\infty(X) \rtimes \Gamma$. For simplicity, we identify $L^\infty(X) \rtimes \Gamma$ with M via θ. Proving a statement like (3.1) means finding a unitary $u \in M$ that conjugates $P = L^\infty(X)$ onto $N = L^\infty(Y)$, and possibly $\{u_g\}_g$ into $\{\mathbb{T}v_h\}_h$ (simultaneously!).

This is difficult even if we somehow know that P, N are uniformly close one to another, but careful averaging techniques can be used to derive the desired conclusion. However, not being allowed "countable error", as in Section 4, there is no reason an isomorphism θ would take one structure close to the other, even on finite sets. This fact constitutes a major obstacle in getting "precise" vNE rigidity results. Moreover,

the Connes–Jones example ([CJ82]), where a group of the form $\Gamma = \Gamma_0 \times \Gamma_1$, with Γ_0 property (T) and Γ_1 an infinite product of non-commutative groups, is shown to have two non-OE free ergodic actions that give the same von Neumann algebra, suggests that vNE rigidity may in fact not occur.

Such problems were overcome in recent years due to a combination of two new ideas and sets of techniques, that we call *deformation/rigidity* and *intertwining subalgebras* (cf. [P01b], [P03], [P04a]).

The intertwining technique establishes some efficient criteria for deciding whether two von Neumann subalgebras P, N of a II_1 factor M can be conjugated one into the other by a unitary element in M, or more generally if one can find $b \in M$ such that $pPpb \subset bN$, for some $p \in \mathcal{P}(P)$ with $pb \neq 0$. If such an "intertwiner" b exists, we write $P \prec_M N$. Of equal importance in this problematic are the techniques for evaluating relative commutants $P' \cap M$ and normalizers $\mathcal{N}(P) = \{u \in \mathcal{U}(M) \mid uPu^* = P\}$ of subalgebras $P \subset M$, which we view as part of the theory of "intertwining subalgebras".

The first criteria for whether $P \prec_M N$ and for estimating $P' \cap M$, $\mathcal{N}(P)''$ appeared in ([P83]; see also [P91]), but for particular classes of factors M and subalgebras. The general criteria below, which give several equivalent characterizations of $P \prec_M N$, is due to insight gained during 1983–1997 in the study of subalgebras of finite Jones index in ([PiP86], [P86], [P91], [P94], [P97]):

Theorem 5.1 ([P01b], [P03]). *Let (M, τ) be a finite von Neumann algebra and $P, N \subset M$ von Neumann subalgebras. The following are equivalent:*

(i) $P \prec_M N$.

(ii) *There exists a Hilbert $P - N$ bimodule $\mathcal{H} \subset L^2(M)$ such that* $\dim \mathcal{H}_N < \infty$.

(iii) *There exists a non-zero projection $f \in P' \cap \langle M, e_N \rangle$ such that* $\mathrm{Tr}(f) < \infty$.

(iv) *There exist projections $p \in P$, $q \in N$ a unital isomorphism $\psi : pPp \to qNq$ (not necessarily onto) and a partial isometry $v \in M$ such that $vv^* \in pPp' \cap pMp$, $v^*v \in \psi(pPp)' \cap qMq$ and $xv = v\psi(x)$ for all $x \in pPp$.*

Moreover, non-(i) *is equivalent to:*

($\bar{\mathrm{v}}$) *For all $a_1, \ldots, a_n \in M$ and for all $\varepsilon > 0$ there exists $u \in \mathcal{U}(P)$ such that $\|E_N(a_i u a_j)\|_2 \leq \varepsilon$ for all i, j.*

This is the "core" result in the series of criteria which constitute the intertwining subalgebras techniques.

Condition ($\bar{\mathrm{v}}$) is very useful as a starting point in contradiction arguments. It is also useful in order to get some information about elements in the algebra P, in case one knows that P cannot satisfy $P \prec_M N$, for instance because it cannot be embedded into N (e.g. if say N is abelian and P is type II_1).

Condition (iv) is of course the one we seek when we expect P to be unitary conjugated into N. It is however non-trivial to get from (iv) a unitary u with $uPu^* \subset N$, because one cannot apriori control the relative commutant of the image of the isomorphism ψ (of which we only know it exists). This is solved on a case by case basis, by arguments in the spirit of ([P83]). It is in fact condition ($\bar{\text{v}}$) that allows controlling the relative commutant of the algebra P, in many situations.

An important case when the relative commutants and normalizers can be accurately estimated is if $M = L^\infty(Y) \rtimes \Lambda$ comes from a free mixing action $\Lambda \curvearrowright Y$. Thus, if one denotes $N = L\Lambda$ and take a diffuse subalgebra $Q \subset N$, then $Q' \cap M \subset N$, in fact all the normalizer of Q in M is contained in N. This implies that whenever ψ, v are as in (iv) then $v^*v \in N$ and further work gives the unitary u ([P03]). Other situations when this can be resolved is if $M = N \mathbin{\overline{\otimes}} N_0 = P \mathbin{\overline{\otimes}} P_0$ ([OzP04]; see also 6.6 below), or if M is a free product $M = N * N_0$ ([Oz04], [IPeP05]).

For general vNE rigidity problems it is particularly important to deal with the case when both P, N are maximal abelian in M (Cartan subalgebras). In this case one can overcome the "relative commutant issue" altogether, and get from (iv) a unitary element that conjugates P onto N ([P01b]). However, the proof of the (3.1)-type vNE strong rigidity result in ([P03], [P04a]; see Section 8) will only use the criterion for conjugating Cartan subalgebras after first showing that $L\Gamma$, $L\Lambda$ can be unitary conjugate onto each other, by using 5.1 and deformation/rigidity. Then $L\Gamma \prec_M L\Lambda$ is shown to imply $L^\infty(X)$ unitary conjugate to $L^\infty(Y)$, under no other assumptions but some good mixing conditions on the actions (see [P04a]). The proof of this implication does use a lot 5.1 and the criterion for conjugating Cartan subalgebras, but combined with lengthy, hard asymptotic analysis in the ultrapower factor M^ω. It is the most difficult result in this series of intertwining techniques. One then proves that $L\Gamma \prec_M L\Lambda$ and $L^\infty(X) \prec_M L^\infty(Y)$ implies there exists $u \in \mathcal{U}(M)$ that conjugates simultaneously $L^\infty(X)$ onto $L^\infty(Y)$ and $L\Gamma$ onto $L\Lambda$, which in turn implies $\mathrm{Ad}\, u$ takes $\{u_g\}_g$ into scalar multiples of $\{v_h\}_h$ as well.

Specific intertwining results can be obtained when the unit ball of P is "almost contained" in a subalgebra N of M, i.e. $\|E_N(x) - x\|_2 \leq \varepsilon$ for all $x \in P$, $\|x\| \leq 1$, for some small $\varepsilon > 0$. A pioneering such result appeared in ([Ch79]), where the basic construction framework $\langle M, e_N \rangle$ was for the first time used. Theorem 5.1 does cover also such cases, as P almost contained in N trivially implies $P' \cap \langle M, e_N \rangle$ has finite non-zero projections. A detailed analysis of how to get from this a unitary conjugacy is carried out in ([P01b], [PSS04]), using subfactor methods.

6. Deformation and rigidity in II_1 factors

As the discussion in the previous section shows, in order to recapture the building data of a group measure space factor, or at least part of it, it is sufficient to fit into one of the equivalent conditions of the criteria for intertwining subalgebras. For instance, to prove (3.1)-type results it is sufficient, by Section 5, to obtain finite dimensional

$L^\infty(X)-L^\infty(Y)$ and $L\Gamma-L\Lambda$ Hilbert bimodules in $M = L^\infty(X)\rtimes\Gamma = L^\infty(Y)\rtimes\Lambda$.

Our strategy for producing such finite dimensional bimodules is to use deformability properties of the target group action and rigidity properties of the source group action. The method, which we call *deformation/rigidity*, works only when both conditions are met, taking a concrete technical form on a case by case basis. So first of all we need to single out classes of group actions whose associated factors satisfy both rigidity and deformability properties.

It is the II_1 factor framework that makes this approach possible, as these algebras are particularly well adapted to deformations: by automorphisms, c.p. maps, completely bounded maps, etc. For us here, by a *deformation* of the identity id_M of a II_1 factor M, we mean a sequence ϕ_n of subunital, subtracial, c.p. maps on M such that $\lim_n \|\phi_n(x) - x\|_2 = 0$ for all $x \in M$. The maps ϕ_n of the deformations will frequently be automorphisms, but also conditional expectations and c.p. maps coming from positive definite functions on the group (for factors coming from group actions). The purpose of deformations is to reveal some "pole of rigidity" of the factor, i.e. a subalgebra P that has a rigid position (in a sense or another) inside M. This roughly means that any deformation ϕ_n (often from a pre-assigned family of c.p. maps) must converge to id_P on the unit ball of P.

In order for the deformations to reveal the position of P relative to N, besides $P \subset M$ being rigid we need M to have "many" N-bilinear deformations, i.e. M to be in some sense deformable ("soft") relative to N. In the end, we want that "$\phi_n \approx \mathrm{id}_P$ on $(P)_1$" gives enough information so that, after some additional work, one gets from it a $P-N$ Hilbert bimodule $\mathcal{H} \subset L^2(M)$ with $\dim \mathcal{H}_N < \infty$. The "additional work" required may be minimal in some cases, like in examples 6.1, 6.6 and Section 7, or it may represent a substantial part of the argument, like in Example 6.2 and the results in Section 8–10. Moreover, the deformation/rigidity may require first an embedding of M into a larger II_1 factor $\tilde{M}$, then taking deformations of $\tilde{M}$ (e.g. by automorphisms, like in Sections 8–10). We illustrate this general strategy with a number of concrete situations where it has been be applied, postponing to the next sections the exact statement of the applications. The generic II_1 factor M involved in each situation is $M = L^\infty(X) \rtimes \Gamma = L^\infty(Y) \rtimes \Lambda$, as in (3.1), with the subalgebras $P, N \subset M$ being either $P = L^\infty(X)$, $N = L^\infty(Y)$, or $P = L\Gamma$, $N = L\Lambda$.

6.1. Haagerup deformation and relative property (T) ([P01b]). A II_1 factor M has *property* H (*Haagerup property*) *relative to* N if there exists a deformation of id_M with subunital subtracial N-bilinear c.p. maps $\{\phi_n\}_n$ which are *compact relative to* N, i.e. for all $\{x_k\}_k \subset M$ with $E_N(x_m^* x_m) \leq 1$ and $\lim_k \|E_N(x_k^* x_m)\|_2 = 0$ for all m, one has $\lim_m \|\phi_n(x_m)\|_2 = 0$ (cf. [Cho83] for the case $N = \mathbb{C}$, [Bo93] in general). For subalgebras of the form $N \subset M = N \rtimes \Lambda$, this is equivalent to Λ having the Haagerup approximation property ([H79]), i.e. there exist positive definite functions φ_n on Λ that tend pointwise to 1_Γ and vanish at ∞ ($\varphi_n \in c_0(\Lambda)$). The typical (non-amenable) example of groups with this property are the free groups $\mathbb{F}_n$ ([H79]), but

all discrete subgroups in $SU(n, 1)$, $SO(n, 1)$ have the property as well (see [CaH85]; also [CCJJV01] for a survey.)

An inclusion $P \subset M$ is *rigid* (or has the *relative property* (T)) if any deformation of id_M with subunital subtracial c.p. maps of M tends uniformly to id_P on the unit ball of $(P)_1$ ([P01b]). For subalgebras of the form $P = LH \subset LG = M$, where $H \subset G$ are discrete groups, the rigidity of $LH \subset LG$ is equivalent to the relative property (T) of the inclusion $H \subset G$, as considered in ([K67], [Ma82]). (N.B. This property requires that unitary representations of Γ which almost contain the trivial representation of Γ must contain the trivial representation of H.) A well known example is the inclusion of groups $\mathbb{Z}^2 \subset \mathbb{Z}^2 \rtimes \mathrm{SL}(2, \mathbb{Z})$ ([K67], [Ma82]), more generally $\mathbb{Z}^2 \subset \mathbb{Z}^2 \rtimes \Gamma$ for any $\Gamma \subset \mathrm{SL}(2, \mathbb{Z})$ non-amenable ([Bu91]).

With these concepts in hand, let us prove the result in ([P01b]), showing that if $P, N \subset M$ are so that $P \subset M$ is rigid and M has property H relative to N then $P \prec_M N$. Indeed, since M has N-bilinear subunital subtracial c.p. maps ϕ that are compact relative to N and close to id_M, such ϕ follow uniformly close to id_M on $(P)_1$. If $P \not\prec_M N$ then by 5.1 one can construct recursively $u_k \in \mathcal{U}(P)$ such that $\lim_k \|E_N(u_k^* u_m)\|_2 = 0$ for all m. Thus, $\lim_k \|\phi_n(u_k)\|_2 = 0$ for all n by compactness of ϕ_n, while for large (but fixed) k one has $\phi_k(u_n) \approx u_n$ uniformly in n, contradiction.

6.2. Malleability as source of intertwiners. Loosely speaking, a malleable deformation of a II_1 factor M over a subalgebra $N \subset M$ is an embedding of M in a larger II_1 factor $\tilde{M}$ and a continuous path α_t of automorphisms of $\tilde{M}$ such that N is fixed by α_t for all t, with $\alpha_0 = \mathrm{id}$ and $\alpha_1(M \ominus N) \perp (M \ominus N)$ as (pre)Hilbert spaces. More generally, one can merely require the automorphism α_1 satisfying the above conditions to be in the connected component of $\mathrm{id}_{\tilde{M}}$ in $\mathrm{Aut}_N(\tilde{M}) = \{\rho \in \mathrm{Aut}(\tilde{M}) \mid N \subset \tilde{M}^\rho\}$. The interest of such deformations is that if $P \subset M$ is a subalgebra for which there exists $b \in \tilde{M}$ non-zero with $Pb \subset b\alpha_1(P)$ (i.e. $P \prec_{\tilde{M}} \alpha_1(P)$) and the intertwiner b can be shown to belong to the M-bimodule $L^2(\mathrm{sp}M\alpha_1(M)$, then $P \prec_M N$, more precisely a reinterpretation of b as an element in the M-bimodule $L^2(\langle M, e_N\rangle, \mathrm{Tr})$ produces a (non-zero) finite dimensional $P - N$ bimodule, which by 5.1 means $P \prec_M N$.

Thus, such deformations can be used to obtain unitary conjugacy between subalgebras of M, provided one can show that the continuous path $\alpha_t(P)$ in $\tilde{M}$ produces an intertwiner between P and $\alpha_1(P)$. If the path is uniformly continuous on P then by the remarks at the end of Sections 4 and 5 one can find intertwiners between $\alpha_t(P)$ and $\alpha_{t+\mathrm{d}t}(P)$, for "incremental" $\mathrm{d}t$, then try to patch them. To have uniform continuity and do the patching certain assumptions must be made, as explained below.

6.3. Malleability and property (T) ([P01a], [P03], [P04a]). Malleability properties and their importance in studying group actions and algebras were discovered in (2.1 of [P01a]), inspired by some considerations in (4.3.2 of [P86]). The formal way the concept is defined in (2.1 in [P01a] and 1.4, 1.5 in [P03]) is as follows: An

action $\Lambda \curvearrowright (B, \tau)$ is *malleable* if there exist an embedding $B \subset \tilde{B}$ with an action $\Lambda \curvearrowright \tilde{B}$ extending $\Lambda \curvearrowright B$, and a continuous path α_t of automorphisms of $\tilde{B}$ commuting with the Λ-action, such that $\alpha_0 = \mathrm{id}_{\tilde{B}}$, $\alpha_1(B) \perp B$ (in the sense of [P83]) and $\tilde{B} = \overline{\mathrm{sp}} B\alpha_1(B)$. In case $B = L^\infty(Y)$ this amounts to $\tilde{B} \simeq L^\infty(Y) \mathbin{\overline{\otimes}} L^\infty(Y)$ with $\Lambda \curvearrowright L^\infty(Y) \otimes L^\infty(Y)$ the "double" action. Such deformations α_t implement automorphisms of $\tilde{M} \stackrel{\mathrm{def}}{=} \tilde{B} \rtimes \Lambda$, still denoted α_t, so this does fit into the general framework 6.2 for $M = B \rtimes \Lambda$, $N = L\Lambda$. Moreover, the condition $\mathrm{sp}B\alpha_1(B)$ dense in $\tilde{B}$ implies $\mathrm{sp}M\alpha_1(M)$ dense in $\tilde{M}$, insuring that any intertwiner of $P, \alpha_1(P)$ in $\tilde{M}$ produces an intertwiner of P, N in M.

Examples of actions satisfying the malleability condition are all generalized Bernoulli actions $\Lambda \curvearrowright \mathbb{T}^I$, corresponding to some action of Λ on a countable set I, and the non-commutative Bernoulli and Bogoliubov actions on the hyperfinite II_1 factor R ([P01a], [P03]). It was recently noticed in ([Fu06]) that Gaussian actions are malleable as well (see [CW81] or [CCJJV01] for the definition of such actions).

More "lax" conditions for malleable deformations, where $\mathrm{sp}B\alpha_1(B)$ is no longer required dense in $\tilde{B}$, were considered in (4.2 of [P03]) and (6.1 of [P01a]). In such cases, an element b intertwining P into $\alpha_1(P)$ can be shown to belong to $L^2(\mathrm{sp}M\alpha_1(M))$ whenever some appropriate *relative weak mixing* condition of $\Lambda \curvearrowright \tilde{B}$ wrt $\Lambda \curvearrowright L^2(\mathrm{sp}B\alpha_1(B))$ holds true (e.g. 4.2.1 in [P03], 2.9 in [P05], 6.1 in [P01a]). All generalized Bernoulli actions $\Lambda \curvearrowright (B_0, \tau_0)^I$, with B_0 an arbitrary finite, AFD (equivalently amenable, by [C76]) von Neumann algebra, have malleable deformations satisfying the relative weak mixing requirement. Same for the "free Bernoulli actions" $\Lambda \curvearrowright (B_0, \tau_0)^{*I} = *_{i \in I}(B_0, \tau_0)_i$ with AFD base (B_0, τ_0) (cf. 6.1 in [P01a]).

Typically, if $\Lambda \curvearrowright B$ is a malleable action as above, or more generally M is malleable over N, corresponding to $M = B \rtimes \Lambda$, $N = L\Lambda$, the rigidity condition required on the subalgebra $P \subset M$ is the relative property (T) as defined in 6.1. If $P = L\Gamma$, where $\Gamma \curvearrowright X$ is another action with $M = L^\infty(Y) \rtimes \Lambda = L^\infty(X) \rtimes \Gamma$ as in (3.1), one requires that Γ itself has property (T). By rigidity, $\alpha_t(P)$ and $\alpha_{t+\mathrm{d}t}(P)$ are then uniformly close, for "incremental" $\mathrm{d}t$, so there is a non-zero intertwiner between them (for groups, this is trivial by the observations in Section 4). Patching these intertwiners gives an intertwiner between P and $\alpha_1(P)$, which from the above shows that $P = L\Gamma$ can be intertwined into $N = L\Lambda$. But there are actually big difficulties in doing the "patching", as the intertwiners are apriori partial isometries and not unitaries, so when gluing them repeatedly we may end up getting 0. The malleable deformations with a symmetry, called *s-malleable*, were introduced in (2.1, 6.1 of [P01a], 1.4 of [P03]) to overcome this issue. All above examples carry natural such symmetry, and so do the "free"-deformations found in ([IPeP05). In turn, much less than property (T) for Γ is enough to obtain an intertwiner between $L\Gamma$ and $L\Lambda$ through this argument. Thus, if the Λ-action is mixing then it is sufficient that Γ has an infinite subgroup $H \subset \Gamma$ with the relative property (T) and some weak normality condition, for instance existence of a chain of normal inclusions from H to Γ (H is *w-normal* in Γ).

6.4. Malleability in free product algebras. A malleable deformation was also used in ([P01a]) to prove a cocycle rigidity result for actions of property (T) groups Γ on $B = L\mathbb{F}_\Gamma \simeq L\mathbb{F}_\infty$, by free Bernoulli shifts. Inspired by (4.3.2 of [P86]) it gives an explicit construction of an action α of $\mathbb{R}$ on $\tilde{B} = B * B$ which commutes with the double action of Γ on $\tilde{B}$ and checks $\alpha_1(B*\mathbb{C}) = \mathbb{C}*B$. The cocycle rigidity is proved by using the general scheme 6.2, with $M = B \rtimes \Gamma$, $\tilde{M} = \tilde{B} \rtimes \Gamma$, $N = L\Gamma$ and the natural extension to $\tilde{M}$ of the deformation α_t. But this malleable deformation no longer satisfies the "tight" generating condition $\mathrm{sp}B\alpha_1(B)$ dense in $\tilde{B}$, and "descending" the intertwiner between $B, \alpha_1(B)$ from $\tilde{B}$ to $L^2(B\alpha_1(B))$ requires more work.

Another malleable deformation in free product framework was discovered in ([IPeP05]), but for the acting group rather than for the action. Thus, let $\Gamma = \Gamma_1 * \Gamma_2 \curvearrowright (B, \tau)$ and denote $M = B \rtimes \Gamma$, $\tilde{M} = B \rtimes (\Gamma * \mathbb{F}_2)$, with $\mathbb{F}_2$ acting trivially on B. Then $\tilde{M}$ can also be viewed as the amalgamated free product $(B \rtimes \Gamma_1 * \mathbb{Z}) *_B (B \rtimes \Gamma_1 * \mathbb{Z})$. If $u_1 \in L(\mathbb{Z} * 1) \subset L(\mathbb{F}_2)$, $u_2 \in L(1 * \mathbb{Z}) \subset L(\mathbb{F}_2)$ are the canonical generating unitaries and $h_j = h_j^*$ are so that $\exp(ih_j) = u_j$, then h_j commute with B. Thus $\alpha_t = \mathrm{Ad}(\exp(ith_1)) *_B \mathrm{Ad}(\exp(ith_2))$ implements an action of $\mathbb{R}$ on $\tilde{M}$ leaving B fixed and satisfying $\alpha_1 = \mathrm{Ad}(u_1) * \mathrm{Ad}(u_2)$, $\alpha_1(L\Gamma) = u_1 L\Gamma_1 u_1^* * u_2 L\Gamma_2 u_2^* \perp L\Gamma$.

6.5. A general notion of rigidity for subalgebras. The above considerations justify considering the following:

Definition 6.5.1 ([P04b]). Let M be a II_1 factor, $P \subset M$ a von Neumann subalgebra and $\mathcal{L}$ a family of subunital subtracial c.p. maps of M. We say that the inclusion $Q \subset M$ is *rigid with respect to* (wrt) $\mathcal{L}$ if given any deformation of id_M by c.p. maps $\phi_n \in \mathcal{L}$ we have $\|\phi_n(x) - x\|_2 \to 0$ uniformly for $x \in (P)_1$.

Note that the rigidity of $P \subset M$ as defined in 6.1 amounts to condition 6.5.1 for $\mathcal{L}$ the family of all subunital subtracial c.p. maps on M, the particular case $P = M$ of which amounts to the Conne–Jones definition of property (T) for the II_1 factor M ([CJ85]). Also, the malleability/rigidity arguments above only used the rigidity of the inclusion $P \subset \tilde{M}$ wrt $\mathcal{L} = \{\alpha_t\}_t \subset \mathrm{Aut}(\tilde{M})$, where α is the malleable deformation.

Besides its rôle in deformation/rigidity approach to proving statements such as (3.1), the idea of defining various notions of rigidity for inclusions of algebras $P \subset M$ has other applications as well. Thus, if the family $\mathcal{L}$ has an abstract description, depending only on the isomorphism class of $P \subset M$, then the rigidity of $P \subset M$ wrt $\mathcal{L}$ is, of course, an isomorphism invariant for $P \subset M$. This point of view gives rise to useful applications to OE ergodic theory. For instance, a new OE invariant for a free ergodic m.p. action $\Gamma \curvearrowright X$ (more generally for equivalence relations $\mathcal{R}_\Gamma$) was defined in ([P01b]) by requiring that the inclusion $L^\infty(X) \subset L^\infty(X) \rtimes \Gamma$ (resp $L^\infty(X) \subset L(\mathcal{R}_\Gamma)$) is rigid (see also [PeP04]). From 6.1 it follows that if $\Gamma \subset \mathrm{SL}(2, \mathbb{Z})$ is non-amenable then $\Gamma \curvearrowright \mathbb{T}^2 = \hat{\mathbb{Z}}^2$ has this property. More examples were constructed in ([Va05]). This notion of relative property (T) for free ergodic actions played an important rôle in the proof that free groups have uncountably many OE-inequivalent

actions in ([GP03]). Another particular case of 6.5.1 recovers a concept considered in ([An87], [P86]): A II_1 factor M has the *property* (T) *relative to* a subalgebra $P \subset M$ (or P is *co-rigid* in M) if $M \subset M$ is rigid wrt the family of all subunital subtracial P-bilinear c.p. maps on M. Again, by the definition, this notion is an isomorphism invariant for the inclusion $P \subset M$, so in case $P = L^\infty(Y) \subset L^\infty(Y) \rtimes \Lambda = M$, it gives an OE invariant for the free action $\Lambda \curvearrowright Y$. For such inclusions, it is shown in ([P86]) that co-rigidity is equivalent to the property (T) of Λ.

6.6. Example ([P04c]). We end this discussion with a simple but very suggestive example related to definition 6.5.1: Let M be a II_1 factor of the form $M = Q \mathbin{\overline{\otimes}} R$, where R is the hyperfinite II_1 factor and Q is a non(Γ) II_1 factor ([MvN43]). Let $\mathcal{L}$ be the family of all conditional expectations onto non(Γ) II_1 subfactors $P \subset M$ with the property that $P' \cap M \simeq R$ and $M = P \vee (P' \cap M)$. It is easy to see that $Q \subset M$ is rigid wrt $\mathcal{L}$. Recovering the building data means in this case to show that if $M = P_0 \mathbin{\overline{\otimes}} R_0$ is another decomposition with P_0 non(Γ) and $R_0 \simeq R$ then there exists a unitary element $u \in M$ such that $uP_0u^* = Q^t$, $uR_0u^* = R^{1/t}$, for some $t > 0$, where the identification $Q \mathbin{\overline{\otimes}} R = Q^t \mathbin{\overline{\otimes}} R^{1/t}$ is self-explanatory. To prove this, one takes $P_n = P_0 \otimes \mathrm{M}_{2^n \times 2^n}(\mathbb{C})$ where $\mathrm{M}_{2^n \times 2^n}(\mathbb{C}) \nearrow R_0$ and apply the rigidity of $Q \subset M$ with respect to the deformation E_{P_n} to conclude that for a large enough n, the unit ball of Q is almost contained in P_n. By the intertwining criteria 5.1, there exists $u \in \mathcal{U}(M)$ that conjugates Q into P_n, which from the split-off conditions implies the result.

Similarly, one can show that if M is a II_1 factor with $Q \subset M$ a von Neumann algebra such that $\{\mathrm{Ad}(u) \mid u \in \mathcal{U}(Q)\}$ *has spectral gap* wrt $Q' \cap M$ (i.e. there exist $u_1, \ldots, u_n \in \mathcal{U}(Q)$ and $c > 0$ such that $\Sigma_i \|u_i x u_i^* - x\|_2 \geq c\|x\|_2$ for all $x \in Q' \cap M^\perp$), then $Q' \cap M \subset M$ is rigid wrt $\mathcal{L} = \mathrm{Aut}(M)$ ([P06]).

7. vNE/OE rigidity from relative property (T) and H

We formally state here the result discussed in 6.1, which uses Haagerup-type deformation of the acting group and relative property (T) of the action. This is a typical vNE/OE rigidity result, in the terminology established in (3.1), as it shows that for a certain class of group measure space II_1 factors, any algebra isomorphism comes from an orbit equivalence of the actions, modulo perturbation by an inner automorphism.

Theorem 7.1 ([P01b]). *Let $\Gamma \curvearrowright (X, \mu)$, $\Lambda \curvearrowright (Y, \nu)$ be ergodic (not necessarily free) m.p. actions and assume $L^\infty(X) \subset L(\mathcal{R}_\Gamma)$ is rigid while $L(\mathcal{R}_\Lambda)$ has property* H *relative to $L^\infty(Y)$. If $\theta\colon L(\mathcal{R}_\Gamma) \simeq L(\mathcal{R}_\Lambda)$ is an algebra isomorphism then there exists $u \in \mathcal{U}(L(\mathcal{R}_\Lambda))$ such that* $\mathrm{Ad}(u)(\theta(L^\infty(X))) = L^\infty(Y)$.

The next corollary lists some concrete examples when the assumptions of 7.1 are satisfied.

Corollary 7.2. *Let* $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ *be a non-amenable subgroup and* $\Gamma \curvearrowright \mathbb{T}^2 = \hat{\mathbb{Z}}^2$ *the action induced by the restriction to* Γ *of the* $\mathrm{SL}(2,\mathbb{Z})$ *action on* $\mathbb{Z}^2$. *Let* $\Lambda \curvearrowright (Y,\nu)$ *be a free ergodic m.p. action of a group* Λ *having Haagerup's compact approximation property, e.g.* $\Lambda \subset \mathrm{SL}(2,\mathbb{Z})$. *If* $\theta\colon L^\infty(X)\rtimes\Gamma \simeq (L^\infty(Y)\rtimes\Lambda)^t$, *then there exists a unitary element* u *in the target algebra such that* $\mathrm{Ad}(u)\circ\theta$ *takes* $L^\infty(X)$ *onto* $L^\infty(Y)^t$.

It is easy to check that both the rigidity of a Cartan inclusion $A \subset M$ and the property H of M relative to A are stable to amplifications. Thus, the class HT of factors with Cartan subalgebras satisfying both conditions is stable to amplifications. By 7.1, given an HT factor M there exists a unique equivalence relation $\mathcal{R}_M^{HT}$ associated to its unique (up to conjugacy) HT Cartan subalgebra. Thus, for the factors in this class, all OE invariants for $\mathcal{R}_M^{HT}$ are isomorphism invariants for the factor M and $\mathcal{F}(\mathcal{R}_M^{HT}) = \mathcal{F}(M)$. In particular, since Gaboriau showed in ([G00], [G01]) that the equivalence relation of any free ergodic action $\mathbb{F}_n \curvearrowright X$, $2 \le n < \infty$, has trivial fundamental group and that for different n's the $\mathbb{F}_n$-actions are OE-inequivalent, we derive:

Corollary 7.3. 1°. *If* $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ *is finitely generated nonamenable group then the factor* $M = L(\mathbb{Z}^2 \rtimes \Gamma) = L^\infty(\mathbb{T}^2)\rtimes\Gamma$ *has trivial fundamental group,* $\mathcal{F}(M) = \{1\}$.

2°. *If* $\mathbb{F}_n \subset \mathrm{SL}(2,\mathbb{Z})$ *is some embedding of the free group with n generators, then the* II_1 *factors* $L(\mathbb{Z}^2 \rtimes \mathbb{F}_n) = L^\infty(\mathbb{T}^2)\rtimes\mathbb{F}_n$ *are mutually non-isomorphic,* $2 \le n \le \infty$.

Corollary 7.3 gave the first examples of II_1 factors with trivial fundamental group ([P01b]). In particular, this solved a longstanding problem of Kadison (Problem 3 in [Ka67]), asking whether there exist II_1 factors M with the property that $\mathrm{M}_{n\times n}(M) \not\simeq M$ for all $n \ge 2$. By 7.3, the group factor LG, arising from the arithmetic group $G = \mathbb{Z}^2 \rtimes \mathrm{SL}(2,\mathbb{Z})$, does satisfy this property, in fact $\mathcal{F}(LG) = \{1\}$. The corollary also gives the first examples of non-isomorphic group measure space factors associated with actions $\mathbb{F}_n \curvearrowright X$ of free groups $\mathbb{F}_n$ with different number of generators, $n = 2, 3, \ldots$. It is an open problem whether $L\mathbb{F}_n \not\simeq L\mathbb{F}_m$ for $n \ne m$, despite remarkable progress in the study of free group factors through Voiculescu's free probability theory ([Vo90], [Vo94]). Using these techniques, it was shown in ([R94], [Dy93]) that "$L\mathbb{F}_n$, $2 \le n \le \infty$, are all non-isomorphic" $\Leftrightarrow$ "two of them are non-isomorphic" $\Leftrightarrow$ "$\mathcal{F}(L\mathbb{F}_n) \ne \mathbb{R}_+^*$ for some $2 \le n < \infty$" $\Leftrightarrow$ "$\mathcal{F}(L\mathbb{F}_n) = \{1\}$ for all $2 \le n < \infty$". The same techniques have led to the proof that $\mathbb{Q} \subset \mathcal{F}(L\mathbb{F}_\infty)$ in ([Vo90]) and finally $\mathcal{F}(L\mathbb{F}_\infty) = \mathbb{R}_+^*$ in ([R94]).

8. vNE strong rigidity from property (T) and malleability

We now state rigidity results obtained by using malleability of actions as "deformability property" and the property (T) of the acting group as the "rigidity property", discussed in 6.3. These statements are exactly of the type (3.1). They are the first vNE Strong Rigidity results pertaining to von Neumann algebras.

The source groups Γ considered below are required to be ICC and to have infinite w-normal subgroups $H \subset \Gamma$ with the relative property (T). Examples are all the ICC property (T) groups and the groups $\mathbb{Z}^2 \rtimes \Gamma_0$, with $\Gamma_0 \subset \mathrm{SL}(2,\mathbb{Z})$ non-amenable (cf. [K67], [Ma82], [Bu91]; see [Va05] for more examples). If Γ satisfies the property (e.g. Γ ICC with property (T)), then $\Gamma \times H'$ satisfies the property as well for all H' ICC.

Theorem 8.1 ([P03], [P04a]). *Assume Γ is ICC and has an infinite normal subgroup with the relative property* (T). *Let $\Gamma \curvearrowright (X,\mu)$ be an arbitrary free ergodic m.p. action. Let Λ be an arbitrary ICC group and $\Lambda \curvearrowright (Y,\nu)$ a Bernoulli action, or more generally a free, relative weak mixing quotient of a Bernoulli Λ-action.*

If $\theta : L^\infty(X) \rtimes \Gamma \simeq (L^\infty(Y) \rtimes \Lambda)^t$ is an isomorphism of II_1 factors, for some $0 < t \leq 1$, then $t = 1$ and θ is of the form $\theta = \mathrm{Ad}(u) \circ \theta^\gamma \circ \theta^{\Delta,\delta}$, where: u is a unitary element in $L^\infty(Y) \rtimes \Lambda$; $\theta^\gamma \in \mathrm{Aut}(L^\infty(Y) \rtimes \Lambda)$ is implemented by some $\gamma \in \mathrm{Hom}(\Lambda, \mathbb{T})$; $\theta^{\Delta,\delta} : L^\infty(X) \rtimes \Gamma \simeq L^\infty(Y) \rtimes \Lambda$ is implemented by isomorphisms $\Delta : (X,\mu) \simeq (Y,\nu)$, $\delta : \Gamma \simeq \Lambda$ which give a conjugacy of $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$.

More generally, the above statement holds true for target actions $\Lambda \curvearrowright Y$ that are *relative weak mixing quotients* of actions that are s-malleable and *clustering*. An action $\Lambda \curvearrowright (Y,\nu)$ is a quotient of an action $\Lambda \curvearrowright (Y',\nu')$ if there exists a Λ-invariant m.p. surjection $(Y',\nu') \to (Y,\nu)$, equivalently a Λ-invariant m.p. embedding $L^\infty(Y) \subset L^\infty(Y')$. The quotient is relative weak mixing if there exists $g_n \to \infty$ in Λ such that $\lim_n \|E_{L^\infty(Y)}(xg_n(y))\|_2 = 0$ for all $x, y \in L^\infty(Y')$, with $y \perp L^\infty(Y)$ (cf. Furstenberg and Zimmer). The clustering condition is a certain multi-mixing condition which is satisfied, like s-malleability, by all Bernoulli actions.

The proof of this result is in three parts: The malleability of $\Lambda \curvearrowright Y$ combined with the rigidity assumption on Γ allows a deformation/rigidity argument in $\tilde{M} = L^\infty(Y \times Y) \rtimes \Lambda$. Taking $t = 1$, $M = L^\infty(Y) \rtimes \Lambda = L^\infty(X) \rtimes \Gamma$ for simplicity, this gives rise to a non-zero $L\Gamma - L\Lambda$ Hilbert bimodule $\mathcal{H} \subset L^2(M)$ which is finite dimensional as a right $L\Lambda$-module. Using intertwining technique, from $\mathcal{H}$ one gets a unitary element $u \in M$ that conjugates $L\Gamma$ into $L\Lambda$. The second part of the proof uses this information to derive that $L^\infty(X)$ can be unitarily conjugated onto $L^\infty(Y)$, by using ultrapower algebra techniques, "asymptotic analysis" of Fourier expansions and 5.1 (repeatedly). The final part of the proof consists in showing that if both the Cartan subalgebras and the group algebras can be (separately) conjugated by unitaries, then there exists a unitary that conjugates $L^\infty(X)$ onto $L^\infty(Y)$ and carries the canonical unitaries of the source factor onto scalar multiples of the canonical unitaries of the target factor.

It has been recently shown in ([P06]) that in fact 8.1 holds true for any group of the form $\Gamma = HH'$ with H non-amenable and H' infinite (e.g. Γ non-amenable with infinite center, or $\Gamma = H \times H'$), and even for groups Γ that have a non-amenable subgroup H whose centralizer is infinite and w-normal in Γ.

Taking the source and target group actions to satisfy both sets of conditions, and taking into account that a factor arising from the Bernoulli Γ-action with diffuse base

is the same as the group factor of the wreath product $\mathbb{Z} \wr \Gamma$, from 8.1 we derive a positive answer to a wreath product version of Connes' rigidity conjecture (3.2):

Corollary 8.2. *Let Γ_i be an ICC group having an infinite normal subgroup with the relative property* (T) *and denote $G_i = \mathbb{Z} \wr \Gamma_i$ the corresponding wreath product, $i = 0, 1$. Then $LG_0 \simeq LG_1^t$ implies $t = 1$, $G_0 \simeq G_1$ and $\Gamma_0 \simeq \Gamma_1$. In particular, all such factors have trivial fundamental group.*

We mention that (6.4 and 7.13 in [PV06]) provides a class $\mathcal{W}$ of "generalized" wreath product groups for which a (3.2′)-type statement (i.e. a version of the strong Connes rigidity conjecture) holds true, i.e. any isomorphism $\theta\colon LG_1 \simeq LG_2^t$, $G_1, G_2 \in \mathcal{W}$, entails $t = 1$ and $\theta = \mathrm{Ad}(u) \circ \theta^\gamma \circ \theta^\delta$, for some $\gamma \in \mathrm{Hom}(G_2, \mathbb{T})$ and $\delta\colon G_1 \simeq G_2$. In particular, if $G \in \mathcal{W}$ then $\mathrm{Out}(LG) = \mathrm{Hom}(G, \mathbb{T}) \rtimes \mathrm{Out}(G)$.

Arguments similar to the ones used in the first part of the proof of 8.1 allow showing that for any countable subgroup $S \subset \mathbb{R}_+^*$ there exist II_1 factors and equivalence relations from ergodic m.p. actions of countable groups which have S as fundamental group.

Theorem 8.3 ([P03]). *Let $S \subset \mathbb{R}_+^*$ be a countable subgroup and $\{s_n\}_n \subset S$ a set of generators. Let Γ be an ICC group having an infinite w-normal subgroup with the relative property* (T). *For each n, let μ_n be the probability measure on $\{0, 1\}$ satisfying $\mu_n(\{0\})/\mu_n(\{1\}) = s_n$ and let $\mathcal{S}_n$ be the equivalence relation on $(\{0, 1\}, \mu_n)^\Gamma$ given by $(t_g)_g \sim (t'_g)_g$ iff there exists a finite subset $F \subset \Gamma$ such that $t_g = t'_g$ for all $g \in \Gamma \setminus F$ and $\Pi_{g\in F}\mu_0(t_g) = \Pi_{g\in F}\mu_0(t'_g)$. Let $\mathcal{R}_0$ be the product of the equivalence relations $\mathcal{S}_n$ on the product probability space $(X, \mu) = \Pi_n(\{0, 1\}, \mu_n)^\Gamma$ and $\mathcal{R}$ be the equivalence relation generated by $\mathcal{R}_0$ and the Bernoulli Γ-action $\Gamma \curvearrowright X$ (which leaves $\mathcal{R}_0$ invariant). If $\mathcal{F}(L\Gamma) = \{1\}$, for instance if $\Gamma = H \rtimes \Gamma_0$ with $\Gamma_0 \subset \mathrm{SL}(2, \mathbb{Z})$ finite index subgroup (cf.* 7.3), *then $\mathcal{F}(L(\mathcal{R})) = \mathcal{F}(\mathcal{R}) = S$.*

A construction similar to 8.3 can be used to prove that in fact any subgroup $S \subset \mathbb{R}_+^*$ can be realized as the fundamental group of a non-separable II_1 factor ([P03]), solving completely a problem raised by Murray–von Neumann in ([MvN43]). This construction of concrete equivalence relations $\mathcal{R}$ with arbitrary countable fundamental group, obtained through II_1 factor methods, is completely new for OE theory as well.

When applied to isomorphisms θ coming from an OE $\mathcal{R}_\Gamma \simeq (\mathcal{R}_\Lambda)^t$, 8.1 becomes an OE strong rigidity result. In fact, one can even derive an OE Strong Rigidity for *embeddings* of equivalence relations:

Theorem 8.4 ([P04a]). *Let $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$ be as in* 8.1. *If $\Delta\colon (X, \mu) \simeq (Y, \nu)$ takes each Γ-orbit into a Λ-orbit then there exist a subgroup $\Lambda_0 \subset \Lambda$ and $\alpha \in [\Lambda]$ such that $\alpha \circ \Delta$ conjugates $\Gamma \curvearrowright X$, $\Lambda_0 \curvearrowright Y$.*

9. Cocycle superrigidity from property (T) and malleability

If in Theorem 8.4 we take Γ to have property (T) and Δ to give an orbit equivalence of $\Gamma \curvearrowright X$, $\Lambda \curvearrowright Y$, and use that property (T) is an OE invariant, then the statement becomes an OE Strong Rigidity where all conditions are on one side, a type of result labelled "OE superrigidity" in Section 3. In fact, if we assume all conditions are say on the side of the source group action $\Gamma \curvearrowright X$, then the deformation/rigidity arguments in the proof of 8.1 get simplified considerably, allowing us to prove a *cocycle superrigidity* result from which the OE superrigidity is a mere consequence.

To state the result, recall that if $\mathcal{V}$ is a Polish group then a $\mathcal{V}$-valued *measurable* (left) *cocycle* for $\Gamma \curvearrowright X$ is a measurable map $w\colon \Gamma \times X \to \mathcal{V}$ satisfying $w(g_1, g_2t)w(g_2, t) = w(g_1g_2, t)$ for all $g_1, g_2 \in \Gamma, t \in X$. Cocycles w, w' are *equivalent* if there is a measurable $u\colon X \to \mathcal{V}$ such that $w'(g, t) = u(gt)w(g, t)u(t)^{-1}$ for all g, t (a.e.). Note that w is independent of $t \in X$ iff it is a group morphism $\Gamma \to \mathcal{V}$.

A Polish group $\mathcal{V}$ is *of finite type* if it is isomorphic to a closed subgroup of the group of unitary elements $\mathcal{U}(N)$ of a finite von Neumann algebra N (equivalently of a II_1 factor). We denote by $\mathcal{U}_{\mathrm{fin}}$ the class of Polish groups of finite type. All countable discrete groups and all separable compact groups are of finite type. But by ([KaSi82]) a connected locally compact group $\mathcal{V}$ is of finite type iff $\mathcal{V} = K \times V$ with K compact and $V \simeq \mathbb{R}^n$.

Theorem 9.1 (P05]). *Assume Γ has an infinite w-normal subgroup H with the relative property* (T) *and that $\Gamma \curvearrowright (X, \mu) = (X_0, \mu_0)^I$ is a generalized Bernoulli action with $|Hi| = \infty$ for all $i \in I$.*

Then $\Gamma \curvearrowright X$ is $\mathcal{U}_{\mathrm{fin}}$-cocycle superrigid, i.e. for all $\mathcal{V} \in \mathcal{U}_{\mathrm{fin}}$, any $\mathcal{V}$-valued cocycle for $\Gamma \curvearrowright X$ is equivalent to a group morphism $\Gamma \to \mathcal{V}$. Moreover, same is true if $\Gamma \curvearrowright X$ is a relative weak mixing quotient of an action satisfying these conditions.

The above statement actually holds true for all malleable actions which are weak mixing on the subgroup H, and for all relative weak mixing quotients of such actions. The proof uses a version of the general deformation/rigidity argument explained in 6.2, in the group measure space von Neumann algebra $M = L^\infty(X) \mathbin{\overline{\otimes}} V \rtimes \Gamma$, where V is a II_1 factor with $\mathcal{V} = \overline{\mathcal{V}} \subset \mathcal{U}(V)$ and $\Gamma \curvearrowright L^\infty(X) \mathbin{\overline{\otimes}} V$ is the product of the action $\Gamma \curvearrowright L^\infty(X)$ and the trivial action of Γ on V. Also, the larger algebra $\tilde{M}$ in which we perform the deformation is $(L^\infty(X) \mathbin{\overline{\otimes}} V \mathbin{\overline{\otimes}} L^\infty(X)) \rtimes \Gamma$. We use the observation that a measurable function $w\colon \Gamma \times X \to \mathcal{U}(V)$ is a cocycle for $\Gamma \curvearrowright X$ iff the $g \mapsto u'_g = w_g u_g$ is a representation of the group Γ in M, where u_g denote the canonical unitaries in M, and $w_g = w(g, \cdot)$. With the notations in 6.2, the algebra N corresponds to $L\Gamma \mathbin{\overline{\otimes}} V$ while P corresponds to the von Neumann algebra generated by u'_g, $g \in \Gamma$. Due to the more concrete form of this set-up, the deformation/rigidity argument in $\tilde{M}$ gives in fact an intertwiner of the Γ-representations u'_g and $\alpha_1(u'_g)$, which lies in $L^\infty(X) \mathbin{\overline{\otimes}} V \mathbin{\overline{\otimes}} L^\infty(X)$. After the usual "re-interpretation" of this intertwiner, we get $u \in \mathcal{U}(L^\infty(X) \otimes V)$ such that $uu'_hu^* \in 1 \otimes V \rtimes \Gamma$. This means

$uw_h h(u)^* \in V$, so we have untwisted w as a $\mathcal{U}(V)$-valued cocycle for $H \curvearrowright X$. But then it follows automatically untwisted as a $\mathcal{V}$-valued cocycle, due to the weak mixing property. Applying the w-normality of $H \subset \Gamma$ and the weak mixing property again, it follows untwisted on all Γ.

The II_1 factor framework is used again to show that if a group action $\Gamma \curvearrowright X$ is cocycle superrigid then it is OE superrigid, i.e. any OE $\Delta\colon X \simeq Y$ of this action with an arbitrary free action $\Lambda \curvearrowright Y$ comes from a conjugacy. More precisely, let $w = w_\Delta\colon \Gamma \times X \to \Lambda$ be the *Zimmer cocycle* associated to Δ, which to $t \in X$, $g \in \Gamma$ assigns the unique (by freeness) $h \in \Lambda$ such that $\Delta(gt) = h\Delta(t)$ ([Z80], [Z84]). Since w takes values in Λ, which is discrete and thus in the class $\mathcal{U}_{\mathrm{fin}}$, by 9.1 it can be untwisted. The II_1 factor setting allows to re-interpret the "untwister" of this cocycle as a natural "conjugator" of the two actions, thus showing that cocycle superrigidity with arbitrary discrete targets implies OE superrigidity:

Theorem 9.2 ([P05]). *Let $\Gamma \curvearrowright X$ be a free, weakly mixing, cocycle superrigid action, e.g. an action as in* 9.1. *Assume Γ has no finite normal subgroups. Let $\Lambda \curvearrowright (Y, \nu)$ be an arbitrary free ergodic m.p. action and $\Delta\colon \mathcal{R}_\Gamma \simeq \mathcal{R}_\Lambda^t$ an orbit equivalence, for some $t > 0$.*

Then $n = 1/t$ is an integer and there exist a subgroup $\Lambda_0 \subset \Lambda$ of index $[\Lambda : \Lambda_0] = n$, a subset $Y_0 \subset Y$ of measure $\nu(Y_0) = 1/n$ fixed by $\Lambda_0 \curvearrowright Y$, an automorphism $\alpha \in [\Lambda]$ and a group isomorphism $\delta\colon \Gamma \simeq \Lambda_0$ such that $\alpha \circ \Delta$ takes X onto Y_0 and conjugates the actions $\Gamma \curvearrowright X$, $\Lambda_0 \curvearrowright Y_0$.

In fact, 9.1 even implies the superrigidity of embeddings of $\mathcal{R}_\Gamma$ into equivalence relations $\mathcal{R}_\Lambda$ of arbitrary free ergodic actions (in the spirit of 8.4), as well as for morphisms of $\mathcal{R}_\Gamma$ onto $\mathcal{R}_\Lambda$ that are bijective on each orbit, i.e. for *local OE* morphisms (see [P05] for details). Theorem 9.1 also shows that the $\mathbb{T}$-valued first cohomology group $\mathrm{H}^1(\mathcal{R}_\Gamma)$ of a Bernoulli Γ-action is equal to $\mathrm{Hom}(\Gamma, \mathbb{T})$, thus recovering a result from ([P01a], [PSa03]). This implies that given any abelian group L one can construct free quotients of Bernoulli Γ-actions with first cohomology group $\mathrm{H}^1(\mathcal{R}_\Gamma) = \mathrm{Hom}(\Gamma, \mathbb{T}) \times L$ (cf. [P04b]). Thus, any group Γ with an infinite w-normal subgroup with the relative property (T) has uncountably many "concrete" non-OE free ergodic m.p. actions. Another application of 9.1 shows that the equivalence relations $\mathcal{R}$ described in the statement of 8.3 have the property that for all $t > 0$, $\mathcal{R}^t$ cannot be implemented by a free ergodic action of a group (5.10 in [P05]). The first examples of equivalence relations with this property were found in ([Fu99b]).

The Cocycle Superrigidity 9.1 was recently used in ([Fu06]) to show that if Γ, Λ are lattices in a higher rank semisimple Lie group $\mathcal{G}$ then the action $\Gamma \curvearrowright \mathcal{G}/\Lambda$ cannot be realized as a quotient of a Bernoulli Γ-action, more generally of a s-malleable weak mixing action. Also, 9.1 was used in ([Th06]) to answer some open problems in descriptive set theory, showing for instance that the universal countable Borel equivalence relation E_∞ cannot be implemented by a free action of a countable group. Moreover, a new $\mathcal{U}_{\mathrm{fin}}$-cocycle superrigidity result was obtained in ([P06]), by combining malleability with spectral gap rigidity (see final comment in 6.6 above).

It shows that if $\Gamma \curvearrowright X$ is a generalized Bernoulli action and $H \subset \Gamma$ is a subgroup such that $H \curvearrowright X$ has spectral gap (thus H is automatically non-amenable) then any $\mathcal{V}$-valued cocycle for $\Gamma \curvearrowright X$, where $\mathcal{V} \in \mathcal{U}_{\text{fin}}$, can be untwisted on the centralizer H' of H in Γ. Thus, if H' is w-normal in Γ (e.g. $\Gamma = H \times H'$) and $H' \curvearrowright X$ is weak mixing then the cocycle follows untwisted on all Γ. In particular, such $\Gamma \curvearrowright X$ are OE superrigid. This adds to the rigidity phenomena involving product groups discovered in recent years in ergodic theory, Borel equivalence relations and II_1 factors (e.g. [MoS02], [MoS04], [OzP04], [HjKe05]).

10. Bass–Serre type rigidity for amalgamated free products

The malleable deformation explained in the second part of 6.4 is used in ([IPeP05]) to prove a series of rigidity results, through the deformation/rigidity approach. These results can be viewed as von Neumann algebra versions of the "subgroup theorems" and "isomorphism theorems" for amalgamated free products of groups in Bass–Serre theory. The main "subalgebra theorem" shows that, under rather general conditions, any rigid von Neumann subalgebra $Q \subset M = M_1 *_B M_2$ can be conjugated by an inner automorphism of M into either M_1 or M_2. For simplicity, we only formulate the result in the case $M = (B \rtimes \Gamma_1) *_B (B \rtimes \Gamma_2) = B \rtimes (\Gamma_1 * \Gamma_2)$.

Theorem 10.1 ([IPeP05]). *Let $\Gamma \curvearrowright (B, \tau)$ be an action of a group $\Gamma = \Gamma_1 * \Gamma_2$ on a finite von Neumann algebra (B, τ) and denote $M_i = B \rtimes \Gamma_i$, $i = 1, 2$, $M = B \rtimes \Gamma = M_1 *_B M_2$. Let $Q \subset M$ be a rigid inclusion. Assume no corner qQq of Q can be embedded into B and that the normalizer of Q in M generates a factor P. Then there exists a unique $i \in \{1, 2\}$ such that $uQu^* \subset M_i$ for some $u \in \mathcal{U}(M)$, which also satisfies $uPu^* \subset M_i$.*

Taking the action $\Gamma \curvearrowright B$ in 10.1 to come from an action on a probability space, the theorem can be used to prove Bass–Serre type vNE and OE rigidity results for actions of free products of groups, as follows:

Theorem 10.2 ([IPeP05]). *Let Γ_i, Λ_j, $1 \leq i \leq n \leq \infty$, $1 \leq j \leq m \leq \infty$, be ICC groups having normal, non virtually abelian subgroups with the relative property* (T). *Denote $\Gamma = \Gamma_1 * \cdots$, $\Lambda = \Lambda_1 * \cdots$ and let $\Gamma \curvearrowright (X, \mu)$, $\Lambda \curvearrowright (Y, \nu)$ be free m.p. actions, ergodic on each Γ_i, Λ_j, $i, j \geq 1$. Denote $M = L^\infty(X) \rtimes \Gamma$, $N = L^\infty(Y) \rtimes \Lambda$, $M_i = L^\infty(X) \rtimes \Gamma_i \subset M$, $N_j = L^\infty(Y) \rtimes \Lambda_j \subset N$ the corresponding group measure space factors. If $\theta : M \simeq N^t$ is an isomorphism, for some $t > 0$, then $m = n$ and there exists a permutation π of indices $j \geq 1$ and unitaries $u_j \in M_2^t$ such that $\text{Ad}(u_j)(\theta(M_j)) = N_{\pi(j)}^t$, $\text{Ad}(u_j)(\theta(L^\infty(X))) = (L^\infty(Y))^t$ for all $j \geq 1$. In particular, $\mathcal{R}_\Gamma \simeq \mathcal{R}_\Lambda^t$ and $\mathcal{R}_{\Gamma_j} \simeq \mathcal{R}_{\Lambda_{\pi(j)}}^t$ for all $j \geq 1$.*

In particular, taking the isomorphism θ between the group measure space factors in 10.2 to come from an orbit equivalence of the actions, one gets the following converse to a result in ([G05]):

Corollary 10.3. *Let* Γ_i, Λ_j, $1 \leq i \leq n \leq \infty$, $1 \leq j \leq m \leq \infty$, $\Gamma \curvearrowright (X, \mu)$, $\Lambda \curvearrowright (Y, \nu)$ *be as in* 10.2. *If* $\mathcal{R}_\Gamma \simeq \mathcal{R}_\Lambda^t$ *then* $n = m$ *and there exists a permutation* π *of the set of indices* $i \geq 1$ *such that* $\mathcal{R}_{\Gamma_i} \simeq \mathcal{R}^t_{\Lambda_{\pi(i)}}$ *for all* $i \geq 1$.

In turn, applying 10.1 to Γ-actions on the hyperfinite II_1 factor $B = R$ and using results from ([P90]) one can prove:

Theorem 10.4 ([IPeP05]). 1°. *For any* $\Gamma_0 = \mathrm{SL}(n_0, \mathbb{Z})$, $n_0 \geq 2$ *and any group* Γ_1 *having an infinite normal subgroup with the relative property* (T) *there exist properly outer actions* $\Gamma_0 * \Gamma_1 \curvearrowright R$ *such that:*

(a) $R \subset R \rtimes \Gamma_0$ *is a rigid inclusion;*

(b) $\Gamma_1 \curvearrowright R$ *is a non-commutative Bernoulli action, i.e.* R *can be represented as* $R = \overline{\otimes}_{g \in \Gamma_1} (\mathrm{M}_{n \times n}(\mathbb{C}), \mathrm{tr})_g$, $n \geq 2$, *with* Γ_1 *acting on it by Bernoulli shifts;*

(c) $\Gamma_1 \subset \mathrm{Out}(R)$ *is freely independent with respect to the normalizer* $\mathcal{N}_0$ *of* Γ_0 *in* $\mathrm{Out}(R)$.

2°. *If* $\Gamma_0 * \Gamma_1 \curvearrowright R$ *is an action as in* 1° *and* $M = R \rtimes (\Gamma_0 * \Gamma_1)$, *then* $\mathcal{F}(M) = \{1\}$ *and* $\mathrm{Out}(M) = \mathrm{Hom}(\Gamma_0, \mathbb{T}) \times \mathrm{Hom}(\Gamma_1, \mathbb{T})$. *In particular, given any separable compact abelian group* K, *there exist free actions of* $\Gamma = \mathrm{SL}(3, \mathbb{Z}) * (\mathrm{SL}(3, \mathbb{Z}) \times \hat{K})$ *on* R *such that* $M = R \rtimes \Gamma$ *satisfies* $\mathcal{F}(M) = \{1\}$ *and* $\mathrm{Out}(M) = K$.

Part 2° of the above theorem gives the first examples of II_1 factors with calculable outer automorphism group, in particular of factors with trivial outer automorphism group, thus answering in the affirmative a well known problem posed by Connes in 1973. However, since the proof of part 1° uses a Baire category argument, 10.4.2° is actually an existence result. By using a refinement of techniques in ([P03], [P04a]) and results from ([Oz04]), some concrete examples of group measure space factors with trivial outer automorphism group were recently constructed in ([PV06]) from generalized Bernoulli actions of $\Gamma = \mathrm{SL}(4, \mathbb{Z}) \ltimes \mathbb{Z}^4$ on $(X, \mu) = (\{0, 1\}, \mu_0)^{\Gamma / \Gamma_0}$, with Γ_0 a certain abelian subgroup of Γ and $\mu_0(0) \neq \mu_0(1)$. In fact, ([PV06]) gives also concrete examples of factors M with $\mathrm{Out}(M)$ any prescribed finitely generated group.

Note that when applied to the case $B = \mathbb{C}$, 10.1 becomes a von Neumann algebra analogue of Kurosh's classical theorem for free products of groups, similar to Ozawa's pioneering result of this type in ([Oz04]; see also his paper in these proceedings), but covering a different class of factors and allowing amplifications. For instance, if $M_i = L\Gamma_i, 2 \leq i \leq n$, $L\Lambda_j, 2 \leq j \leq m$, are factors from ICC groups having infinite normal subgroups with relative property (T), then $M_1 * M_2 * \cdots * M_m \overset{\theta}{\simeq} (N_1 * N_2 * \cdots * N_n)^t$ implies $m = n$ and $\theta(M_i)$ inner conjugate to N_i^t for all i, after some permutation of indices. When combined with results in ([DyR00]) and to the fact that $P = L(\mathbb{Z}^2 \rtimes \mathrm{SL}(2, \mathbb{Z}))$ has trivial fundamental group ([P01b]), this can be used to show that for all subgroups $S = \{s_j\}_j \subset \mathbb{R}_+^*$, $M = *_j P^{s_j}$ has fundamental

group equal to S. This provides a completely new class of factors M with $\mathcal{F}(M)$ an arbitrary subgroup $S \subset \mathbb{R}_+^*$, than the ones in ([P03]). Indeed, by Voiculescu's striking result in ([V94], cf. also [Sh04]) the factors $*_j P^{s_j}$ have no Cartan subalgebras, while the ones in ([P03]) arise from equivalence relations.

References

[An87] Anantharaman-Delaroche, C., On Connes' property (T) for von Neumann algebras. *Math. Japon.* **32** (1987), 337–355.

[Bo93] Boca, F., On the method for constructing irreducible finite index subfactors of Popa. *Pacific J. Math.* **161** (1993), 201–231.

[Bu91] Burger, M., Kazhdan constants for SL(3, $\mathbb{Z}$). *J. Reine Angew. Math.* **413** (1991), 36–67.

[CaH85] de Cannière, J., Haagerup, U., Multipliers of the Fourier algebra of some simple Lie groups and their discrete subgroups. *Amer. J. Math.* **107** (1985), 455–500.

[CCJJV01] Cherix, P.-A., Cowling, M., Jolissaint, P., Julg, P., Valette, A., *Groups with Haagerup property*. Progr. Math. 197, Birkhäuser, Basel 2001.

[Cho83] Choda, M., Group factors of the Haagerup type. *Proc. Japan Acad.* **59** (1983), 174–177.

[Ch79] Christensen, E., Subalgebras of a finite algebra. *Math. Ann.* **243** (1979), 17–29.

[C75] Connes, A., Sur la classification des facteurs de type II. *C. R. Acad. Sci. Paris* **281** (1975), 13–15.

[C76] Connes, A., Classification of injective factors. *Ann. of Math.* **104** (1976), 73–115.

[C80] Connes, A., A type II_1 factor with countable fundamental group. *J. Operator Theory* **4** (1980), 151–153.

[C82] Connes, A., Classification des facteurs. In *Operator algebras and applications* (Kingston, Ont., 1980), Part 2, Proc. Sympos. Pure Math. 38, Amer. Math. Soc., Providence, R.I., 1982, 43–109.

[CFW81] Connes, A., Feldman, J., Weiss, B., An amenable equivalence relation is generated by a single transformation. *Ergodic Theory Dynam. Systems* **1** (1981), 431–450.

[CJ82] Connes, A., Jones, V. F. R., A II_1 factor with two non-conjugate Cartan subalgebras. *Bull. Amer. Math. Soc.* **6** (1982), 211–212.

[CJ85] Connes, A., Jones, V. F. R., Property (T) for von Neumann algebras. *Bull. London Math. Soc.* **17** (1985), 57–62.

[CSh03] Connes, A., Shlyakhtenko, D., L^2-homology for von Neumann algebras. *J. Reine Angew. Math.* **586** (2005), 125–168.

[CW80] Connes, A., Weiss, B., Property (T) and asymptotically invariant sequences. *Israel J. Math.* **37** (1980), 209–210.

[CoH89] Cowling, M., Haagerup, U., Completely bounded multipliers and the Fourier algebra of a simple Lie group of real rank one. *Invent. Math.* **96** (1989), 507–549.

[CoZ89] Cowling, M., Zimmer, R., Actions of lattices in Sp(n, 1). *Ergodic Theory Dynam. Systems* **9** (1989), 221–237.

[Di54] Dixmier, J., Sous-anneaux abéliens maximaux dans les facteurs de type fini. *Ann. of Math.* **59** (1954), 279–286.

[D59] Dye, H., On groups of measure preserving transformations I. *Amer. J. Math.* **81** (1959), 119–159.

[D63] Dye, H., On groups of measure preserving transformations II. *Amer. J. Math.* **85** (1963), 551–576.

[Dy93] Dykema, K., Interpolated free group factors. *Duke Math J.* **69** (1993), 97–119.

[DyR00] Dykema, K., Rădulescu, F., Compressions of free products of von Neumann algebras. *Math. Ann.* **316** (1) (2000), 61–82.

[EL77] Effros, E., Lance, C., Tensor products of operator algebras. *Adv. Math.* **25** (1977), 1–34.

[FM77] Feldman, J., Moore, C. C., Ergodic equivalence relations, cohomology, and von Neumann algebras I; II. *Trans. Amer. Math. Soc.* **234** (1977), 289–324; 325–359.

[Fu99a] Furman, A., Gromov's measure equivalence and rigidity of higher rank lattices. *Ann. of Math.* **150** (1999), 1059–1081.

[Fu99b] Furman, A., Orbit equivalence rigidity. *Ann. of Math.* **150** (1999), 1083–1108.

[Fu06] Furman, A., On Popa's Cocycle Superrigidity Theorem. In preparation.

[G00] Gaboriau, D., Cout des rélations d'équivalence et des groupes. *Invent. Math.* **139** (2000), 41–98.

[G01] Gaboriau, D., Invariants ℓ^2 de rélations d'équivalence et de groupes. *Inst. Hautes Études Sci. Publ. Math.* **95** (2002), 93–150.

[G05] Gaboriau, D., Examples of groups that are measure equivalent to free groups. *Ergodic Theory Dynam. Systems* **25** (6) (2005), 1809–1827.

[GP03] Gaboriau, D., Popa, S., An Uncountable Family of Non Orbit Equivalent Actions of $\mathbb{F}_n$. *J. Amer. Math. Soc.* **18** (2005), 547–559.

[GeGo88] Gefter, S. L., Golodets, V. Y., Fundamental groups for ergodic actions and actions with unit fundamental groups. *Publ. Res. Inst. Math. Sci.* **6** (1988), 821–847.

[GoNe87] Golodets, V. Y., Nesonov, N. I., T-property and nonisomorphic factors of type II and III. *J. Funct. Anal.* **70** (1987), 80–89.

[HaV89] de la Harpe, P., Valette, A., La propriété T de Kazhdan pour les groupes localement compacts. *Astérisque* **175**, (1989).

[H79] Haagerup, U., An example of a non-nuclear C^*-algebra which has the metric approximation property. *Invent. Math.* **50** (1979), 279–293.

[Hj02] Hjorth, G., A converse to Dye's Theorem. *Trans Amer. Math. Soc.* **357** (2004), 3083–3103.

[HjKe05] Hjorth, G., Kechris, A., Rigidity theorems for actions of product groups and countable Borel equivalence relations. *Mem. Amer. Math. Soc.* **177** (833) 2005.

[I04] Ioana, A., A relative version of Connes $\chi(M)$ invariant. *Ergodic Theory Dynam. Systems*, to appear; arXiv:math.OA/0411164.

[IPeP05] Ioana, A., Peterson, J., Popa, S., Amalgamated free products of w-rigid factors and calculation of their symmetry groups. *Acta Math.*, to appear; arXiv:math.OA/0505589.

[Jo02] Jolissaint, P., On Property (T) for pairs of topological groups. *L'Enseignement Math.* **51** (2005), 31–45.

[J83] Jones, V. F. R., Index for subfactors. *Invent. Math.* **72** (1983), 1–25.

[J90] Jones, V. F. R., von Neumann algebras in mathematics and physics. In *Proceedings of the International Congress of Mathematicians* (Kyoto, 1990), Vol. I, The Mathematical Society of Japan, Tokyo, Springer-Verlag, Tokyo, 1991, 121–138.

[J00] Jones, V. F. R., Ten problems. In *Mathematics: perspectives and frontieres* (ed. by V. Arnold, M. Atiyah, P. Lax and B. Mazur), Amer. Math. Soc., Providence, RI, 2000, 79–91.

[Ka67] Kadison, R. V., Problems on von Neumann algebras. Baton Rouge Conference 1967.

[KaSi52] Kadison, R. V., Singer, I. M., Some remarks on representations of connected groups. *Proc. Nat. Acad. Sci. U.S.A.* **38** (1952), 419–423.

[K67] Kazhdan, D., Connection of the dual space of a group with the structure of its closed subgroups. *Funct. Anal. Appl.* **1** (1967), 63–65.

[Ma82] Margulis, G., Finitely-additive invariant measures on Euclidian spaces. *Ergodic Theory Dynam. Systems* **2** (1982), 383–396.

[Mc70] McDuff, D., Central sequences and the hyperfinite factor. *Proc. London Math. Soc.* **21** (1970), 443–461.

[Mo06] Monod, N., An invitation to bounded cohomology. In *Proceedings of the International Congress of Mathematicians* (Madrid, 2006), Volume II, EMS Publishing House, Zürich 2006, 1183–1211.

[MoS02] Monod, N., Shalom, Y., Orbit equivalence rigidity and bounded cohomology. *Ann. of Math.* **164** (2006), 825–878.

[MoS04] Monod, N., Shalom, Y., Cocycle superrigidity and bounded cohomology for negatively curved spaces. *J. Differential Geom.* **67** (2004), 395–455.

[M82] Moore, C. C., Ergodic theory and von Neumann algebras. In *Operator algebras and applications* (Kingston, Ont., 1980), Part 2, Proc. Symp. Pure Math. 38, Amer. Math. Soc., Providence, R.I., 179–226.

[MvN36] Murray, F., von Neumann, J., On rings of operators. *Ann. of Math.* **37** (1936), 116–229.

[MvN43] Murray, F., von Neumann, J., Rings of operators IV. *Ann. of Math.* **44** (1943), 716–808.

[OW80] Ornstein, D., Weiss, B., Ergodic theory of amenable group actions I. The Rohlin Lemma. *Bull. Amer. Math. Soc.* (1) **2** (1980), 161–164.

[Oz02] Ozawa, N., There is no separable universal II_1-factor. *Proc. Amer. Math. Soc.* **132** (2004), 487–490.

[Oz04] Ozawa, N., A Kurosh type theorem for type II_1 factors. *Internat. Math. Res. Notices*, Article ID 97560.

[OzP04] Ozawa, N., Popa, S., Some prime factorization results for type II_1 factors. *Invent Math.* **156** (2004), 223–234.

[Pe04] Peterson, J., A 1-cohomology characterization of property (T) in von Neumann algebras. *Pacific J. Math.*, to appear; arXiv:math.OA/0409527.

[PeP04] Peterson, J., Popa, S., On the notion of relative property (T) for inclusions of von Neumann algebras. *J. Funct. Anal.* **219** (2005), 469–483.

[PiP86] Pimsner, M., Popa, S., Entropy and index for subfactors. *Ann. Sci. École Norm. Sup.* **19** (1986), 57–106.

[P83] Popa, S., Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras. *J. Operator Theory* **9** (1983), 253–268.

[P86] Popa, S., Correspondences. INCREST preprint No. 56/1986, www.math.ucla.edu/~popa/preprints.html.

[P90] Popa, S., Free independent sequences in type II_1 factors and related problems. *Astérisque* **232** (1995), 187–202.

[P91] Popa, S., Markov traces on universal Jones algebras and subfactors of finite index. *Invent. Math.* **111** (1993), 375–405.

[P94] Popa, S., Classification of subfactors of type II. *Acta Math.* **172** (1994), 163–255.

[P97] Popa, S., Some properties of the symmetric enveloping algebras with applications to amenability and property T. *Doc. Math.* **4** (1999), 665–744.

[P01a] Popa, S., Some rigidity results for non-commutative Bernoulli shifts. *J. Funct. Anal.* **230** (2006), 273–328.

[P01b] Popa, S., On a class of type II_1 factors with Betti numbers invariants. *Ann. of Math.* **163** (2006), 809–889.

[P03] Popa, S., Strong Rigidity of II_1 Factors Arising from Malleable Actions of w-Rigid Groups I. *Invent. Math.* **165** (2006), 369–408.

[P04a] Popa, S., Strong Rigidity of II_1 Factors Arising from Malleable Actions of w-Rigid Groups II. *Invent. Math.* **165** (2006), 409–451.

[P04b] Popa, S., Some computations of 1-cohomology groups and construction of non orbit equivalent actions. *J. Inst. Math. Jussieu* **5** (2006), 309–332.

[P04c] Popa, S., *Deformation, Rigidity and Classification Results for Group Actions and von Neumann Algebras* . Course at College de France, Nov. 2004.

[P05] Popa, S., Cocycle and orbit equivalence superrigidity for malleable actions of w-rigid groups. arXiv:math.GR/0512646.

[P06] Popa, S., On the superrigidity of malleable actions with spectral gap. In preparation.

[PSa03] Popa, S., Sasyk, R., On the cohomology of Bernoulli actions. *Ergodic Theory Dynam. Systems* **27** (2007), 241–251.

[PSS04] Popa, S., Sinclair, A., Smith, R., Perturbation of subalgebras of type II_1 factors. *J. Funct. Anal.* **213** (2004), 346–379.

[PV06] Popa, S., Vaes, S., Strong rigidity of generalized Bernoulli actions and computations of their symmetry groups. arXiv:math.OA/0605456.

[R94] Radulescu, F., Random matrices, amalgamated free products and subfactors of the von Neumann algebra of a free group. *Invent. Math.* **115** (1994), 347–389.

[Sc81] Schmidt, K., Amenabilty, Kazhdan's property T, strong ergodicity and invariant means for ergodic group-actions. *Ergodic Theory Dynam. Systems* **1** (1981), 223–236.

[Sch63] Schwartz, J., Two finite, non-hyperfinite, non-isomorphic factors. *Comm. Pure Appl. Math.* **16** (1963), 19–26.

[S00] Shalom, Y., Rigidity of commensurators and irreducible lattices. *Invent. Math.* **141** (2000), 1–54.

[S05] Shalom, Y., Measurable group theory. In *Proceedings of the European Congress of Mathematics* (Stockholm, 2004), EMS Publishing House, Zürich 2004, 391–423.

[Sh04] Shlyakhtenko, D., On the classification of Full Factors of Type III. *Trans. Amer. Math. Soc.* **356** (2004) 4143–4159.

[Si55] Singer, I. M., Automorphisms of finite factors. *Amer. J. Math.* **177** (1955), 117–133.

[T03] Takesaki, M., *Theory of operator algebras*. Encyclopaedia Math. Sci. 127, Springer-Verlag, Berlin 2003.

[Th06] Thomas, S., Popa Superrigidity and Countable Borel Equivalence Relations. In preparation.

[To06] Tornquist, A., Orbit equivalence and actions of $\mathbb{F}_n$. *J. Symbolic Logic* **71** (2006), 265–282.

[V06] Vaes, S., Rigidity results for Bernoulli actions and their von Neumann algebras (after Sorin Popa). Séminaire Bourbaki, exposé 961; *Astérisque*, to appear.

[Va05] Valette, A., Group pairs with relative property (T) from arithmetic lattices. *Geom. Dedicata* **112** (2005), 183–196.

[Ve71] Vershik, A., Nonmeasurable decompositions, orbit theory, algebras of operators. *Dokl. Akad. Nauk SSSR* **199** (1971), 1218–1222.

[Vo90] Voiculescu, D., Circular and semicircular systems and free product factors. In *Operator algebras, unitary representations, enveloping algebras, and invariant theory* (Paris, 1989), Prog. Math. 92, Birkhäuser, Boston, 1990, 45–60.

[Vo94] Voiculescu, D., The analogues of entropy and of Fisher's information theory in free probability II. *Invent. Math.* **118** (1994), 411–440 .

[Z80] Zimmer, R., Strong rigidity for ergodic actions of semisimple Lie groups. *Ann. of Math.* **112** (1980), 511–529.

[Z84] Zimmer, R., *Ergodic Theory and Semisimple Groups*. Monogr. Math. 81, Birkhäuser, Basel 1984.

[Z91] Zimmer, R., Superrigidity, Ratner's theorem and the fundamental group. *Israel J. Math.* **74** (1991), 199–207.

Department of Mathematics, University of California, Los Angeles, CA 90095-155505, U.S.A.

E-mail: popa@math.ucla.edu

Cardiovascular mathematics

Alfio Quarteroni*

Abstract. In this paper we introduce some basic differential models for the description of blood flow in the circulatory system. We comment on their mathematical properties, their meaningfulness and their limitation to yield realistic and accurate numerical simulations, and their contribution for a better understanding of cardiovascular physio-pathology.

Mathematics Subject Classification (2000). 92C50,96C10,76Z05,74F10,65N30,65M60.

Keywords. Cardiovascular mathematics; mathematical modeling; fluid dynamics; Navier–Stokes equations; numerical approximation; finite element method; differential equations.

1. Introduction

The cardiovascular system has the task of supplying the human organs with blood. Its main components are the heart, the arteries and the veins. The so-called *large* (systemic) *circulation* brings oxygenated blood from the left ventricle via the aorta to the various organs through the arterial system, then brings it back through the venous system and the vena cava to the right atrium.

The *small circulation* is the one between the heart and the lungs. Blood is pumped from the right ventricle via the pulmonary artery to the lungs at a peak pressure of about 4 kPa. Venous blood enters the pulmonary system, gets oxygenated and returns to the left heart atrium (see Figure 1). In the past decade, the application of mathematical models, seconded by the use of efficient and accurate numerical algorithms, has made impressive progress in the interpretation of the circulatory system functionality, in both physiological and pathological situations, as well as in the perspective of providing patient specific design indications to surgical planning.

This has called for the development of a new field of applied mathematics: however, although many substantial achievements have been made in the field of modeling, mathematical and numerical analysis, and scientific computation, where a variety of new concepts and mathematical techniques have been introduced, most of the difficulties are still on the ground and represent major challenges for the years to come.

*I gratefully acknowledge the help from L. Formaggia, A. Veneziani, P. Zunino (MOX-Politecnico di Milano), G. Fourestey, G. Rozza (CMCS-EPFL) during the preparation of these notes. This research has been made possible by the financial support of EU Project HPRN-CT-2002-00270 "Haemodel", the MIUR grant "Numerical Modelling for Scientific Computing and Advanced Applications" and the INDAM grant "Integration of Complex Systems in Biomedicine".

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

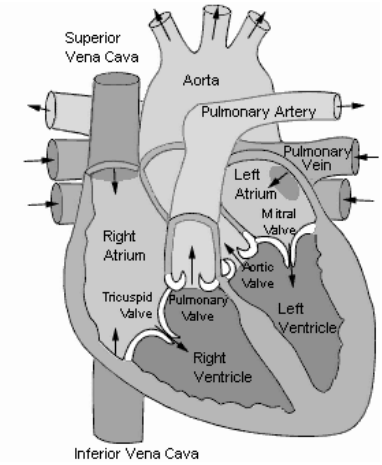


Figure 1. The human heart. Courtesy of the Texas Heart®Institute.

The main impulse to develop this field of study is the increasing demand from the medical community for scientifically rigorous and quantitative investigations of cardiovascular diseases, which are responsible today for about the 40% od deaths in industrialized societies. The 3/4 of them are related to atherosclerosis, which manifests as, e.g., stroke, myocardial infarction or peripheral vascular diseases. For example, in vascular surgery, arterial bypass grafting is a common practice to treat coronary artery and peripheral vascular diseases. Nonetheless, over 50% of coronary artery bypass grafts fail within 10 years and more than 25% of infra-inguinal grafts within 5 years (see [9], [31], [96]). The principal cause is neo-intimal hyperplasia that may degenerate in atherosclerosis. A better understanding of local haemodynamics, like the detection of regions of low wall shear stress and of high residence time for blood particles, is of utmost importance to assess its correlation with atherogenesis ([11]).

The vascular system is highly complex and able to regulate itself: an excessive decrease in blood pressure will cause the smaller arteries (the arterioles) to contract and the heart rate to increase, whereas an excessive blood pressure is counter-reacted by a relaxation of the arterioles (which causes a reduction of the periphery resistance to the flow) and a decrease of the heart beat. Yet, it may happen that some pathological conditions develop. For example, the arterial wall may become more rigid, due to illness or excessive smoking habits, fat may accumulate in the arterial walls causing a reduction of the vessel section (a stenosis) and eventually an aneurysm may develop. The consequence of these pathologies on the blood field as well as the possible outcome of a surgical intervention to cure them may be studied by numerical simulations, that are less invasive than *in-vivo* investigation, and far more accurate and flexible than *in-vitro* experiments. Numerical models require patient's data (the

initial and boundary conditions for the PDE systems, as well as geometrical data to characterize the shape of the computational domain) that can be generated by radiological acquisition through, e.g., computer tomography, magnetic resonance, doppler anemometry, etc. Besides their employment in medical research, numerical models of vascular flows can provide a virtual experimental platform to be used as training system. For instance, a technique now currently used to cure a stenosis is angioplasty, which consists of inflating a balloon positioned in the stenotic region by the help of a catheter. The balloon should squash the stenosis and approximately restore the original lumen area. The success of the procedure depends, among other factors, on the sensitivity of the surgeon and his ability of placing the catheter in the right position. A training system which couples virtual reality techniques with the simulation of the flow field around the catheter, the balloon and the vessel walls, employing geometries extracted from real patients, could well serve as training bed for new vascular surgeons. A similar perspective could provide specific design indications for the realization of surgical operations. For instance, numerical simulations could represent a tool for the design of new prototypes, or for devising prosthetic devices by the help of shape optimization theory. In particular, shape optimization has been used for minimizing the downstream vorticity in coronary by-pass grafts (see [1], [76], [85]). These numerical investigations can help the surgeon in understanding how the different surgical solutions may affect blood circulation and guide the choice of the most appropriate procedure for a specific patient. In such "virtual surgery" environments, the outcome of alternative treatment plans for the individual patient can be foreseen by simulations, yielding a new paradigm of the clinical practice which is referred to as "predictive medicine" (see [92]).

In this presentation we will address some of the most basic models that are used to describe blood flow dynamics in local arterial environments (Section 2) and to predict the vessel wall deformation in compliant arteries (Section 3). Then we will introduce appropriate geometrical multiscale models that integrate three-dimensional, one-dimensional and zero-dimensional models for the simulation of blood circulation in the whole arterial tree (Section 4). Finally, in Section 5 we consider the problem of modeling biochemical processes occurring across the several layers of the arterial wall.

2. Mathematical models for local blood flow dynamics

The mathematical equations of fluid dynamics are the key components of haemodynamics modeling. Rigorously speaking, blood is not a fluid but a suspension of particles in a fluid called *plasma*, which is made of water for the 90–92%, proteins (like serum albumin, globulins and fibrinogen) for the 7% and inorganic constituents for the rest. The most important blood particles are red cells, white cells and platelets. Red cells (erythrocytes) are responsible for the exchange of oxygen and carbon-dioxide with the cells. They are about $4\text{–}6 \cdot 10^6$ biconcave disks per mm^3 and provide the

45% of blood volume; they are made by the 65% of water, the 3% of membrane components, and around the 32% by haemoglobin.

White cells (leukocytes), play a major role in the human immune system: they are (roughly) spherical, and are $4–11 \cdot 10^3$ per mm^3. Platelets (thrombocytes) are the main responsible for blood coagulation: they are rounded or oval disks and there are $3–5 \cdot 10^5$ per mm^3.

Rheological models in smaller arterioles and capillaries should account for the presence of blood cells since their size becomes comparable to that of the vessel. In this section, however, we will bound our investigation to flow in *large and medium sized vessels*.

The principal quantities which describe blood flow are the *velocity* $\boldsymbol{u}$ and *pressure* P. Knowing these fields allows the computation of the *stresses* to which an arterial wall is subjected due to the blood movement. When addressing fluid-structure interaction problems (see Section 3), the *displacement* of the vessel wall due to the action of the flow field is another quantity of relevance. Pressure, velocity and vessel wall displacement will be functions of time and the spatial position. Accounting for *temperature* variation may be relevant in some particular context, for instance in the hyperthermia treatment, where some drugs are activated through an artificial localized increase in temperature (see [47], [28]). Temperature may also have a notable influence on blood properties, in particular on blood viscosity. Yet, this aspect is relevant only in the flow through very small arterioles/veins and in the capillaries, a subject which is covered only partially in these notes. Another aspect related with blood flow modeling is the *chemical interaction* with the vessel wall, which is relevant both for the physiology of the blood vessels and for the development of certain vascular diseases. Not mentioning the potential relevance of such investigation for the study of the propagation/absorption of pharmaceutical chemicals. A short account will be given in Section 5.

A major feature of blood flow is represented by its pulsatility. With some approximation one may think the blood flow to be periodic in time. Yet, this is usually true only for relatively short periods, since the various human activities require to change the amount of blood sent to the various organs. The cardiac cycle features two distinct phases. The *systolic* phase, when the heart pumps the blood into the arterial system, is characterized by the highest flow rate. The *diastolic* phase is when the heart is filling up with the blood coming from the venous system and the aortic valve is closed. Figure 2 illustrates a typical flow rate curve of a large artery during the cardiac cycle. Pulsatility induces flow reversal which manifests near arterial walls, a phenomenon that can enhance the appearance of stenoses in specific vascular districts, like the carotid bifurcation (see Figure 3).

To simplify our presentation, in this section we will introduce the flow equations in a "truncated" blood vessel like the one illustrated in Figure 4, which is representative of a small portion of the arterial system. We will make the further assumption that the vessel is rigid, thus the flow domain, denoted by Ω, is independent of time. (This unphysical restriction will be removed in next section where we will specifically

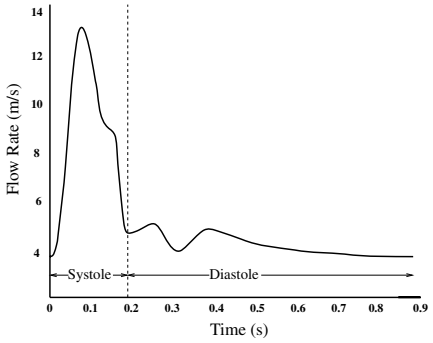


Figure 2. A typical flow rate in an artery during the cardiac cycle.

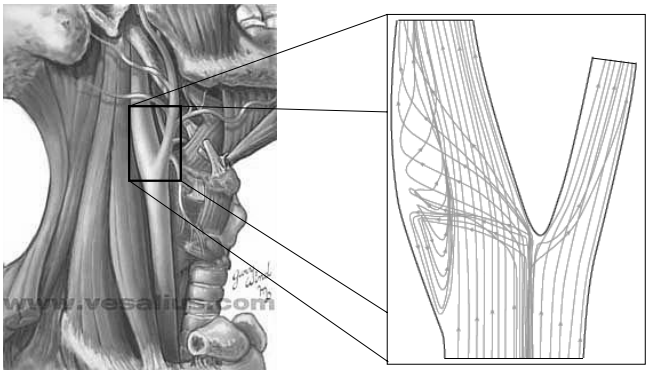


Figure 3. Recirculation in the carotid bifurcation. On the left we illustrate the location of the carotid bifurcation. The image on the right shows the particle path during the diastolic period in a model of the carotid bifurcation. A strong recirculation occurs inside the carotid sinus. The image on the left is courtesy of vesalius.com.

address the interaction between blood flow and arterial wall deformation.) If we denote by $\rho = \rho(\boldsymbol{x}, t)$ the blood density and by $\boldsymbol{u} = \boldsymbol{u}(\boldsymbol{x}, t)$ the blood velocity, the principle of conservation of mass yields the *continuity equation*

$$\partial_t \rho + \operatorname{div}(\rho \boldsymbol{u}) = 0 \quad \text{for } x \in \Omega,\ t > 0 \tag{1}$$

where ∂_t is the partial derivative w.r.t. t, while $\operatorname{div} \boldsymbol{u} = \sum_{i=1}^{3} \partial_{x_i} u_i$ is the spatial divergence of the vector field $\boldsymbol{u}$.

In large and medium size vessels the blood density can be assumed to be constant, then from (1) we derive the kinematic constraint

$$\operatorname{div}(\boldsymbol{u}) = 0 \quad \text{in } \Omega, \tag{2}$$

which in view of the Euler expansion formula implies flow incompressibility.

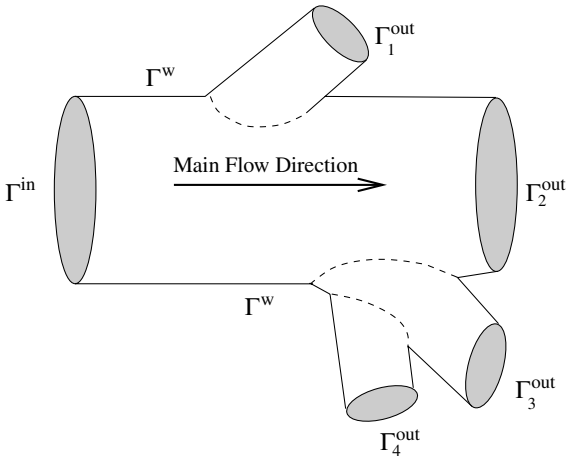


Figure 4. An example of a computational domain made of a section of the vascular system. We need to provide proper boundary conditions at inflow Γ^{in}, outflow Γ^{out} and wall Γ^{w}.

On the other hand, the principle of conservation of momentum, which states that body forces, applied surface forces and internal "cohesion" forces must be in equilibrium, writes

$$\rho \frac{D\boldsymbol{u}}{Dt} - \operatorname{div}(\boldsymbol{T}) = \rho \boldsymbol{f} \quad \text{for } x \in \Omega,\ t > 0, \tag{3}$$

where $\frac{D\boldsymbol{u}}{Dt} = \partial_t \boldsymbol{u} + (\boldsymbol{u} \cdot \nabla)\boldsymbol{u}$ is the fluid acceleration (∇ is the spatial gradient), $\boldsymbol{f}$ is the specific body force (e.g., $\boldsymbol{f} = -g\boldsymbol{e_3}$ where $\boldsymbol{e_3}$ represents the unit vector in the vertical direction and g the gravitational acceleration), while $\boldsymbol{T}$ is the Cauchy stress tensor (see [3] and [86]). The system (2),(3) can be closed by using a constitutive law that relates the Cauchy stress to kinematic quantities (velocity and pressure), and which is peculiar to the specific rheological behavior of the fluid under consideration. In large and medium size vessel, blood behaves as a Newtonian incompressible fluid, where we have

$$\boldsymbol{T} = -P\boldsymbol{I} + 2\mu \boldsymbol{D}(\boldsymbol{u}); \tag{4}$$

P is a scalar function (the pressure), $\boldsymbol{I}$ is the identity matrix, μ is the dynamic viscosity, $\boldsymbol{D}(\boldsymbol{u}) = \frac{1}{2}(\nabla \boldsymbol{u} + \nabla \boldsymbol{u}^T)$ is the *strain rate* tensor, $D_{ij} = \frac{1}{2}\big(\frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i}\big)$, $i, j = 1, \ldots, 3$. Then (3) becomes

$$\partial_t \boldsymbol{u} + (\boldsymbol{u} \cdot \nabla)\boldsymbol{u} + \nabla p - 2\operatorname{div}(\nu \boldsymbol{D}(\boldsymbol{u})) = \boldsymbol{f} \tag{5}$$

where $p = \frac{P}{\rho}$ is a scaled pressure and $\nu = \frac{\mu}{\rho}$ is the kinematic viscosity. More in general, ν may depend on kinematic quantities. Several models have been proposed in this respect, as we will see later in this section.

The Navier–Stokes system of continuity and momentum equations must be closed by initial conditions on velocity, say $\boldsymbol{u} = \boldsymbol{u_0}$ for $x \in \Omega$ and $t = 0$, and boundary conditions on the domain boundary, for all $t > 0$. Mathematically admissible boundary conditions are of either Dirichlet or Neumann type

$$\boldsymbol{u} = \boldsymbol{g} \ \text{ on } \Gamma_D, \quad \boldsymbol{T} \cdot \boldsymbol{n} = \boldsymbol{\varphi} \ \text{ on } \Gamma_N, \tag{6}$$

respectively, where $\boldsymbol{n}$ is the unit outward normal vector on $\partial\Omega$, $\Gamma_D \cup \Gamma_N = \partial\Omega$, and either Γ_D or Γ_N may be empty. The conditions to apply are normally driven by physical considerations. For instance, for a viscous fluid ($\mu > 0$), we have to impose the homogeneous Dirichlet condition $\boldsymbol{u} = \boldsymbol{0}$ at a solid fixed boundary, like the vessel wall Γ^{w} in Figure 4. When we will consider the coupled problem between fluid and vessel wall, Γ^{w} will deform, hence the homogeneous Dirichlet condition will be replaced by $\boldsymbol{u} = \boldsymbol{w}$, where $\boldsymbol{w}$ is the (unknown) wall velocity. When dealing with an artificial boundary, that is a boundary which truncates the space occupied by the fluid (for computational reasons) like the sections Γ^{in} and Γ^{out} in Figure 4, the choice of appropriate conditions is often more delicate and should in any case guarantee the well-posedness of the resulting differential problem.

We anticipate the fact (without providing the proof) that this choice of boundary conditions, with the hypothesis that at Γ^{out} the velocity satisfies everywhere the condition $\boldsymbol{u} \cdot \boldsymbol{n} > 0$, is sufficient to guarantee that the solution of the Navier–Stokes problem exists and is continuously dependent from the data (initial solution, boundary conditions, forcing terms), provided that the initial data and the forcing term be sufficiently small.

Unfortunately, the homogeneous Neumann condition is rather unphysical for the case of a human vessel. As a matter of fact, it completely neglects the presence of the remaining part of the circulatory system. The issue of devising appropriate boundary conditions on artificial boundaries of deformable arteries is still open and is the subject of active research. A possibility is provided by coupling the Navier–Stokes equations on a specific portion of the artery with reduced models, which are able to represent, although in a simplified way, the presence of the remaining part of the circulatory system. Techniques of this type has been used and analyzed in [32], [33]. An account will be given in Section 4. Normally, on arterial sections like Γ^{in} and Γ^{out} only "averaged" data are available (mean velocity and mean pressure instead of a vector condition like that in (6)), which are therefore insufficient for a "standard" treatment of the mathematical problem. One has thus to devise alternative formulations for the boundary conditions which, on one hand, reflect the physics and exploit the available data and, on the other hand, permit to formulate a mathematically well posed problem. In these notes we will not investigate this particular aspect, which is however illustrated and analyzed in [34], [97], [98].

Now we will make some considerations on the behavior of blood flow. Most often, it is laminar. Characteristic values of the Reynolds number, $\mathrm{Re} = \frac{\rho U L}{\mu}$, where U is a representative mean flow velocity and L is a linear length of the vessel at hand, are given in Table 1. In normal physiological situations, the values of the Reynolds

number reached in the cardiovascular system do not allow the formation of full scale turbulence. Some flow instabilities may occur only at the exit of the aortic valve and

Table 1. Some representative values of velocity, vessel size, average Reynolds numbers, cross-sectional area and thickness of blood vessels.

Vessel	Number	Diameter [cm]	Area [cm^2]	Wall thickness [cm]	Velocity [cm/s]	Average Reynolds number
Aorta	1	2.5	4.5	0.2	48	3400
Arteries	159	0.4	20	0.1	45	500
Arterioles	400	0.005	$5.7 \cdot 10^7$	0.002	5	0.7
Capillaries	4500	0.0008	$1.6 \cdot 10^{10}$	0.0001	0.1	0.002
Venules	4000	0.002	$1.3 \cdot 10^9$	0.0002	0.2	0.01
Veins	40	0.5	200	0.05	10	140
Vena cava	18	3	0.15	3300	38	3300

limited to the systolic phase. In this region the Reynolds number may reach the value of few thousands only for the portion of the cardiac cycle corresponding to the peak systolic velocity, however, there is not enough time for a full turbulent flow to develop.

When departing from physiological conditions, there are several factors that may induce transition from laminar to turbulent flows. For instance, the increase of flow velocity because of physical exercise, or due to the presence of a stenotic artery or a prosthetic implant such as a shunt, may induce an increase of the Reynolds number and lead to turbulence. Smaller values of blood viscosity also raise the Reynolds number; this may happen in the presence of severe anemia, when the hematocrit drops sharply (and so does the viscosity).

The rheological behavior of blood flow is complex to describe, and is still a subject of investigation. Nonetheless, a few peculiar phenomena are worth being mentioned. Red blood cells tend to aggregate by attaching each other side by side (resembling stacks of coins) forming *rouleaux*. Under shear stress, red blood cells can deform into a variety of shapes (for instance they become ellipsoids) without modifying their volume or surface area. Both aggregation and deformability affect the rheological properties of blood flow, and, particularly, blood viscosity at low shear rates and its sedimentation velocity.

In general terms, blood is a non-Newtonian fluid. At low shear rates, viscoelastic effects become relevant. In small capillaries, at small Reynolds and Womersley number, viscous effects become predominant, whereas inertial forces become negligible. The Womersley number is defined as $\alpha = R(\omega/\nu)^{1/2}$, where R is the radius, ω is the angular frequency of the oscillatory motion and ν is the kinematic viscosity. Below a critical vessel caliber (about 1 mm), blood viscosity becomes dependent on the vessel radius and decreases very sharply. This is known as Fahraeus–Lindquist effect: red

blood cells move to the central part of the capillary whereas the plasma stay in contact with the vessel wall. This layer of plasma facilitates the motion of the red cells, thus causing a decrease of the apparent viscosity. High shear rate and increased blood cell deformation are further important factors that explain viscoelastic behavior.

Some blood diseases may severely alter the rheological behavior of blood. For instance thalassemia causes red blood cells to become less deformable. In leukemia there is an increased number of poorly deformable white blood cells. In hypertension the haematocrit increases leading to a significant high blood viscosity with elevated total plasma protein, albumin, globulin and fibrinogen. See [56].

To account for these phenomena we have to abandon the Newtonian law (4). In *generalized Newtonian fluids*, the viscosity μ is assumed to depend on the shear rate $\dot{\gamma}$, a measure of the rate of shear deformation. For a simple shear flow in a straight channel (see Figure 5), $\dot{\gamma} = U/h$ is just the gradient of velocity. More in general, $\dot{\gamma} = \sqrt{2\,\mathrm{tr}(\boldsymbol{D}(\boldsymbol{u}))^2}$.

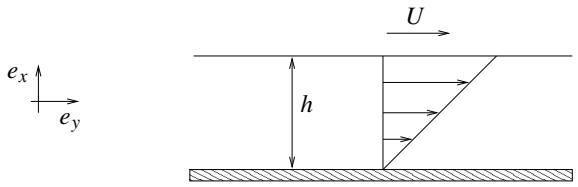


Figure 5. Schematic example of a simple shear flow in a straight channel.

A simple model is given by the so-called *Power-Law* where n is named the power-law index. The flow is *shear thinning* if $n < 1$ and *shear thickening* if $n > 1$. (Shear thinning fluids are those for which viscosity decreases as the shear rate increases.) The Prandtl–Eyring model, $\mu(\dot{\gamma}) = \mu_0 \sinh^{-1}(\lambda\dot{\gamma})/\lambda\dot{\gamma}$ where λ is a material constant, the Powell–Eyring model, $\mu(\dot{\gamma}) = \mu_\infty + (\mu_0 - \mu_\infty)\sinh^{-1}(\lambda\dot{\gamma})/\lambda\dot{\gamma}$, the Cross-model $\mu(\dot{\gamma}) = \mu_\infty + (\mu_0 - \mu_\infty)/(1 + (\lambda\dot{\gamma})^n)^{-1}$, the Carreau model $\mu(\dot{\gamma}) = \mu_\infty + (\mu_0 - \mu_\infty)/(1 + (\lambda\dot{\gamma})^2)^{(1-n)/2}$, represent other noticeable examples of generalized Newtonian models.

Blood is in general modeled as a shear thinning, nonlinear viscoelastic flow.

More complicated models are the shear thinning generalized Oldroyd-B models, where $\boldsymbol{T} = -P\boldsymbol{I} + \boldsymbol{\tau}$ and $\boldsymbol{\tau}$ satisfies the differential problem

$$\boldsymbol{\tau} + \lambda_1[\dot{\boldsymbol{\tau}} - (\nabla \boldsymbol{u})\boldsymbol{\tau} - \boldsymbol{\tau}(\nabla \boldsymbol{u}^T)] = \mu(\boldsymbol{D}(\boldsymbol{u}))\boldsymbol{D}(\boldsymbol{u}) + \lambda_2[\dot{\boldsymbol{D}}(\boldsymbol{u}) - (\nabla \boldsymbol{u})\boldsymbol{D}(\boldsymbol{u}) - \boldsymbol{D}(\boldsymbol{u})(\nabla \boldsymbol{u}^T)]$$

where λ_1, λ_2 are material constants that characterize the model. For a discussion on rheological properties of blood flow we refer, e.g., to [12], [38], [39], [94], [57]. For a more thorough mathematical analysis of Oldroyb-B models see, e.g., [102], [4], [83], [68], [40], [41], [71].

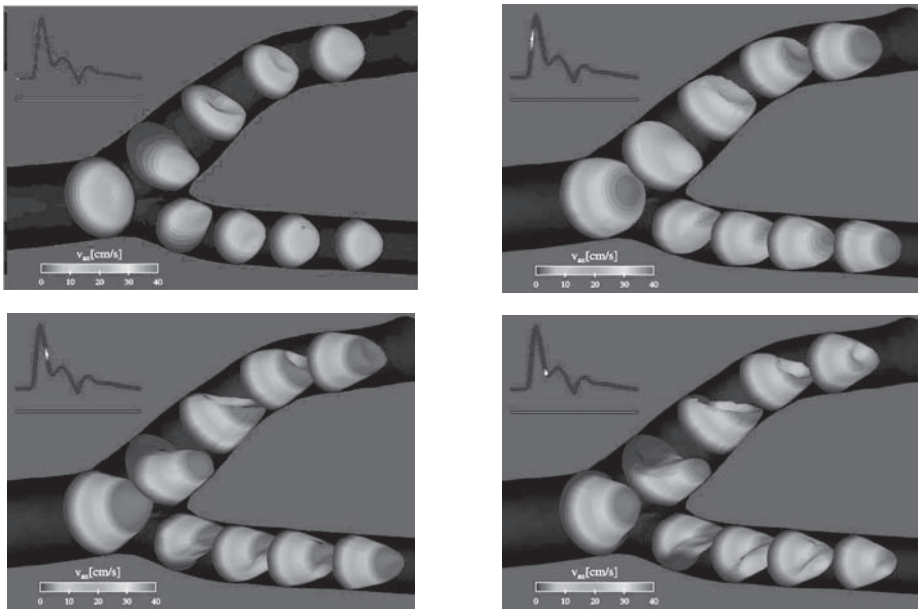


Figure 6. Velocity profiles computed in a carotid bifurcation during systole and diastole (courtesy of M. Prosi).

3. Mathematical models for local blood-flow dynamics in compliant vessels

In human physiology, the arterial walls deform under the action of the flow field. This aspect is relevant especially for large or even relatively large vessels, whereas in arterioles and capillaries the movement of the wall may be considered negligible. In the aorta, for example, the radius may vary in a range of 5% to 10% between diastole and systole. This is quite a large displacement, which affects the flow field. The fluid wall interaction problem is the responsible for the propagation of pulse pressure waves. Indeed, no propagative phenomena would otherwise occur in an incompressible fluid like blood. This interaction problem is a particular instance of the more general fluid-structure interaction (FSI) problem (the solid structure being here the vessel wall). It is indeed a rather complex one, since the time scales associated to the interaction phenomena are two orders of magnitude greater than those associated to the bulk flow field.

The vascular wall has a very complex nature; devising an accurate model for its mechanical behavior is rather difficult. Its structure is indeed formed by many layers with different mechanical characteristics [38], [48]. The most important are the endothelium (of about 2 microns, with anti-adhesive function), the tunica intima (of 10 microns, made of connective tissue), the internal elastic lamina, of 2 microns,

the media (of about 300 microns, with structural functions) and the adventitia, where the vasa vasorum stand (see Figure 7). Unfortunately, experimental results obtained by specimens are only partially significant. Indeed, the vascular wall is a living tissue with the presence of muscular cells which contribute to its mechanical behavior. It may then be expected that the dead tissue used in the laboratory will have different mechanical characteristics than the living one. Moreover, the arterial mechanics depends also on the type of the surrounding tissues, an aspect almost impossible to reproduce in a laboratory. It is the role of mathematical modeling to find reasonable

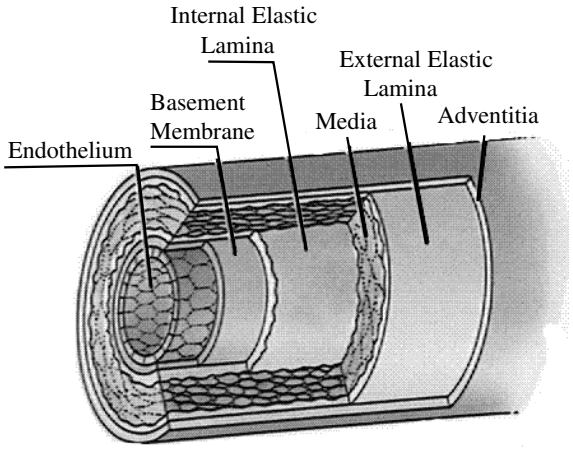


Figure 7. The vessel wall is formed by many layers made of tissues with different mechanical characteristics. Image taken from "Life: the Science of Biology" by W.K. Purves et al., fourth edition, published by Sinauer Associates Inc. and W.H. Freeman and Company.

simplifying assumptions by which major physical characteristics remain present, yet the problem becomes amenable to numerical analysis and computational solution.

The geometry of a portion of an artery where no branching is present may be described by using a curvilinear cylindrical coordinate system (r, θ, z) with the corresponding base unit vectors $\boldsymbol{e}_r$, $\boldsymbol{e}_\theta$, and $\boldsymbol{e}_z$, where $\boldsymbol{e}_z$ is aligned with the axis of the artery, as shown in Figure 10. (In this figure, R indicates the radius of the lumen.) Clearly, the vessel structure may be studied using full three dimensional models, which may also account for its multilayered nature. However, it is common practice to resort to simplified 2D or even 1D mechanical models in order to reduce the overall computational complexity when the final aim is to study the coupled fluid-structure problem. A 2D model may be obtained by either resorting to a shell-type description or considering longitudinal sections ($\theta = \text{const.}$) of the vessels. In the first case we exploit the fact that the effective wall thickness is relatively small to reduce the whole structure to a surface. A rigorous mathematical derivation (for the linear case) may be found in [15]. In the second case we neglect the variations of

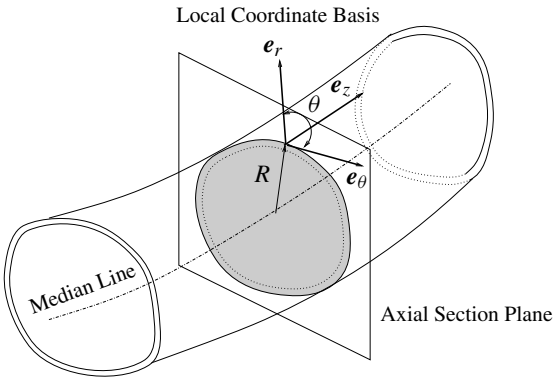


Figure 8. A model of a "realistic" section of an artery with the principal geometrical parameters.

the stresses in the circumferential direction. In this way we are able to eliminate all terms containing derivatives with respect to θ in the equations and we may consider each plane $\theta = \text{const.}$ independently. The resulting displacement field will depend only parametrically on θ. If, in addition, we assume that the problem has an axial symmetry (which implies the further assumption of a straight axis) the dependence on θ is completely neglected. In this case, also the fluid would be described by a 2D axi-symmetric model (see [25]).

The simplest models, called 1D models, are derived by making the same assumption on the wall thickness made for the shell model, yet starting from a 2D model. The structure will then be represented by a line on a generic longitudinal section. Even with all these simplifying assumptions an accurate model of the vessel wall mechanics is rather complex.

A three-dimensional model that describes the complete coupled system made of the equations of blood flow and those for the vessel wall deformation can be derived by adopting a coupled Eulerian–Lagrangian approach (differently to what done in Section 2 where the vessel walls were considered as being rigid).

With this purpose, we denote by $\hat{\Omega}$ a reference domain (corresponding, e.g., to a specific portion of an arterial vessel at rest, or else at an initial time). We write $\bar{\hat{\Omega}} = \bar{\hat{\Omega}}^s \cup \bar{\hat{\Omega}}^f$, where $\hat{\Omega}^f$ is the portion of the domain occupied by the fluid (i.e. the lumen) while $\hat{\Omega}^s$ corresponds to the portion of the solid vessel wall (see Figure 9 for a two dimensional representation). In a given time interval $[0, T]$ the domain deformation is described through a couple of functions:

$$L^s : \hat{\Omega}^s \times [0, T] \to \Omega^s(t), \quad A^f : \hat{\Omega}^f \times [0, T] \to \Omega^f(t),$$

where $\Omega^s(t)$ denotes the domain occupied by the solid (the vessel wall) and $\Omega^f(t)$ that occupied by the fluid at time t. The computational domain in which we aim at solving the coupled fluid-wall problem at time t is then $\Omega(t)$ s.t. $\bar{\Omega}(t) = \bar{\Omega}^s(t) \cup \bar{\Omega}^f(t)$. Note

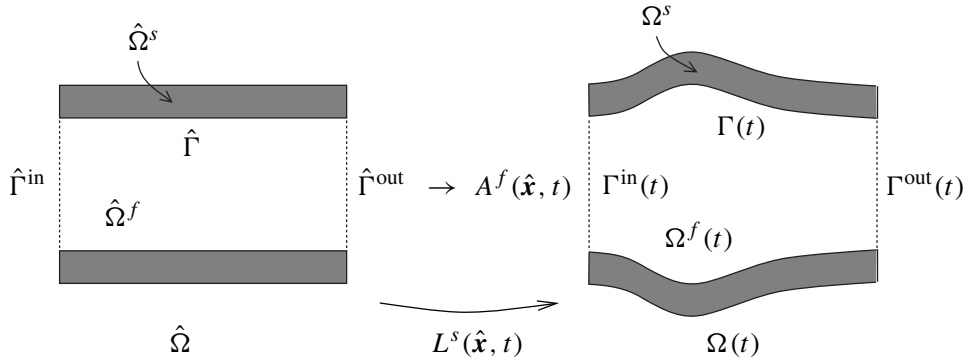


Figure 9. Parametrization of the domain.

that the boundary $\partial\Omega(t)$ of $\Omega(t)$ is made of a physical boundary (the external surface of the vessel wall, that has deformed) plus a virtual boundary (the vertical walls in the domain of Figure 9) that has not changed its position from its reference state. In fact, L^s is the Lagrangian transformation of the solid domain: the domain displacement is described by the law $\boldsymbol{\eta}(\hat{\boldsymbol{x}}, t) = L^s(\hat{\boldsymbol{x}}, t) - \hat{\boldsymbol{x}}$ for all $\hat{\boldsymbol{x}} \in \hat{\Omega}^s$, and the velocity of any point $\hat{\boldsymbol{x}}$, given by $\partial_t L^s(\hat{\boldsymbol{x}}, t) = \partial_t \boldsymbol{\eta}(\hat{\boldsymbol{x}}, t)$, is denoted by $\dot{\boldsymbol{\eta}}(\hat{\boldsymbol{x}}, t)$.

Within the fluid domain $\Omega^f(t)$, A^f is a transformation such that $A^f|_{\hat{\Gamma}} = L^s|_{\hat{\Gamma}}$ but which otherwise does not follow the material trajectories. The set of transformation $\{L^s, A^f\}$ is in fact an *Arbitrary Lagrangian Eulerian transformation* (ALE) that, at each time t, is capable to retrieve the actual position of the computational domain $\Omega(t)$ starting from the reference domain $\hat{\Omega}$. Let us denote by

$$\boldsymbol{F}^s(\hat{\boldsymbol{x}}, t) = \nabla_{\hat{\boldsymbol{x}}} L^s(\hat{\boldsymbol{x}}, t) = \boldsymbol{I} + \nabla_{\hat{\boldsymbol{x}}} \boldsymbol{\eta}(\hat{\boldsymbol{x}}, t) \quad \text{and} \quad \boldsymbol{F}^f(\hat{\boldsymbol{x}}, t) = \nabla_{\hat{\boldsymbol{x}}} A^f(\hat{\boldsymbol{x}}, t)$$

the gradients of the two maps, called the *deformation tensors*, and by

$$J^s(\hat{\boldsymbol{x}}, t) = \det \boldsymbol{F}^s(\hat{\boldsymbol{x}}, t) \quad \text{and} \quad J^f(\hat{\boldsymbol{x}}, t) = \det \boldsymbol{F}^f(\hat{\boldsymbol{x}}, t)$$

their determinants. The fluid domain velocity is denoted by $\hat{\boldsymbol{w}}(\hat{\boldsymbol{x}}, t) = \partial_t A^f(\hat{\boldsymbol{x}}, t)$. Note that, still referring to the case depicted in Figure 9, on the vertical (virtual) boundaries it is $\hat{\boldsymbol{w}} \cdot \boldsymbol{n} = \boldsymbol{0}$, whereas on $\hat{\Gamma}$ we have $\hat{\boldsymbol{w}} = \dot{\boldsymbol{\eta}}$.

The structural deformation can be modeled in many different ways, as we have anticipated at the beginning of this section. Here we will consider the following model

$$\rho^s \frac{\partial^2 \boldsymbol{\eta}}{\partial t^2} - \operatorname{div}_{\hat{\boldsymbol{x}}}(\boldsymbol{F}^s \boldsymbol{\Sigma}^s) = 0 \quad \text{in } \hat{\Omega}^s, \ t > 0$$

where $\boldsymbol{\Sigma}^s$ is the second Piola–Kirchoff stress tensor. It depends on the Green-St.Venant strain tensor $\boldsymbol{E} = \frac{1}{2}((\boldsymbol{F}^s)^T \boldsymbol{F}^s - \boldsymbol{I})$, according to a constitutive law characteristic of the solid structure at hand. Typically, $\boldsymbol{\Sigma}^s = \frac{\partial \boldsymbol{\Psi}}{\partial \boldsymbol{E}}$, where $\boldsymbol{\Psi}$ is the density

of a given elastic energy. Finally, ρ^s is the density of the structure in the reference configuration. By combining this equation with the Navier–Stokes equations (2)–(3) for the fluid we end up with the following coupled fluid-structure problem, for all $t > 0$:

$$\hat{\boldsymbol{w}} = H(\dot{\boldsymbol{\eta}}|_{\hat{\Gamma}}) \quad \text{in } \hat{\Omega}^f, \quad \boldsymbol{w} = \hat{\boldsymbol{w}} \circ (A^f)^{-1}, \tag{7}$$

$$\rho^f \frac{\partial \boldsymbol{u}}{\partial t|_{\hat{\boldsymbol{x}}}} + \rho^f (\boldsymbol{u} - \boldsymbol{w}) \cdot \nabla \boldsymbol{u} + \operatorname{div}(\boldsymbol{T}^f) = \rho^f \boldsymbol{f} \quad \text{in } \Omega^f(t), \tag{8}$$

$$\operatorname{div}(\boldsymbol{u}) = 0 \quad \text{in } \Omega^f(t), \tag{9}$$

$$\rho^s \frac{\partial^2 \boldsymbol{\eta}}{\partial t^2} - \operatorname{div}_{\hat{\boldsymbol{x}}}(\boldsymbol{F}^s \boldsymbol{\Sigma}^s) = 0 \quad \text{in } \hat{\Omega}^s, \tag{10}$$

$$\boldsymbol{u} = \dot{\boldsymbol{\eta}} \circ (L^s)^{-1} \quad \text{on } \Gamma(t), \tag{11}$$

$$\boldsymbol{F}^s \boldsymbol{\Sigma}^s \cdot \hat{\boldsymbol{n}}^s = J^f \boldsymbol{T}^f \cdot (\boldsymbol{F}^f)^{-T} \cdot \hat{\boldsymbol{n}}^s \quad \text{on } \hat{\Gamma}, \tag{12}$$

where $\hat{\boldsymbol{n}}^s$ denotes the outward unit vector on $\hat{\Gamma}$, $\frac{\partial}{\partial t|_{\hat{\boldsymbol{x}}}}$ represents the ALE time derivative (see [75]) and $H(.)$ denotes any continuous extension operator from $\hat{\Gamma}$ to the fluid domain $\hat{\Omega}^f$ (for instance the harmonic extension, or else the extension by the linear elasticity operator).

This coupled problem needs to be completed with the initial conditions on $\boldsymbol{u}$, $\boldsymbol{\eta}$ and $\dot{\boldsymbol{\eta}}$ as well as by suitable boundary conditions on $\partial\Omega^s(t)\backslash\Gamma(t)$ and $\partial\Omega^f(t)\backslash\Gamma(t)$.

At the best of our knowledge, a complete mathematical analysis of the coupled fluid-structure problem (7)–(12) is not available yet. In the steady case, for small enough applied forces, existence of regular solutions is proven in [44]. In the unsteady case, local solvability in time is proven in the simple case where the structure is a collection of rigid moving bodies in [45]. See also [27]. Formulations based on optimal control on simpler models have been investigated, e.g., in [55], [72], [66], [67], [103], [104].

As previously mentioned, simpler models than (10) can be adopted to describe the vessel deformation. Of special interest are models based on a single spatial coordinate, the one along the longitudinal axis, which usually describes the radial deformation of the vessel wall. These models are based on the following further simplifying assumptions.

Small thickness and plain stresses. The vessel wall thickness h is sufficiently small to allow a shell-type representation of the vessel geometry. In addition, we will also suppose that it is constant in the reference configuration. The vessel structure is subjected to plain stresses.

Cylindrical reference geometry and radial displacements. The reference vessel configuration is described by a circular cylindrical surface with straight axes. Indeed, this assumption may be partially dispensed with, by assuming that the reference configuration is "close" to that of a circular cylinder. The model here derived may be supposed valid also in this situation. The displacements are only in the radial direction.

Small deformation gradients. We assume that the deformation gradients are small, so that the structure basically behaves like a linear elastic solid and $\frac{\partial R}{\partial \theta}$ and $\frac{\partial R}{\partial z}$ remain uniformly bounded during the motion.

Incompressibility. The vessel wall tissue is incompressible, i.e. it maintains its volume during the motion. This is a reasonable assumption since biological tissues are indeed nearly incompressible.

Under the above assumptions we can derive the following one dimensional model that describes the radial displacement $\boldsymbol{\eta} = \eta \boldsymbol{e}_r$ of the arterial wall (see [75]):

$$\rho^s \frac{\partial^2 \eta}{\partial t^2} - a \frac{\partial^2 \eta}{\partial z^2} + b\eta - c \frac{\partial^3 \eta}{\partial t \partial z^2} = g, \quad 0 < z < L, \ t > 0, \tag{13}$$

where z denotes the longitudinal space coordinate (aligned along the vessel axis), L the length of the vessel at rest, while a, b and c are suitable coefficients which depend on material properties. Precisely:

$$a = \frac{\sigma_z}{h}, \quad b = \frac{E}{(1 - \varsigma^2) R_0^2},$$

while c is a positive coefficient that accounts for viscoelastic effects, R_0 is the radius of the cylindrical vessel at rest and h is the thickness of the vessel wall at rest, ς is the Poisson ratio, E is the Young modulus, while σ_z is the magnitude of the longitudinal stress.

The first term in (13) models the inertia, the second one the shear, the third one the elasticity, the fourth one the viscoelastic damping. Finally, g accounts for the forcing terms.

When the one-dimensional wall model (13) is used instead of (10), the coupled fluid-structure model is made of equations (7)–(9), plus the equilibrium equation (13) where the source term g is the projection along the radial direction of the normal stress of the fluid on the right hand side of (12), that is $g = J^f \boldsymbol{T}^f \cdot (\boldsymbol{F}^f)^{-T} \cdot \hat{\boldsymbol{n}}^s \cdot \boldsymbol{e}_r$; the equation (11) now reads $\boldsymbol{u} \circ A^f = \dot{\eta} \boldsymbol{e}_r$ on $\hat{\Gamma}$.

When supplemented by suitable boundary and initial conditions, this coupled system satisfies an a priori estimate stating that the kinematic energy of the fluid plus the elastic energy of the 1D vessel is controlled by the initial data and the source term (see [75]). A result of existence of strong solutions in the case of periodic conditions in space is given in [5].

The numerical solution of a coupled fluid-structure nonlinear problem like (7)–(12) (or that discussed above based on the one dimensional model (13) for the radial vessel deformation) poses many challenges. After space discretization (e.g. by the finite element method, see [77]) one obtains a coupled nonlinear algebraic system.

Since the density of the structure is comparable to that of the fluid, the stability of numerical simulations of fluid-structure interactions relies heavily on the accuracy in solving the nonlinear coupled problem at each time step [23], [59], [60], [70], [88].

Ideally, implicit schemes should be used as they would guarantee energy conservation (up to the dissipation terms) and therefore numerical stability. This is outlined on a simplified fluid-structure interaction problem in [13], where implicit and staggered algorithms are analyzed by taking into account the so-called added-mass effect. In particular it is shown that numerical instabilities may occur when using loosely coupled time-advancing schemes. To account for the nonlinear coupling between fluid and structure, common strategies rely on fixed point methods [14]. Several ad-hoc variants have been proposed, including steepest descent algorithms in [88], Aitken-like acceleration formulas [63], [64], and transpiration boundary conditions [23] to avoid the computation of the fluid matrices at each sub-iteration. Yet, in general, these methods are slow, and in some cases may even fail to converge [70], [13], [25]. A more radical approach consists of using Newton based methods, owing to their potentially faster convergence [25], [29], [46], [61]. However, since they demand the evaluation of the Jacobian associated to the fluid-solid coupled state equations, a critical step is the evaluation of the *cross* Jacobian [93], which expresses the sensitivity of the fluid state to solid motions. This evaluation can be made inexactly, either by resorting to finite difference approximation of derivatives (see, e.g., [93]), or by barely replacing the tangent operator of the coupled system with a simpler one [42], [43]. However, either approximation may seriously compromise the convergence rate. Acceleration techniques using Krylov spaces have been proposed in [26], [46], [62]. A Newton method with exact Jacobian has been investigated both mathematically and numerically in [29].

Methods based on a fractional-step solution of the coupled system are proposed in [30]. In this case, the coupling conditions (11) and (12) are not exactly enforced. The diffusion term of the momentum equations are advanced first from the time step t^n to $t^{n+1} = t^n + \delta t$ ($\delta t > 0$ being the time-step), and the normal component of the continuity equation (11) is imposed; then the equation for the solid structure (10) is coupled with the projection step of the Navier–Stokes equations, and the stress continuity equation (12) is enforced.

Another strategy is mutuated from domain decomposition techniques (see [78]) and is proposed in [24]. The global coupled problem (7)–(12) is reduced to a (generally nonlinear) interface equation, the so-called pseudo-differential *Steklov–Poincaré* equation, where the only unknown is the displacement of the interface separating the fluid and the structure. At any time-step, after space discretization, the aim is to exploit the physically decoupled structure of the original problem, in such a way that the solution is obtained through a sequence of independent solves involving each subproblem separately.

A preliminary approach in this direction can be found in [88], [65], where the coupling between Stokes equations and a linearized shell model is considered. The analysis of the Steklov–Poincaré operators associated to the fluid and shell models is developed, and a Richardson scheme in which the shell operator acts as preconditioner is proposed and tested. Another instance is presented by Mok and Wall [63], who proposed an iterative substructuring method requiring, at each step, the independent

solution of a fluid and a structure subproblem, supplemented with suitable Dirichlet or Neumann boundary conditions on the interface.

As it was observed, one of the advantages of the Steklov–Poincaré approach is that the whole problem is reduced to an equation involving only interface variables. In this respect, it can be regarded as a special instance of *heterogeneous domain decomposition*, arising whenever in the approximation of certain physical phenomena two (or more) different kinds of boundary value problems hold within two disjoint subregions of the computational domain (see, e.g., [78]). The key to efficiency is to set up convenient preconditioners for the discretized Steklov–Poincaré equation, as done in [24]. In Figure 10 we plot the numerical simulation of the wall deformation of a straight cylindrical vessel at two different time-instants of the cardiac beat. The gray scales indicate pressure iso-values. In Figure 11 the same kind of simulation is reported for a carotid artery. Arrows indicate the blood velocity field.

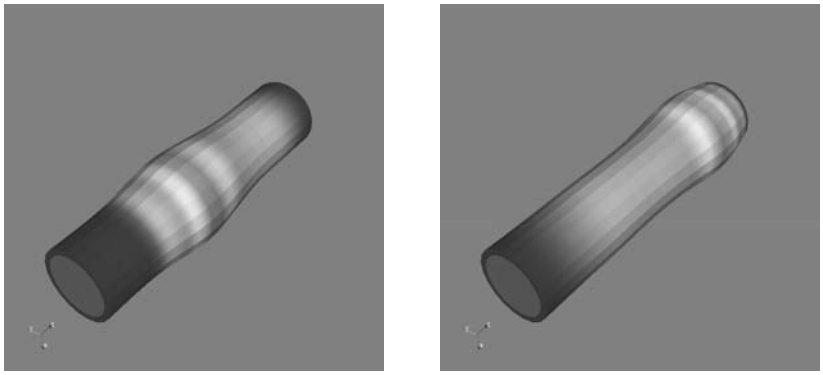


Figure 10. Pressure wave propagation in a straight vessel (simulation by G. Fourestey).

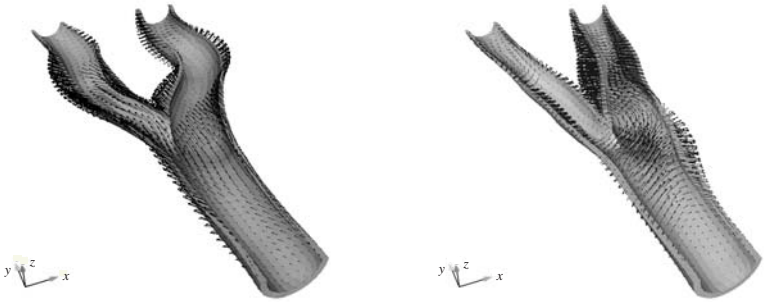


Figure 11. (From [24]). Structure deformation of a carotid artery and velocity at time $t = 10\,\text{ms}$ (left) and $t = 20\,\text{ms}$ (right).

4. Modeling the whole circulatory system

So far we have shown how to set-up mathematical models to simulate local phenomena. In fact, a change of perspective is necessary if we want to investigate processes that occur on the vascular tree at large: instances include the propagation of the pressure pulse from heart to periphery, the self-regulation process that governs the dynamics of blood solutes (oxygen, drugs, etc.), the aging effects on the arterial elasticity, the overload on the heart induced by the implant of an endovascular prosthesis, the regulating processes that the body activates to contrast severe changes in external conditions, etc.

Modeling these processes requires to integrate multiple scales in space and time, and to account for the correlation between actions and reactions in different cardiovascular compartments.

The simulation of a large part of the circulatory system by solving the three-dimensional Navier–Stokes equations everywhere would require the availability of a large set of morphological data (quite difficult to obtain), not to mention the computational costs that would be out of reach. On the other hand, the richness of detail intrinsic to a 3D model may not be necessary when one is primarily interested in the simulation of global flow features. Rather, suitable hierarchies of reduced models, made of networks of 1D pipes and lumped parameter circuits carrying different level of detail, can be developed to provide sufficiently reliable answers to our questions.

By exploiting the fact that, at least locally, an artery is a quasi-cylindrical vessel and that blood flows mainly in the axial direction, we build a simplified model that neglects the transversal components of the velocity, assumes that the wall deforms along the radial direction only, and describes the fluid-structure interaction blood flow problem in terms of two scalar functions: the measure $A(z,t)$ of a generic axial section $\mathcal{A}(z)$ of the vessel and the mean flux $Q(z,t) = \int_{\mathcal{A}(z)} u_z d\sigma$. Here, z indicates the axial coordinate (see Figure 12, left). Under simplifying, yet realistic, hypotheses the following one dimensional (1D) model is obtained [75]:

$$\begin{aligned} &\frac{\partial A}{\partial t} + \frac{\partial Q}{\partial z} = 0, \\ &\frac{\partial Q}{\partial t} + \frac{\partial A}{\partial \rho}\frac{\partial p}{\partial A} - \alpha \bar{u}_z^2 \frac{\partial A}{\partial z} + 2\alpha \bar{u}_z \frac{\partial Q}{\partial z} + K_R\Big(\frac{Q}{A}\Big)Q = 0, \end{aligned} \qquad z \in (0, L),\ t > 0 \quad (14)$$

which describes the flow of a Newtonian fluid in a compliant straight cylindrical pipe of length L. Here, $\bar{u}_z = A^{-1}\int_{\mathcal{A}} u_z d\sigma$ is the mean axial velocity and $\alpha = (A\bar{u}^2)^{-1}\int_{\mathcal{A}} u_z^2 d\sigma$ is the *Coriolis* coefficient. The pressure is assumed to be function of A according to a constitutive law that specifies the mechanical behavior of the vascular tissue. Different models can be obtained by choosing different pressure-area laws. Finally, K_R is a parameter accounting for the viscosity of the fluid. For the analysis of the hyperbolic system (14) see [75] and [10].

In this simple (and most popular) one dimensional model the vessel mechanics is overly simplified. In practice, it is reduced to an algebraic relationship between the

mean axial pressure (more precisely the average intra-mural pressure) and the area of the lumen. However, one may also account for other mechanical properties such as viscoelasticity, longitudinal pre-stress, wall inertia. In the latter case, the relation between pressure and vessel area is governed by a differential equation. Yet, it is still possible, at a price of some simplifications, to recover again a system of two partial differential equations [35], [33]. By so doing, the wall inertia introduces an additional dispersive term, while viscoelasticity contributes with a dissipation term. The treatment of these additional terms is problematic as further boundary conditions would be required. However, for physiological situations inertia and viscoelastic effects are not very important. Further improvements account for tapering and curvature (the latter cannot be neglected in arterial vessels such as the coronaries, the aortic arch, etc.). The model becomes fairly more involved, an account is given, e.g., in [54], [84]. At some extent, the arterial system in its entirety can be regarded as a network

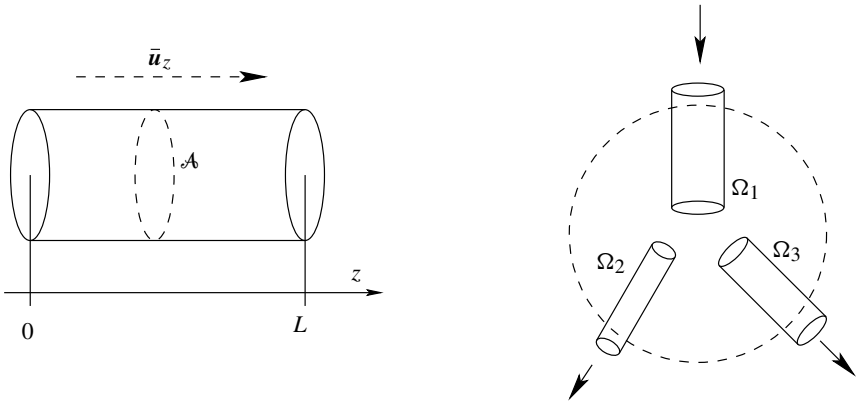


Figure 12. Left: Representation of an arterial cylindrical segment. Right: Sketch of a bifurcation

of 1D pipes, each of these being modeled by the hyperbolic system (14) (or its variants that account for curved vessels), supplemented by suitable matching conditions at the branching or bifurcation points (like in Figure 12, right) ensuring mass and energy conservation (see [75]). Its mathematical investigation would require the analysis of nonlinear hyperbolic systems on networks (see, e.g., [19], [53]).

The resulting network of one dimensional hyperbolic models are very well suited to describe the propagation of waves (the *pulse*), a phenomenon generated by the interaction between blood flow and compliant vessel wall and intrinsically related to the elastic properties of the arteries. In Figure 13 we report some snapshots of the numerical solution obtained by simulating with 1D models the application of a prosthesis at the abdominal bifurcation to cure an aneurysm. Figures on the top represents the case of an endo-prosthesis made with material softer that the vascular tissue. On the bottom the case where the prosthesis is stiffer. The presence of a strong back-reflection in the latter case is evident. When the reflected wave reaches the

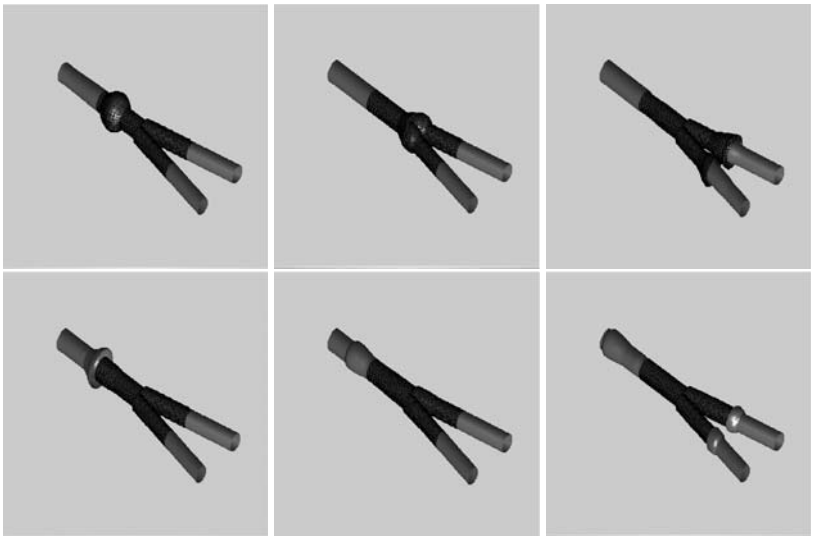


Figure 13. (from [36]). Snapshots of the simulation of a vascular bifurcation with a prosthesis, carried out with a 1D model. The three pictures in the top row illustrate the case of a prosthesis softer than the arterial wall. The most relevant reflection is at the distal interface between the prosthesis and the vessels (right). At he bottom row the results obtained using the same boundary data but with a prosthesis stiffer than the vascular wall. The most relevant reflection is at the proximal interface between the vessel and the prosthesis (left) and it back propagates up to the heart.

heart it may induce a pressure overload. These results may guide the design of better prostheses. A more complete 1D network, like the one including the largest 55 arteries shown in Figure 14, left, may be adopted for a more sound numerical investigation of the systemic dynamics.

Peripheral circulation in smaller arteries and capillaries may be accounted as well by *lumped parameter models*.

Here, a further simplification in the mathematical description of the circulation relies on the subdivision of the vascular system into *compartments*, according to criteria suited for the problem at hand. The blood flow as well as the other quantities of interest are described in each compartment by a set of parameters, typically the average flux and pressure in the compartment, depending only on time. The mathematical model is then made of a system of algebraic and ordinary differential equations in time that govern the dynamics of each compartment and their mutual coupling. Often, these models are called (with a little abuse of notation) 0D *models* ("zero" because there is no space variability any longer). In this way, large parts of the circulation system (if not all) can be modeled. The level of detail can be varied according to the problem needs.

A useful way of representing lumped parameter models of the circulation is based

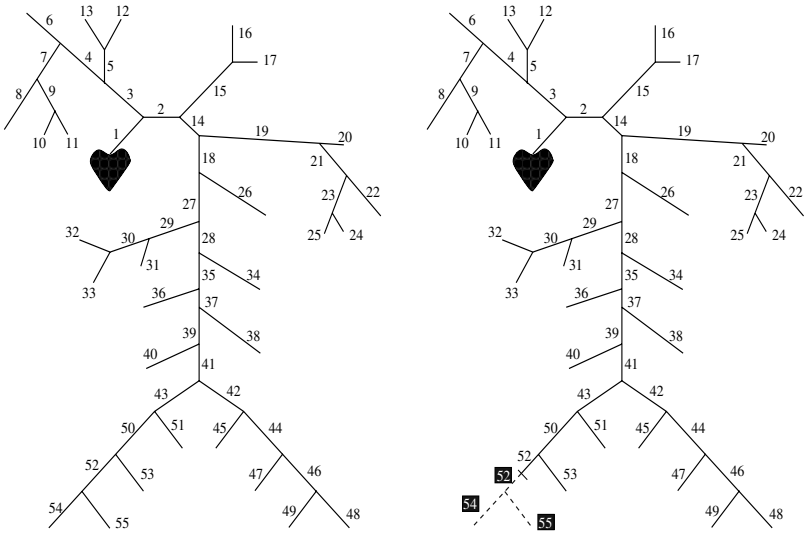


Figure 14. Arterial tree composed of a set of 55 straight vessels, described by 1D models (see [100]). On the right a pathological case, in which some of the vessels are supposed to be completely occluded.

on the analogy with electric networks, where the flow rate is represented by the electric current and pressure by the voltage. The equations coupling the different compartments are given by the *Kirchhoff balance laws*, which derive from the continuity of mass and pressure. The effects on blood dynamics due to the vascular compliance is here represented by means of capacitances. Similarly, inductances and resistances represent the inertial terms and the effect of blood viscosity, respectively (see e.g. [37] and references therein). Figure 15 illustrates different electrical schemes that may be used to describe blood flow in a passive compartment. Exploiting the same analogy, it is also possible to devise a lumped parameter representation of the heart. Since, as stated in [69], Chapter 13, left ventricle and arterial circulation represent two mechanical units that are joined together to form a coupled biological system, we need to couple the 1D model with a model of the heart (or at least of the left ventricle), for instance a lumped parameter model. The opening of the aortic valve is driven by the difference between the ventricular and the aortic pressure, P_v and P_a, while the closing is governed by the flux. The electric analog of each ventricle is given in Figure 16 where the presence of heart valves has been taken into account by *diodes* which allow the current flow in one direction only. A simple ordinary differential equation that accounts for this dynamics reads $\frac{d}{dt}(C(t)P_v(t)) = -M_Q(t)$, where Q represents the incoming flow rate, and M_Q is the action exerted by the contraction of the cardiac muscle. Precisely, $M_Q = \frac{dV_0}{dt}$, V_0 being the reference volume that changes in time because of the variation of the length of the muscle fibers. The action

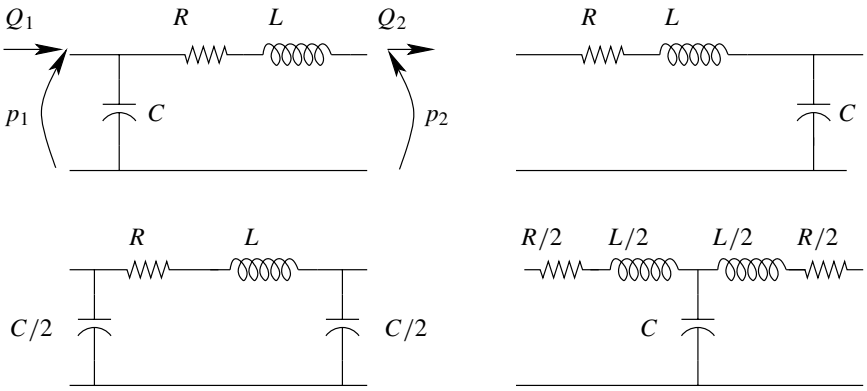


Figure 15. (From [36]). Four possible lumped parameters representation of a compliant vessel in terms of electrical circuits. The four cases differ for the state variables and the upstream/downstream data to be prescribed. The letters R, L, C indicate resistances, inductances and capacitances, respectively, while Q and p denote flow rate and pressure.

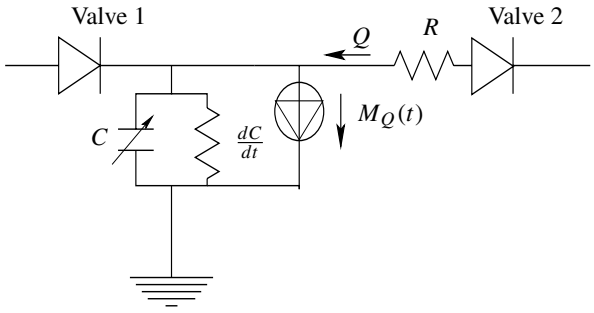


Figure 16. (From [36]). Network for the lumped parameter model of a ventricle.

of the aortic valve is described by setting $Q = 0$ when $P_a > P_v$, $P_a = P_v - RQ$ if $Q > 0$. For more details about this model, see [37]. More sophisticated ODE models are available, such as the visco-elasto-plastic model in [7].

From a mathematical standpoint, a general representation of lumped parameters models is a Differential-Algebraic-Equations (DAE) system in the form

$$\begin{aligned} &\frac{d\mathbf{y}}{dt} = B(\mathbf{y}, \mathbf{z}, t) \quad t \in (0, T] \\ &G(\mathbf{y}, \mathbf{z}) = 0 \end{aligned} \tag{15}$$

supplemented with the *initial condition* $\mathbf{y}|_{t=t_0} = \mathbf{y}_0$. Here, $\mathbf{y}$ is the vector of *state variables* while $\mathbf{z}$ are the other variables of the network which do not appear as time derivative, G is a set of algebraic equations that derive from Kirchhoff laws. If $\frac{\partial G}{\partial \mathbf{z}}$ is nonsingular, then by the implicit function theorem the DAE system (15) can be

formulated in terms of $\boldsymbol{y}$ solely. By coupling together schemes like those illustrated in Figure 15 for the different compartments and schemes like that in Figure 16 (or more sophisticated ones) to model the blood supply from heart it is possible to derive a lumped parameter model of the whole circulatory system. An example is provided by the four-compartment model illustrated in Figure 17, which comprises a lumped description of heart, lungs, arterial and venous circulation. Unfortunately, the param-

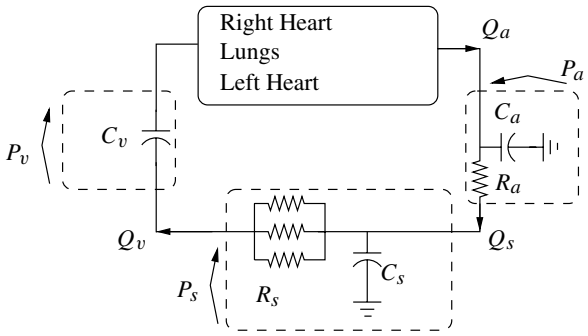


Figure 17. (From [36]). A four compartment description of the vascular system with self-regulating controls.

eters that govern the model, like resistances and compliances, can hardly be obtained from measurements or other means. In fact the circulatory system ensures a correct blood supply to organs and tissues in very diverse situations, at rest as well as after a long run. This is possible thanks to self regulating mechanisms. One of such mechanisms ensures that the arterial pressure is maintained within a physiological range (about 90–100 mmHg). Indeed, if pressure falls below this range, the oxygenation of the peripheral tissues would be seriously affected; on the other hand, a high arterial pressure would induce vascular diseases and heart overload. This regulation mechanism is called *baroreflex effect* and is described, for instance, in [49] and [52]. The elements of the feedback baroreceptor loop are a set of *baroreceptors* located in the carotid arteries and the aortic arch, which transmit impulses to the brain at a rate increasing with the arterial pressure, the *parasimpathetic nervous system*, which is excited by the activity of baroreceptors and can slow down the heart rate, and the *simpathetic nervous system*, which is inhibited by the baroreceptors and can increase the heart rate. It controls also the venous pressure and the systemic resistance.

Another ingredient of the self-regulating capabilities of the arterial system is the so called *chemoreflex effect*, a mechanism able to induce capillaries dilation and opening when an increment of oxygen supply is required by the organs, for instance during heavy exercise.

Chemoreflex and baroreflex effects can be included in the differential models presented so far through another coupled ODE system that models these feedback mechanisms (see, e.g., [21], [20] and the references therein).

Being able to adopt equations in different geometrical dimensions (3D, 1D and 0D, as we have illustrated thus far) provides tremendous new opportunities for modeling the circulatory system, but, at the same time, poses severe mathematical challenges. Multiscale geometrical systems can be set-up using 3D models of the type (7)–(12) to provide a complete description of the flow-field and 3D vessel deformation in specific districts (such as, e.g., the carotid bifurcation, the aortic arch, a stenosed coronary artery) combined with a network of 1D models like (14), one for every compliant vessel apt at providing average values of flow-rate and pressure on each vessel axial section. The rest of the system – the heart, the venous system, the capillary bed, the small circulation – may be accounted for by either prescribing appropriate "boundary" conditions at the terminal vessels or, more realistically, by adopting 0D lumped parameter (ODE) models capable of describing the feedback effects due to peripheral circulation. With this approach, difficulties arising from the treatment of boundary conditions for 3D model (mentioned in Section 2) are naturally handled.

From a mathematical standpoint, the use of such a geometrical multiscale model calls for the set up of matching conditions between the various submodels. These conditions should ensure the conservation of mass and stresses at the interfaces between heterogeneous submodels. This is not obvious to achieve, since the submodels live in spaces of different dimensions, are made of equations of different type and number, and feature different kind of unknown variables. Furthermore, the multiple geometrical models coupled with the continuity conditions at interfaces should hopefully define a globally well-posed mathematical problem.

The analysis of the complete system is very difficult, though. Partial results are available on the coupling of 3D and 0D models, and of 1D and 0D, see [33], [32], [81]. An account is given in [37].

So far, we have described the heart ventricle functionality by a simple 0D model. Clearly, this is an overly simplified approach. In fact, the development of a mathematical model for describing the electrical, mechanical and biochemical function of the heart and its coupling with the ventricular blood dynamics is tremendously challenging.

The changes in the electrical potential across the muscle cell outer membrane triggers the myocardium, whose contraction prompts ejection of blood from the ventricles. Electric current flows into a cell, raises the potential and initiates the wave propagation along the cells, which are connected by gap junction proteins. The entire myocardium is activated within 50 ms and the mechanical contraction lasts for about 300 ms.

From a numerical perspective, the difficulty is represented by the need of coupling efficiently large deformation mechanics, electrical excitation and wave propagation, turbulent flow fields, which feature different characteristic spatial and temporal scales. Moreover, the electric activity of the heart influences the activation function of 1D network models like the one in Figure 13 that could be used for the systemic circulation. Reciprocally, the pressure pulse that is modeled by 1D network interacts with the cardiac electrodynamics.

Tremendous progress has been made though in the past two decades. The *immersed boundary method* was introduced by Charles Peskin in his Ph.D thesis in 1972 in order to study the fluid dynamics of heart valves, and it was then extended to become a three-dimensional model of the whole heart (see [73] and the references therein). According to Peskin, "the philosophy of the immersed boundary method is to blur the distinction between fluid dynamics and elasticity". This is accomplished by inserting in the right hand side of the momentum equation (5) a forcing term $F(\boldsymbol{x}, t) = \int_{\hat{\Omega}^s} \boldsymbol{f}(\hat{\boldsymbol{x}}, t)\delta(\boldsymbol{x} - \boldsymbol{X}(\hat{\boldsymbol{x}}, t))d\hat{\boldsymbol{x}}$ representing the forces acting on the blood flow because of the presence of a solid structure (a valve, or the cardiac fibers). The vector $\boldsymbol{f}$ denotes the density distribution of forces (whose expression depends on the mathematical model adopted to describe the structural deformation), δ is a Dyrac function, $\boldsymbol{X}$ describes the motion of the solid structure (like L^s in Section 3), and is related to the fluid velocity $\boldsymbol{u}$ by the Lagrangian relation $\partial_t \boldsymbol{X}(\hat{\boldsymbol{x}}, t)) = \boldsymbol{u}(\boldsymbol{X}(\hat{\boldsymbol{x}}, t), t), \hat{\boldsymbol{x}} \in \hat{\Omega}^s, t > 0$. Both the Eulerian and the Lagrangian variables are employed.

The development of a global cardiac model using finite elements for finite deformation mechanics equations is proposed in [87]. An anatomically based description using finite element shape functions is given, then governing equations are proposed to relate material properties to tissue behavior.

Cardiac tissue is made of discrete cells but it can be modeled as a continuum. For instance, the *bidomain model* (see, e.g., [17], [16]) consists of two interpenetrating domains that represent cells (intracellular domain) and the space surrounding the cells (extracellular domain). These two domains are assumed to co-exist at all points in the computational domain. The tissue microstructure is accounted for in the activation model through the extra-and-intra-cellular conductivity tensors. From the mathematical viewpoint, this macroscopic representation of the cardiac tissue by a reaction-diffusion system of partial differential equations can be rigorously derived by a homogeneization procedure [2], [6].

The development of realistic models for heart functioning is however far from being achieved, due to the tremendous complexity of this physical system and the induced computational complexity of the associated numerical models.

5. Mathematical models for biochemical processes

Besides the biochemical and electrical processes described so far, mathematical models can be set up to describe the transport, diffusion and absorption of biomedical components (such as oxygen, nutrients, drugs, low density lipoproteins (LDL), etc.) in the blood stream and through the different layers of the arterial wall. Numerical simulation of biochemical processes can in fact explain biochemical modifications produced by alterations in blood flow field like those occurring at outer wall of bifurcations, inner wall of curved vessels, in anastomotic junctions (as in a coronary by-pass) and stenotic arteries.

The dynamics of solutes in arteries, like dissolved gases (such as O_2) or macromolecules (such as albumin or LDL) is indeed strongly affected by the blood flow dynamics. The local transfer of mass between blood and arterial walls is functional to the transport of nutrients to cells and the removal of metabolic wastes, yet it also affects the accumulation of potentially atherogenic molecules. For instance the accumulation in the intima of LDL occurs at zones of low and oscillating wall shear stress, which seem to be correlated with the tendency to intima thickening.

The basic step for the modeling of mass transfer is the set up of a mathematical model which describes the filtration of plasma and the transfer of chemicals from the lumen to the arterial wall. The blood flow into the arterial lumen is governed by the Navier–Stokes equations (2), (5), while the filtration across the tissue layers constituting the wall can be described by a Darcy type model,

$$\bar{\boldsymbol{u}} = -\frac{K_D}{\mu}\nabla P \quad \text{with } \operatorname{div}(\bar{\boldsymbol{u}}) = 0, \tag{16}$$

where $\bar{\boldsymbol{u}}$ is the volume-averaged velocity, P is the pressure, K_D is the (Darcy) wall permeability, μ is the dynamic viscosity. On the other side, the dynamics of chemicals is generally governed by a system of advection-diffusion equations. Precisely, applying the mass conservation principle on a generic control volume, we obtain the following equation

$$\partial_t \bar{c} + \operatorname{div}\left(-D\nabla\bar{c} + \gamma\bar{\boldsymbol{u}}\bar{c}/\varepsilon\right) = 0, \tag{17}$$

where $\bar{c}$ is the volume-averaged concentration, D is the diffusivity of the chemical species at hand, $0 \le \varepsilon \le 1$ is the porosity of the considered medium; the case $\varepsilon = 1$ represents the pure fluid phase. Collisions of large molecules with the structure of the porous tissue layer result in a reduced convective transport, a phenomenon that is accounted for by using the *hindrance coefficient* $0 < \gamma \le 1$.

In the simplest *wall-free model*, the fluid dynamics and the mass transport in the arterial lumen are described by the Navier–Stokes equations (2), (5) and the advection-diffusion equation (17). At the interface between the lumen and the arterial wall (the endothelium) appropriate conditions for the volume flux (J_v) and the mass flux (J_s) are assumed:

$$\boldsymbol{u}_l \cdot \boldsymbol{n}_l = J_v \ \text{ on } \Gamma, \quad (-D_l\nabla c_l + \boldsymbol{u}_l c_l)\cdot \boldsymbol{n}_l = J_s \ \text{ on } \Gamma.$$

In this case the values of J_v and J_s are provided by experimental data ([8], [99], [95], [91]). More realistic models are the *fluid-wall* model and the *multilayer* model, both requiring suitable matching conditions describing the flux of fluid (J_v) and the flux of chemicals (J_s) between two solutions (denoted by $i = 1, 2$) separated by a semi-permeable membrane across which concentrations and fluid pressure are different, see [51], [50]. In the case of just one solute, denoting with $\delta p = p_1 - p_2$ and $\delta c = c_1 - c_2$ the driving forces across the membrane, the interface equations originally proposed

by Kedem–Katchalsky read as follows,

$$J_v(P_1, P_2, c_1, c_2) = L_P(\delta P - \delta\pi) \quad \text{with } \delta\pi = \sigma RT\delta c, \tag{18}$$

$$J_s(c_1, c_2, P_1, P_2) = \Pi\delta c + sf(c_1, c_2)J_v, \tag{19}$$

where T is the absolute temperature, while s (the sieving coefficient), L_P (the hydraulic conductivity) and Π (the permeability), R (the gas constant) are phenomenological coefficients.

In their original theory Kedem and Katchalsky provide J_v and J_s in the case of two compartments filled with a free fluid. When taking into account two heterogeneous porous media (like two continuous wall layers) permeated by solutions of different concentrations and pressures, the driving forces are still δP and δc (where c in the case of porous media represents the concentration in the fluid phase), however the phenomenological coefficients now depend on the porosity of each medium and we will call them *effective coefficients*, denoted with $L_{P,\text{eff}}(\varepsilon_1, \varepsilon_2)$, $\Pi_{\text{eff}}(\varepsilon_1, \varepsilon_2)$, $s_{\text{eff}}(\varepsilon_1, \varepsilon_2)$ respectively. This theoretical characterization is a very challenging task, see e.g. [18], [89], [90], [22]. An approach that allows a *direct* estimation of the effective coefficients is proposed in [74].

To define the mathematical problems describing the mass transfer from the lumen to the arterial wall, we label with $i = 1$ the physical quantities associated with the free fluid and with $i = 2$ the ones corresponding to the porous medium, and denote by Γ the interface between these media. Then, the fluid dynamics is governed by eqs. (2), (5) in Ω_1, eq. (16) in Ω_2, and the following conditions at the interface:

$$\boldsymbol{u}_1 \cdot \boldsymbol{n}_1 = \bar{\boldsymbol{u}}_2 \cdot \boldsymbol{n}_1 \text{ and } \bar{\boldsymbol{u}}_2 \cdot \boldsymbol{n}_1 = J_v \quad \text{on } \Gamma. \tag{20}$$

Finally, we observe that in the free fluid (corresponding to a porosity $\varepsilon_1 = 1$) the velocity of the fluid phase is equivalent to the volume averaged one. Thanks to this identification the volume averaged velocity can be referred to as $\bar{\boldsymbol{u}}_i$ in both domains. The concentration $\bar{c}_i$ of a given chemical is governed by the following problem,

$$\begin{aligned}
&\partial_t \bar{c}_i + \operatorname{div}(-D_i\nabla\bar{c}_i + \gamma_i\bar{\boldsymbol{u}}_i\bar{c}_i/\varepsilon_i) + r_i\bar{c}_i = 0, && \text{in } \Omega_i,\ i = 1, 2,\\
&(-D_1\nabla\bar{c}_1 + \gamma_1\bar{\boldsymbol{u}}_1\bar{c}_1/\varepsilon_1)\cdot\boldsymbol{n}_1 \\
&\qquad = \Pi_{\text{eff}}(\bar{c}_1/\varepsilon_1 - \bar{c}_2/\varepsilon_2) + f(\bar{c}_1/\varepsilon_1, \bar{c}_2/\varepsilon_2)J_v && \text{on } \Gamma,\\
&(-D_2\nabla\bar{c}_2 + \gamma_2\boldsymbol{u}_2\bar{c}_2/\varepsilon_2)\cdot\boldsymbol{n}_2 \\
&\qquad = -[\Pi_{\text{eff}}(\bar{c}_1/\varepsilon_1 - \bar{c}_2/\varepsilon_2) + f(\bar{c}_1/\varepsilon_1, \bar{c}_2/\varepsilon_2)J_v] && \text{on } \Gamma,
\end{aligned} \tag{21}$$

where the Kedem–Katchalsky equation (19) has been rewritten in terms of the volume averaged concentration. Finally, we observe that the multilayer model is described by a set of equations similar to (20) and (21). Precisely, its fluid dynamics part is obtained by adding to problem (20) a further domain, describing the intima, that will be coupled to the lumen and the media prescribing that the normal velocity across

the interface between these domains is continuous and equal to the flux J_v, defined in (18). Analogously, the extension of equation (21) to the multilayer case features a third advection-diffusion equation defined in the intima and coupled to the rest of the system by imposing that the total flux of chemical (namely $(-D\nabla\bar{c} + \gamma\bar{\boldsymbol{u}}\bar{c}/\varepsilon)\cdot\boldsymbol{n}$) is continuous across the interfaces and equal to J_s, defined in (19).

Besides their interest for bio-medical applications, (20) and (21) represent a difficult system of nonlinear partial differential equations whose analysis has been specifically addressed in [105], [79], [80]. Irregularities in the flow field across the arterial wall influence the concentration distribution within the wall. Figure 18 displays the concentration contours in the wall of the two different wall models at selected locations in the expanding region of the stenosis. We observe that the perturbations in the velocity field in the intima and the media affect the concentrations as well. For example in the media, the concentration in the region of high filtration velocities is slightly higher than the average value, while it is lower than the average in correspondence of low filtration velocities. More analysis and numerical simulations can be found in [105], [74]. Systems like those introduced in this section can also be applied to

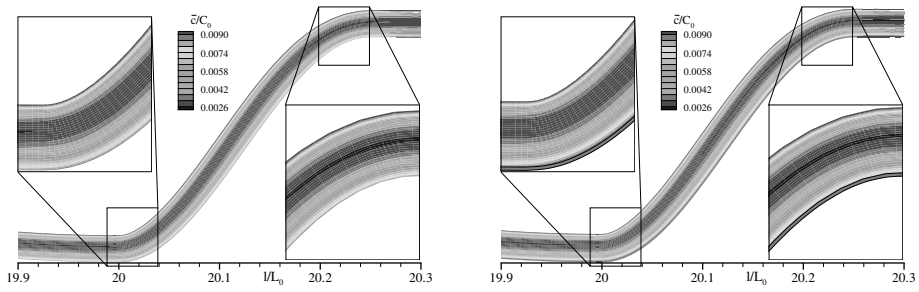


Figure 18. (From [74]). Concentration contours provided by the fluid-wall model (left) and the multilayer model (right). In the latter case, the presence of the intima is put into evidence.

the modeling of biochemical processes arising from the control of peritoneal dialysis [107], drug eluting materials [106], and artificial blood oxygenators [58].

References

[1] Agoshkov, V., Quarteroni, A., Rozza, G., Shape design in aorto-coronaric bypass anastomoses using perturbation theory. *SIAM J. Numer. Anal.* **44** (2006), 367–384.

[2] Ambrosio, L., Colli Franzone, P., Savaré, G., On the asymptotic behaviour of anisotropic energies arising in the cardiac bidomain model. *Interfaces Free Bound.* **2** (2000), 213–266.

[3] Aris, R., *Vectors, Tensors, and the Basic Equations of Fluid Mechanics*. Prentice Hall, Englewood Cliffs, NJ, 1992.

[4] Arada, N., Sequeira, A., Strong steady solutions for a generalized Oldroyd-B model with shear-dependent viscosity in a bounded domain. *Math. Mod. Meth. Appl. Sci.* **13** (9) (2003), 1303–1323.

[5] Beirão da Veiga, H., On the existence of strong solutions to a coupled fluid-structure evolution problem. *J. Math. Fluid Mechanics* **6** (2004), 21–52.

[6] Bellettini, G., Colli Franzone, P., Paolini, M., Convergence of front propagation for anisotropic bistable reaction-diffusion equations. *Asymp. Anal.* **15** (1997), 325–358.

[7] Bestel, J., Clément, F., Sorine, M., A Biomechanical Model of Muscle Contraction. *MICCAI* (2001), 1159–1161.

[8] Bratzler, R. L., Chisolm, G. M., Colton, C. K., Smith, K. A., Lees, R. S., The distribution of labeled low-density lipoproteins across the rabbit thoracic aorta in vivo. *Atherosclerosis* **28** (1977), 289–307.

[9] Campeau, L., Enjalbert, M., Lesperance, J., Vaislic, C., Grondin, C. M., Bourassa, M. G., Atheroslerosis an dlate closure of aortocpronary saphenous vein grafts; sequential angiographic studies at 2 weeks, 1 year, 5-7 year and 10-12 years after surgery. *Circulation* **68** (1983), 1–7.

[10] Canic, S., Kim, E. H., Mathematical analysis of the quasilinear effects in a hyperbolic model of blood flow through compliant axi-symmetric vessels. *Math. Models Methods Appl. Sci.* **26** (14) (2003), 1161–1186.

[11] Caro, C. G., Fitz-Gerald, J. M., Schroter, R. C., Atheroma and arterial wall shear stress. Observations, correlation and proposal of a shear dependent mass transfer mechanism for atherogenesis. *Proc. Roy. Soc. B* **177** (1971), 109–159.

[12] Caro, C. G., Pedley, T. J., Schroter, R. C., Seed, W. A., *The Mechanics of Circulation*. Oxford University Press, 1978.

[13] Causin, P., Gerbeau, J.-F., Nobile, F., Added-mass effect in the design of partitioned algorithms for fluid-structure problems. *Comput. Methods Appl. Mech. Engrg.* **194** (42–44) (2005), 4506–4527.

[14] Cervera, M., Codina, R., Galindo, M., On the computational efficiency and implementation of block-iterative algorithms for nonlinear coupled problems. *Engrg. Comput.* **13** (6) (1996), 4–30.

[15] Ciarlet, P.G., *Introduction to Linear Shell Theory*. Gauthiers-Villars, Paris 1998.

[16] Colli Franzone, P., Pavarino, L., A parallel solver for reaction diffusion systems in computational electro-cardiology. *Math. Models Methods Appl. Sci.* **14** (6) (2004), 883–912.

[17] Colli Franzone, P., Pavarino, L., Taccardi, B., Simulating patterns of excitation, repolarization and action potential duration with cardiac Bidomain and Monodomain models. *Math. Biosci.* **197** (2005), 35–66.

[18] Curry, F. R. E., Mechanics and thermodynamics of transcapillary exchange. In *Handbook of Physiology*, ed. by E. M. Renkin, American Physiological Society, 1984.

[19] Dáger, R., Zuazua, E., Controllability of tree-shaped networks of vibrating strings. *C. R. Acad. Sci. Paris* **332** (12) (2001), 1087–1092.

[20] D'Angelo, C., Papelier, Y., Mathematical modelling of the cardiovascular system and skeletal muscle interaction during exercice. In *CEMRACS 2004—mathematics and applications to biology and medicine* (ed. by Eric Cancès and J-F. Gerbeau), ESAIM Proceedings 14, EDP Sciences, Les Ulis, 2005 72–88.

[21] D'Angelo, C., Milisic, V., Reduced model for coupling of axisymmetric Navier-Stokes equations with a reaction-diffusion model for concentration. EPFL-IACS report 02.2006, submitted.

[22] Deen, W. M., Hindered transport of large molecules in liquid-filled pores. *AIChE Journal* **33** (9) (1987), 1409–1425.

[23] Deparis, S., Fernandez, M., Formaggia, L., Acceleration of a fixed point algorithm for fluid-structure interaction using transpiration conditions. *Math. Model. Numer. Anal.* **37** (4) (2003), 601–616.

[24] Deparis, S., Discacciati, M., Fourestey, G., Quarteroni, A., Fluid-structure algorithms based on Steklov-Poincaré operators. *Comput. Methods Appl. Mech. Engrg.* **195** (2006), 5797–5812.

[25] Deparis, S., Numerical Analysis of Axisymmetric Flows and Methods for Fluid-Structure Interaction Arising in Blood Flow Simulation. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2004.

[26] Deparis, S., Gerbeau, J.-F., Vasseur, X., A dynamic preconditioner for Newton-Krylov algorithm. Application to fluid structure interaction. *INRIA, Rapport de Recherche*, No. 5277, 2004.

[27] Desjardins, B., Esteban, M. J., Existence of a weak solutions for a model of fluid-rigid structure interaction. *Arch. Ration. Mech. Anal.* **146** (1999), 59–71.

[28] Deuflhard, P., Hochmuth, R., Multiscale Analysis of Thermoregulation in the Human Microvascular System. *Math. Methods Appl. Sci.* **27** (2004), 971–989.

[29] Fernandez, M., Moubachir, M., A Newton method using exact jacobians for solving fluid-structure coupling. *Computers & Structures* **83** (2–3) (2005), 127–142.

[30] Fernandez, M., Gerbeau, J.-F., Grandmont, C., A projection semin-implicit scheme for the coupling of an eleastic structure with an incompressible fluid. *INRIA, Rapport de Recherche*, No. 5700, 2005.

[31] Fitzgibbon, G. M., Kafka, H. P., Keon, W. J., Coronary bypass fate: long-term angiographic study. *J. Amer. Coll. Cardiol.* **17** (5) (1991), 1557–1565.

[32] Formaggia, L., Gerbeau, J.-F., Nobile, F., Quarteroni, A., On the Coupling of 3D and 1D Navier-Stokes equations for Flow Problems in Compliant Vessels. *Comput. Methods Appl. Mech. Engrg.* **191** (2001), 561–582.

[33] Formaggia, L., Nobile, F., Quarteroni, A., Veneziani, A., Multiscale Modelling of the Circulatory System: a Preliminary Analysis. *Comput. Vis. Sci.* **2** (1–2) (1999), 75–83.

[34] Formaggia, L., Gerbeau, J.-F., Nobile, F., Quarteroni, A., Numerical treatment of defective boundary conditions for the Navier-Stokes equations. *SIAM J. Numer. Anal.* **40** (1) (2002), 376–401.

[35] Formaggia, L., Lamponi, D., Quarteroni, A., One dimensional models for blood flow in arteries. *J. Engrg. Math.* **47** (2003), 251–276.

[36] Formaggia, L., Quarteroni, A., Veneziani, A., The circulatory system: from case studies to mathematical modeling. In *Complex Systems in Biomedicine* (ed. by A. Quarteroni, L. Formaggia, A. Veneziani), Springer Italia, Milano 2006, 243–287.

[37] Formaggia, L., Veneziani, A., *Reduced and Multiscale Models for the Human Cardiovascular System*. Von Karman Institute Lecture Notes, Seventh Lecture Series on Biological Fluid Dynamics, 2003.

[38] Fung, Y. C., *Biomechanics: Mechanical Properties of Living Tissues*. Springer-Verlag, New York 1993.

[39] Fung, Y. C., *Biodynamics: Circulation*. Springer-Verlag, New York 1997.

[40] Galdi, G. P., Sequeira, A., Further Existence Results for Classical Solutions of the Equation of a Second Grade Fluid. *Arch. Ration. Mech. Anal.* **128** (1994), 297–312.

[41] Galdi, G. P., Rajagopal, K. R., Slow motion of a body in a fluid of second grade. *Internat. J. Engrg. Sci.* **35** (1997), 33–54.

[42] Gerbeau, J.-F., Vidrascu, M., Frey, P., Fluid-structure interaction in blood flows on geometries coming from medical imaging. *Computers & Structures* **83** (2005), 155–165.

[43] Gerbeau, J.-F, Vidrascu, M., A quasi-Newton algorithm based on a reduced model for fluid-structure interaction problems in blood flows. *Math. Model. Numer. Anal.* **37** (4) (2003), 663–680.

[44] Grandmont, C., Existence for a three-dimensional steady state fluid-structure interaction problem. *J. Math. Fluid Mech.* **4** (1) (2002), 669–694.

[45] Grandmont, C., Maday, Y., Existence for an unsteady fluid-structure interaction problem. *Math. Model. Numer. Anal.* **34** (3) (2000), 609–636.

[46] Heil, M., An efficient solver for the fully coupled solution of large displacement fluid-structure interaction problems. *Comput. Methods Appl. Mech. Engrg.* **193** (1–2) (2004), 1–23.

[47] Hochmuth, R., Deuflhard, P., Multiscale Analysis for the Bio-Heat-Transfer Equation — The Nonisolated Case. *Math. Models Methods Appl. Sci.* **14** (11) (2004), 1621–1634.

[48] Holzapfel, G. A., Gasser, T. C., Ogden, R. W., A new constitutive framework for arterial wall mechanics and a comparative study of material models. *J. Elasticity* **61** (2000), 1–48.

[49] Hoppensteadt, F., Peskin, C., *Modeling and Simulation in Medicine and the Life Sciences*. Second edition, Texts Appl. Math. 10, Springer-Verlag, New York 2002.

[50] Katchalsky, A., Curran, P. F., *Nonequilibrium Thermodynamics in Biophysics.* Harvard University Press, 1981,

[51] Kedem, O., Katchalsky, A., Thermodynamic analysis of the permeability of biological membranes to non-electrolytes. *Biochimica et Biophysica Acta* (1958), 229–246.

[52] Keener, J., Sneyd, J., *Mathematical Physiology*. Springer-Verlag, New York 1998.

[53] Lagnese, J., Leugering, G., Schmidt, E. J. P. G., *Modeling, analysis and control of dynamic elastic multi-link structures.* Systems Control Found. Appl., Birkhäuser, Boston, MA, 1994.

[54] Lamponi, D., One dimensional and Multiscale Models for Blood Flow Circulation. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2004.

[55] Lions, J. L., Zuazua, E., Approximate controllability of a hydroelastic coupled system. *ESAIM Control Optim. Calc. Var.* **1** (1995), 1–15.

[56] Lowe, D. O., *Clinical Blood Rheology*. Vol. I, II, CRC Press, Boca Raton, Florida, 1988.

[57] Luo, X. Y., Kuang, Z. B., A study of the constitutive equation of blood. *J. Biomech.* **25** (1992), 929–934.

[58] Mallabiabarrena, I., Experimental set-up and numerical simulations of intravenous gas transfer devices. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2003.

[59] Matthies, H., Steindorf, J., Partitioned but strongly coupled iteration schemes for nonlinear fluid-structure interaction. *Computers & Structures* **80** (2002), 1991–1999.

[60] Matthies, H., Steindorf, J., Partitioned strong coupling algorithms for fluid-structure interaction. *Computers & Structures* **81** (2003), 805–812.

[61] Matthies, H., Steindorf, J., Numerical efficiency of different partitioned methods for fluid-structure interaction. *Z. Angew. Math. Mech.* **2** (80) (2000), 557–558.

[62] Michler, C., Van Brummelen, E. H., De Borst, R., An interface Newton-Krylov solver for fluid-structure interaction. *Int. J. Numer. Methods Fluids* **47** (10-11) (2005), 1189–1195.

[63] Mok, D. P., Wall, W. A., Partitioned analysis schemes for the transient interaction of incompressible flows and nonlinear flexible structures. In *Trends in computational structural mechanics* (ed. by K. Schweizerhof, W. Wall, K. Bletzinger), International Center for Numerical Methods in Engineering (CIMNE), Barcelona 2001.

[64] Mok, D. P., Wall, W. A., Ramm, E., Accelerated iterative substructuring schemes for instationary fluid-structure interaction. In *Computational Fluid and Solid Mechanics* (ed. by K. Bathe), Elsevier, Amsterdam 2001, 1325–1328.

[65] Mouro, J., Interactions Fluide Structure en Grands Déplacements. Resolution Numerique et Application aux Composants Hydrauliques Automobiles. Ph.D. thesis, École Polytechnique, Paris 1996.

[66] Murea, C. M., Vazquez, C., Sensitivity and approximation of coupled fluid-structure equations by virtual control method. *Appl. Math. Optim.* **52** (2) (2005), 357–371.

[67] Murea, C. M., Optimal control approach for the fluid-structure interaction problems. In *Elliptic and parabolic problems* (ed. by J. Bemelmans et al.), World Scientific Publishing Co., River Edge, NJ, 2002, 442–450.

[68] Nazarov, S., Sequeira, A., Videman, J. H., Steady flows of Jeffrey-Hamel type from the half-plane into an infinite channel. Linearization on an anti-symmetric solution. *J. Math. Pures Appl.* **80** (12) (2001), 1069–1098.

[69] Nichols, W. W., O'Rourke, M. F., *Mc Donald's Blood Flow in Arteries*. Third edition, Edward Arnold Ltd., London 1990.

[70] Nobile, F., Numerical Approximation of Fluid-Structure Interaction Problems with Application to Haemodynamics. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2001.

[71] Novotny, A., Sequeira, A., Videman, J. H., Steady motions of viscoelastic fluids in 3-D exterior domains – existence, uniqueness and asymptotic behaviour. *Arch. Ration. Mech. Anal.* **149** (1999), 49–67.

[72] Osses, A., Puel, J. P., Approximate controllability for a linear model of fluid structure interaction. *ESAIM Control Optim. Calc. Var.* **4** (1999), 497–513.

[73] Peskin, C., The immersed boundary method. *Acta Numerica* **11** (2002), 479–517.

[74] Prosi, M., Zunino, P., Perktold, K., Quarteroni, A., Mathematical and numerical models for transfer of low density lipoproteins through the arterial walls: a new methodology for the model set up with applications to the study of disturbed lumenal flow. *J. Biomech.* **38** (2005), 903–917.

[75] Quarteroni, A., Formaggia, L., Mathematical Modelling and Numerical Simulation of the Cardiovascular System. In *Modelling of Living Systems* (ed. by P. G. Ciarlet and J. L. Lions), Handbook of Numerical Analysis Series 12, Elsevier, Amsterdam 2004, 3–127.

[76] Quarteroni, A., Rozza, G., Optimal control and shape optimization in aorto-coronaric bypass anastomoses. *Math. Models Methods Appl. Sci.* **13** (12) (2003), 1801–1823.

[77] Quarteroni, A., Valli, A., *Numerical Approximation of Partial Differential Equations*. Springer Ser. Comput. Math. 23, Springer-Verlag, Berlin 1994.

[78] Quarteroni, A., Valli, A., *Domain Decomposition Methods for Partial Differential Equations*. Oxford University Press, New York 1999.

[79] Quarteroni, A., Veneziani, A., Zunino, P., Mathematical and numerical modelling of solute dynamics in blood flow and arterial walls. *SIAM J. Numer. Anal.* **39** (5) (2002), 1488–1511.

[80] Quarteroni, A., Veneziani, A., Zunino, P., A Domain Decomposition Method for Advection-Diffusion Processes with Application to Blood Solutes. *SIAM J. Sci. Comput.* **23** (6) (2002), 1959–1980.

[81] Quarteroni, A., Veneziani, A., Analysis of a geometrical multiscale model based on the coupling of ODEs and PDEs for blood flow simulations. *SIAM Mult. Models Sim.* **1** (2) (2003), 173–195.

[82] Raback, P., Ruokolainen, J., Lyly, M., Järvinen. Fluid-structure interaction boundary conditions by artificial compressibility. In ECCOMAS *Computational Fluid Dynamics Conference*, Swansea, 2001.

[83] Rajagopal, K. R., Bhatnagar, R. K., Flow of an Oldroyd-B fluid due to a stretching sheet in the presence of a free stream velocity. *Internat. J. Non-Linear Mech.* **30** (3) (1995), 391–405.

[84] Robertson, A. M., Sequeira, A., A director theory approach for modeling blood flow in te arterial system: an alternative to classical 1d models. *Math. Models Methods Appl. Sci.* **15** (6) (2005), 871–906.

[85] Rozza, G., Shape Design by Optimal Flow Control and Reduced Basis Techniques: Applications to Bypass Configurations in Haemodynamics. Ph.D. thesis, École Polytéchnique Fédérale de Lausanne, 2005.

[86] Serrin, J., Mathematical principles of classical fluid mechanics. In *Handbuch der Physik* (ed. by S. Flügge and C. Truesdell), Vol. VIII/1, Springer-Verlag, Berlin 1959, 125–263.

[87] Smith, N. P., Nickerson, D. P., Crampin, E. J., Hunter, P. J., Multiscale computational modelling of the heart. *Acta Numer.* **13** (2004), 371–431.

[88] Tallec, P. L., Mouro, J., Fluid structure interaction with large structural displacements. *Comput. Methods Appl. Mech. Engrg.* **190** (2001), 3039–3067.

[89] Jo, H., Dull, R. O., Hollis, T. M., Tarbell, J. M., Endothelial albumin permeability is shear dependent, time dependent and reversible. *Amer. J. Physiol.* **260** (1991), H1992–H1996.

[90] Wang D. M., Tarbell, J. M., Modelling interstitial flow through arterial media. *ASME J. Biomech. Eng.* **117** (1995), 358–363.

[91] Tarbell, J. M., Lever, M. J., Caro, C. G., The effect of varying albumin concentration and hydrostatic pressure on hydraulic conductivity of the Rabbit common carotid artery. *Microvasc. Res.* **35** (1988), 204–220.

[92] Taylor, C. A., Draney, M. T., Ku, J. P., Parker, D., Steele, B. N., Wang, K., Zarins, C. K., Predictive medicine: Computational techniques in therapeutic decision-making. *Computer Aided Surgery* **4** (5) (1999), 231–247.

[93] Tezduyar, T., Finite element methods for fluid dynamics with moving boundaries and interfaces. *Arch. Comput. Methods Engrg.* **8** (2001), 83–130.

[94] Thurston, G. B., Viscoelstic properties of blood and blood analogs. *Avances in Hemodynamics and hemorheology* **1** (1996), 1–30.

[95] Truskey, G. A., Roberts, W. L., Herrmann, R. A., Malinauskas, R. A., Measurement of endothelial permeability to I-low density lipoproteins in rabbit arteries by use of en face preparations. *Circ. Res.* **7** (4) (1992), 883–897.

[96] Varty, K., Allen, K. E., Bell, P. R. F., London, N. J. M., Infra-inguinal vein graft stenosis. *Br. J. Surg.* **80** (1993), 825–833.

[97] Veneziani, A., Vergara, C., Flow rate defective boundary conditions in haemodynamics simulations. *Int. J. Numer. Methods Fluids* **47** (2005), 803–816.

[98] Veneziani, A., Vergara, C., An approximate method for solving incompressible Navier–Stokes problems with flow rate conditions. *MOX report* **70**, Department of Mathematics, Politecnico di Milano, 2005.

[99] Wada, S., Karino, T., Computational study on LDL transfer from flowing blood to arterial walls. In *Clinical Application of Computational Mechanics to the Cardiovascular System* (ed. by T. Yamaguchi), Springer-Verlag, 2000.

[100] Wang, J. J., Parker, K. H., Wave propagation in a model of the arterial circulation. *J. Biomech.* **37** (2004), 457–470.

[101] Womersley J. R., Method for the calculation of velocity, rate of flow and viscous drag in arteries when the pressure gradient is known. *J. Physiol.* **127** (1955), 553–563.

[102] Yeleswarapu, K. K, Evaluation of Continuum Models for Characterizing the Constitutive Behavior of Blood. Ph.D. thesis, Department of Mechanical Engineering, University of Pittsburgh, 1996.

[103] Zhang, X., Zuazua, E., Polynomial decay and control of a 1-d hyperbolic-parabolic coupled system. *J. Differential Equations* **204** (2) (2004), 380–438.

[104] Zhang, X., Zuazua, E., Long time behavior of a coupled heat-wave system arising in fluid-structure interaction. *Arch. Ration. Mech. Anal.* **184** (2007), 49–120.

[105] Zunino, P., Mathematical and numerical modeling of mass transfer in the vascular system. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2002.

[106] Zunino, P., Multidimensional pharmacokinetic models applied to the design of drug eluting stents. *Cardiov Eng.* **4** (2) (2004), 181–191.

[107] Zunino, P., Mastalli, D., Quarteroni, A., VanBiesen, W., Vecten, D., Pacitti, A., Lameire, N., Neftel, F., Wauters, J. P., Development of a new mathematical approach to optimize peritoneal dialysis. EPFL-IACS report 03.2006.

Modelling and Scientific Computing (CMCS), Institute of Analysis and Scientific Computing (IACS), EPFL, École Polytechnique Fédérale de Lausanne, 1015, Lausanne, Switzerland

and

Dipartimento di Matematica "Francesco Brioschi", MOX, Modellistica e Calcolo Scientifico, Politecnico di Milano, 20133 Milano, Italy

E-mail: alfio.quarteroni@epfl.ch

Conformally invariant scaling limits: an overview and a collection of problems

Oded Schramm

Abstract. Many mathematical models of statistical physics in two dimensions are either known or conjectured to exhibit conformal invariance. Over the years, physicists proposed predictions of various exponents describing the behavior of these models. Only recently have some of these predictions become accessible to mathematical proof. One of the new developments is the discovery of a one-parameter family of random curves called stochastic Loewner evolution or SLE. The SLE curves appear as limits of interfaces or paths occurring in a variety of statistical physics models as the mesh of the grid on which the model is defined tends to zero.

The main purpose of this article is to list a collection of open problems. Some of the open problems indicate aspects of the physics knowledge that have not yet been understood mathematically. Other problems are questions about the nature of the SLE curves themselves. Before we present the open problems, the definition of SLE will be motivated and explained, and a brief sketch of recent results will be presented.

Mathematics Subject Classification (2000). Primary 60K35; Secondary 82B20, 82B43, 30C35.

Keywords. Statistical physics, conformal invariance, stochastic Loewner evolutions, percolation.

1. Introduction

In the past several years, many predictions from physics regarding the large-scale behavior of random systems defined on a lattice in two dimensions have become accessible to mathematical study and proof. Of central importance is the asymptotic conformal invariance of these systems. It turns out that paths associated with these random configurations often fall into a one-parameter family of conformally invariant random curves called stochastic Loewner evolutions, or SLE. We start by motivating SLE through a simple mathematical model of percolation. After giving the definition of SLE, we present a narrative of recent developments. However, since there are good surveys on the subject in the literature [94], [36], [21], [52], [95], this introductory part of the paper will be short and cursory. The rest of the paper will consist of an annotated list of open problems in the subject.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

1.1. Motivation and definition of SLE. To motivate SLE, we now discuss percolation. More specifically, we define one particular model of percolation in two dimensions. Fix a number $p \in [0, 1]$. Let ω be a random subset of the set of vertices in the triangular grid TG, where for vertices $v \in V(\mathrm{TG})$ the events $v \in \omega$ are independent and have probability p. In percolation theory one studies the connected components (a.k.a. clusters) of the random subgraph of TG whose vertex set is ω and whose edges are the edges in TG connecting two elements of ω. Equivalently, one may study the connected components of the set of white hexagons in Figure 1, where each hexagon in the hexagonal grid dual to TG represents a vertex of TG and hexagons corresponding to vertices in ω are colored white. The reasons for considering this dual representation are that the figures come out nicer and that it makes some important definitions more concise.

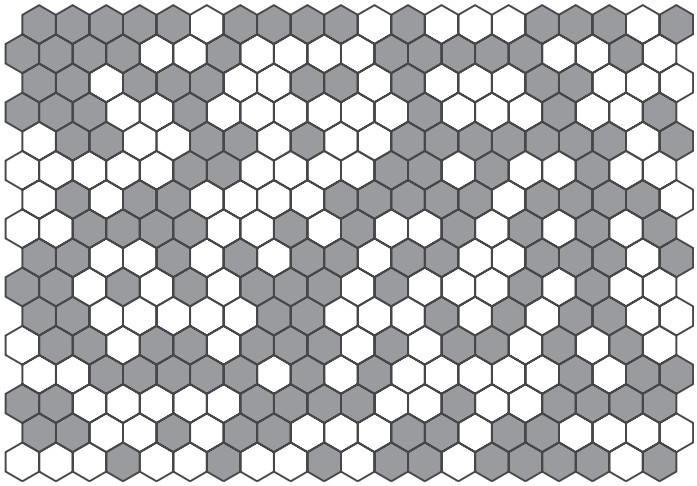


Figure 1. Site percolation on the triangular grid as represented by colored hexagons.

The above percolation model is site (or vertex) percolation on the triangular grid. Likewise, there is a bond (or edge) model, where one considers a random subgraph of a grid whose vertex set is the set of all vertices of the grid, but where each edge of the grid is in the percolation subgraph with probability p, independently. Additionally, there are various percolation models which are not based on a lattice. Some of these will be discussed in later sections.

There is an important value p_c of the parameter p, which is the threshold for the existence of an unbounded cluster and is called the critical value of p. The actual value of p_c varies depending on the particular percolation model. For site percolation on the triangular grid, as well as for bond percolation on the square grid, we have $p_c = 1/2$. This is a theorem of Kesten [43], based on earlier work by Harris [33], Russo [78] and Seymour and Welsh [84]. The underlying reason for this nice value of p_c is a duality which these two models have, though the precise form of the duality they exhibit is

different. For bond percolation on the triangular grid $p_c = 2\sin(\pi/18)$ [98], while for site percolation on the square grid there is not even a prediction for the value of p_c, though rigorous and experimental estimates exist. As p increases beyond p_c, the large scale behavior of percolation undergoes a rapid change. This is perhaps the mathematically simplest model of a phase transition. From now on, we will focus our attention on critical percolation, that is, percolation with $p = p_c$, which is in many ways the most interesting value of p.

We now define and discuss the percolation interface curve indicated in Figure 2. Consider a bounded domain D in the plane $\mathbb{R}^2 = \mathbb{C}$ whose boundary is a simple closed curve. Let $\partial_+ \subset \partial D$ be a proper arc on the boundary of D. Given $\varepsilon > 0$ we may consider the collection of hexagons in a hexagonal grid of mesh ε which intersect $\overline{D}$. Each of these hexagons which meets ∂_+ we color white, each of the hexagons which meet ∂D but not ∂_+ we color black, and each of the hexagons contained in D we color white or black with probability $1/2$, independently. In addition to white clusters (connected components of white hexagons) sometimes, black clusters are also considered. Percolation theory is the study of connected components of random sets, such as these clusters.

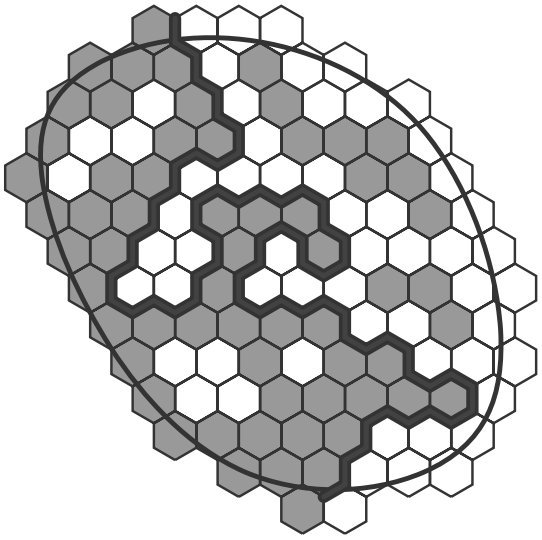


Figure 2. The interface associated with percolation.

For simplicity, we assume that ∂D is sufficiently smooth and ε is sufficiently small so that the union of hexagons intersecting ∂D but not ∂_+ is connected. There is a unique (random) path β, which is the common boundary of the white cluster meeting ∂_+ and the black cluster meeting ∂D.

The law $\mu_{D,\partial_+,\varepsilon}$ of β is a probability measure on the space of closed subsets of $\overline{D}$ with the Hausdorff metric. Smirnov [87] proved that as $\varepsilon \searrow 0$ the measure

$\mu_{D,\partial_+,\varepsilon}$ converges weakly to a measure μ_{D,∂_+}, and that μ is conformally invariant, in the following sense. If $f\colon \overline{D} \to \overline{D'} \subset \mathbb{R}^2$ is a homeomorphism that is analytic in D, then the push forward of μ_{D,∂_+} under f is $\mu_{f(D),f(\partial_+)}$. In other words, if ε is small, then $f(\beta)$ is a good approximation for the corresponding path defined using a hexagonal grid of mesh ε in $f(D) = D'$. This type of conformal invariance was believed to hold for many "critical" random systems in two dimensions. However, the only previous result establishing conformal invariance for a random scaling limit is Lévy's theorem [64] stating that for two-dimensional Brownian motion, the scaling limit of simple random walk on $\mathbb{Z}^2$, is conformally invariant up to a time-change.

Smirnov's proof is very beautiful, and the result is important, but describing the proof will throw us too far off course (since for this paper percolation is just an example model, not the primary topic). The interested reader is encouraged to consult [12], [30], [70], [45] for background in percolation and highlights of percolation theory. An elegant simplification of parts of Smirnov's proof has been discovered by Vincent Beffara [11]. A more detailed version of other parts of Smirnov's argument appears in [19].

Though this was not the original inspiration, we will now use Smirnov's result to motivate the definition of SLE. By conformal invariance, we may venture to understand β in the domain of our choice. The simplest situation turns out to be when $D = \mathbb{H}$ is the upper half plane and ∂_+ is the positive real ray $\mathbb{R}_+$, as in Figure 3.

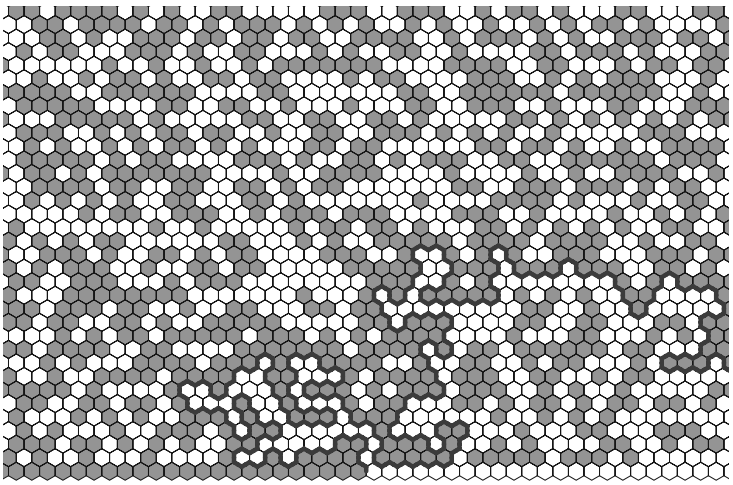


Figure 3. The percolation interface in the upper half plane.

(Though this domain D is unbounded, that does not cause any problems.) We may consider the discrete path β as a simple path $\beta\colon [0, T) \to \overline{\mathbb{H}}$ starting near 0 and satisfying $\lim_{t\to T} |\beta(t)| = \infty$ (where T is finite or infinite).

We would like to learn about β by understanding the one-parameter family of conformal maps g_t mapping $\mathbb{H} \setminus \beta([0, t])$ onto $\mathbb{H}$. To facilitate this, we must first

recall a few basic facts and discuss Loewner's theorem. At this point, assume only that β is a simple path in $\overline{\mathbb{H}}$ with $\beta(0) \in \mathbb{R}$ and $\beta(t) \notin \mathbb{R}$ for $t > 0$. The existence of the conformal maps $g_t : \mathbb{H} \setminus \beta([0,t]) \to \mathbb{H}$ is guaranteed by Riemann's mapping theorem. However, g_t is not unique. In order to choose a specific g_t for every t, we first require that $g_t(\infty) = \infty$. Schwarz reflection in the real axis implies that g_t is analytic in a neighborhood of ∞, and therefore admits a power series representation in $1/z$,

$$g_t(z) = a_1 z + a_0 + a_{-1} z^{-1} + a_{-2} z^{-2} + \cdots ,$$

valid for all z sufficiently large. Since g_t maps the real line near ∞ into the real line, it follows that $a_j \in \mathbb{R}$ for all j, and because $g_t : \mathbb{H} \setminus \beta([0,t]) \to \mathbb{H}$, we find that $a_1 > 0$. We now pick a specific g_t by imposing the so-called hydrodynamic normalization at ∞, namely $a_1 = 1$ and $a_0 = 0$. This can clearly be achieved by post-composing with a map of the form $z \mapsto a z + b$, $a > 0$, $b \in \mathbb{R}$.

The coefficients a_j of the series expansion of g_t are now functions of t. It is not hard to verify that $a_{-1}(t)$ is a continuous, strictly increasing function of t. Clearly, $g_0(z) = z$ and hence $a_{-1}(0) = 0$. We may therefore reparametrize β so as to have $a_{-1}(t) = 2t$ for all $t > 0$. This is called the half-plane capacity parametrization of β. With this parametrization, a variant of Loewner's theorem [65] states that the maps g_t satisfy the differential equation

$$\frac{dg_t(z)}{dt} = \frac{2}{g_t(z) - W(t)}, \tag{1}$$

where $W(t) := g_t\big(\beta(t)\big)$ is called the Loewner driving term. A few comments are in order.

1. Although g_t is defined in $\mathbb{H} \setminus \beta([0,t])$, it does extend continuously to $\beta(t)$, and therefore $W(t)$ is well defined.

2. If $z = \beta(s)$ for some s, then (1) makes sense only as long as $t < s$. That is to be expected. The domain of definition of g_t is shrinking as t increases. A point z falls out of the domain of g_t at the first time $\tau = \tau_z$ such that $\liminf_{t \nearrow \tau} g_t(z) - W(t) = 0$.

3. The main point here is that information about the path β is encoded in $W(t)$, which is a path in $\mathbb{R}$.

4. The proof of (1) is not too hard. In [53, Theorem 2.6] a proof (of a generalization) may be found.

We now return to the situation where β is the percolation interface chosen according to $\mu_{\mathbb{H},\mathbb{R}_+,\varepsilon}$, parametrized by half-plane capacity. It is easy to see that in this case $T = \infty$. Fix some $s > 0$. Suppose that we examine the colors of only those hexagons that are necessary to determine $\beta([0,s])$. This can be done by sequentially testing the hexagons adjacent to β starting from $\beta(0)$ as follows. Each time the already

determined arc of β meets a hexagon whose color has not yet been examined, we test the color (which permits us to extend the determined initial arc of β by at least one segment), until $\beta([0, s])$ has been determined. See Figure 4.

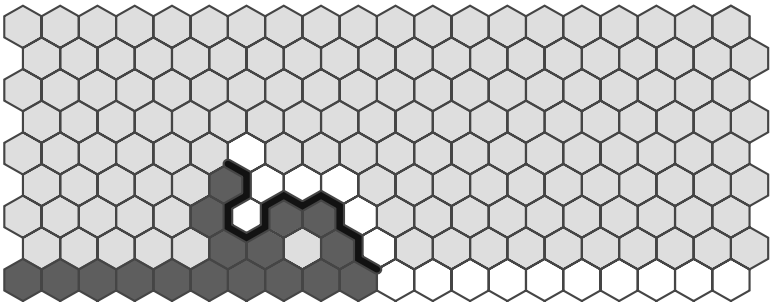


Figure 4. Initial segment of interface.

Now comes the main point. Let D_s be the unbounded component of the collection of hexagons of undetermined color in $\mathbb{H}$, and let ∂_+^s be the subset of ∂D_s lying on the boundary of hexagons of determined color white. Then the distribution of the continuation $\beta([s, \infty))$ of the interface given $\beta([0, s])$ is $\mu_{D_s, \partial_+^s, \varepsilon}$. By Smirnov's theorem, if $G\colon D_s \to \mathbb{H}$ is the conformal map satisfying the hydrodynamic normalization, then the image under G of $\mu_{D_s, \partial_+^s, \varepsilon}$ is close to $\mu_{\mathbb{H}, G(\partial_+^s), \varepsilon}$. (Actually, to justify this, one needs a slightly stronger "uniform" version of Smirnov's theorem. But here we want to convey the main ideas, and do not bother about being entirely precise.) Now, since D_s approximates $\mathbb{H} \setminus \beta([0, s])$, it follows that G is very close to g_s and $G(\partial_+^s)$ is close to $[W(s), \infty) = [g_s(\beta(s)), \infty)$. Therefore, in the limit as $\varepsilon \searrow 0$, we have for β sampled according to $\mu_{\mathbb{H}, \mathbb{R}_+}$ that given $\beta([0, s])$ the distribution of $g_s \circ \beta([s, \infty))$ (which is the conformal image of the continuation of the path) is $\mu_{\mathbb{H}, \mathbb{R}_+}$ translated by $W(s)$.

The Loewner driving term of the path $t \mapsto g_s \circ \beta(s + t)$ is $W(s + t)$, because $g_{s+t} \circ g_s^{-1}$ maps $\mathbb{H} \setminus g_s\big(\beta([s, s + t])\big)$ onto $\mathbb{H}$. The conclusion of the previous paragraph therefore implies that given $(W(t) : t \in [0, s])$ the distribution of the continuation of W is identical to the original distribution of W translated to start at $W(s)$. This is a very strong property. Indeed, for every $n \in \mathbb{N}$ and $t > 0$ we may write $W(t) = \sum_{j=1}^n \big(W(j\,t/n) - W((j-1)t/n)\big)$, which by the above is a sum of n independent identically distributed random variables. If we assume that the variance of $W(t)$ is finite, then it is also the sum of the variances of the summands. By the central limit theorem, $W(t)$ is therefore a Gaussian random variable. By symmetry, $W(t)$ has the same distribution as $-W(t)$, and so $W(t)$ is a centered Gaussian. It now easily follows that there is some constant $\kappa \geq 0$ such that $W(t)$ has the same distribution as $B(\kappa\, t)$, where B is one-dimensional Brownian motion starting at $B(0) = 0$. Using results from the theory of stochastic processes (e.g., the characterization of continuous martingales as time-changed Brownian motion), the same conclusion can be reached

while replacing the assumption that $W(t)$ has finite variance with the continuity of $W(t)$ in t.

We have just seen that Smirnov's theorem implies that the Loewner driving term of a sample from $\mu_{\mathbb{H},\mathbb{R}_+}$ is $B(\kappa t)$ for some $\kappa \geq 0$. This should serve as adequate motivation for the following definition from [79].

Definition 1.1. Fix some $\kappa \geq 0$, and let g_t be the solution of Loewner's equation (1) satisfying $g_0(z) = z$ with $W(t) = B(\kappa t)$, where B is standard one-dimensional Brownian motion starting at $B(0) = 0$. Then $(g_t : t \geq 0)$ is called *chordal stochastic Loewner evolution* with parameter κ or SLE_κ.

Of course, SLE_κ is a random one-parameter family of maps; the randomness is entirely due to the Brownian motion.

It has been proven [76], [59] that with probability 1 there is a (unique) random continuous path $\gamma(t)$ such that for each $t \geq 0$ the domain of definition of g_t is the unbounded component of $\mathbb{H} \setminus \gamma([0, t])$. The path is given by $\gamma(t) = g_t^{-1}(W(t))$, but proving that $g_t^{-1}(W(t))$ is well defined is not easy. It is also known [76] that a.s. $\gamma(t)$ is a simple path if and only if $\kappa \leq 4$ and is space-filling if and only if $\kappa \geq 8$. Sometimes the path γ itself is called SLE_κ. This is not too inconsistent, because g_t can be reconstructed from $\gamma([0, t])$ and vice versa.

If D is a simply connected domain in the plane and $a, b \in \partial D$ are two distinct points (or rather prime ends), then chordal SLE from a to b in D is defined as the image of γ under a conformal map from $\mathbb{H}$ to D taking 0 to a and ∞ to b. Though the map is not unique, the choice of the map does not effect the law of the SLE in D. This follows from the easily verified fact that up to a rescaling of time, the law of the SLE path is invariant under scaling by a positive real constant, as is the case for Brownian motion.

The reason for calling the SLE "chordal" is that it connects two boundary points of a domain D. There is another version of SLE, which connects a boundary point to an interior point, called *radial* SLE. Actually, there are a few other variations, but they all have similar definitions and analogous properties.

1.2. A historical narrative. In this subsection we list some works and discoveries related to SLE and random scaling limits in two dimensions. The following account is not comprehensive. Some of the topics not covered here are discussed in Wendelin Werner's [97] contribution to this ICM proceedings. We start by very briefly discussing the historical background.

In the survey paper [49], Langlands, Pouliot and Saint-Aubin present a collection of intriguing predictions from statistical physics. They have discussed these predictions and some simulation data with Aizenman, which prompted him to conjecture that the critical percolation crossing probabilities are asymptotically conformally invariant (see [49]). This means that the probability $Q_\varepsilon(D, \partial_1, \partial_2)$ that there exists a critical percolation cluster in a domain $D \subset \mathbb{C}$ connecting two boundary arcs ∂_1 and ∂_2 on a lattice with mesh ε has a limit $Q(D, \partial_1, \partial_2)$ as $\varepsilon \searrow 0$ and that the limit is conformally

invariant, namely, $Q(D, \partial_1, \partial_2) = Q\big(f(D), f(\partial_1), f(\partial_2)\big)$ if f is a homeomorphism from $\overline{D}$ to $f(\overline{D})$ that is conformal in D. This led John Cardy [20] to propose his formula (involving hypergeometric functions) for the asymptotic crossing probability in a rectangle between two opposite edges. The survey [49] highlighted these predictions and the role of the conjectured conformal invariance in critical percolation, as well as several other statistical physics models in two dimensions.

Prior to SLE there were attempts to use compositions of conformal slit mappings and even Loewner's equation in the study of diffusion limited aggregation (DLA). DLA is a random growth process, which produces a random fractal and is notoriously hard to analyse mathematically. (See [100], [4] for a definition and discussion of DLA.) Makarov and Carleson [22] used Loewner's equation to study a much simplified deterministic variant of DLA, which is not fractal, and Hastings and Levitov [34] have used conformal mapping techniques for a non-rigorous study of more realistic versions of DLA. Given that the fractals produced by DLA are not conformally invariant, it is not too surprising that it is hard to faithfully model DLA using conformal maps. Harry Kesten [44] proved that the diameter of the planar DLA cluster after n steps grows asymptotically no faster than $n^{2/3}$, and this appears to be essentially the only theorem concerning two-dimensional DLA, though several very simplified variants of DLA have been successfully analysed.

The original motivation for SLE actually came from investigating the Loop-erased random walk (a.k.a. LERW), which is a random curve introduced by Greg Lawler [51]. Consider some bounded simply-connected domain D in the plane. Let $G = G(D, \varepsilon)$ be the subgraph of a square grid of mesh ε that falls inside D and let V_∂ be the set of vertices of G that have fewer than 4 neighbors in D. Suppose that $0 \in D$, and let o be some vertex of G closest to 0. Start a simple random walk on G from o (at each step the walk jumps to any neighbor of the current position with equal probability). We keep track of the trajectory of the walk at each step, except that every time a loop is created, it is erased from the trajectory. The walk terminates when it first reaches V_∂, and the loop-erased random walk from o to V_∂ is the final trajectory. See Figure 5, where D is a disk.

The LERW is intimately related to the uniform spanning tree. In particular, if we collapse V_∂ to a single vertex v_∂ and take a random spanning tree of the resulting projection of G, where each possible spanning tree is chosen with equal probability, then the unique path in the tree joining o to v_∂ (as a set of edges) has precisely the same law as the LERW from o to V_∂ [74]. This is not a particular property of the square grid, the corresponding analog holds in an arbitrary finite graph. In the other direction, there is a marvelous algorithm discovered by David Wilson [99] which builds the uniform spanning tree by successively adding loop-erased random walks. The survey [66] is a good window into the beautiful theory of uniform spanning trees and forests.

Using sophisticated determinantcalculations and Temperley's bijection between the collection of spanning trees and a certain collection of dimer tilings (which is

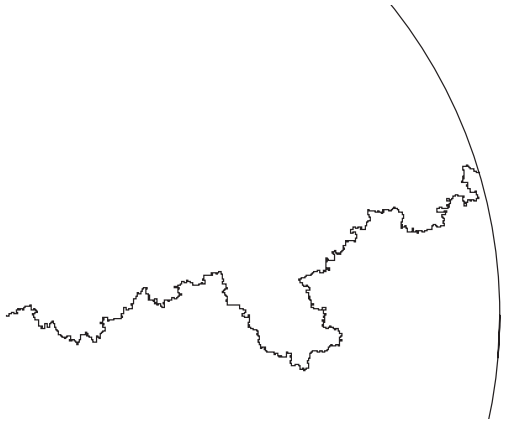


Figure 5. The LERW in a disk.

special to the planar setting), Richard Kenyon [39], [41], [40] was able to calculate several properties of the LERW. For example, it was shown that the variance of the winding number of the above LERW in $G(D, \varepsilon)$ is $(2 + o(1)) \log(1/\varepsilon)$ as $\varepsilon \searrow 0$, and that the growth exponent for the number of edges in a LERW is $5/4$.

In [79] it was shown that *if* the limit of the law of the LERW as $\varepsilon \searrow 0$ exists and is conformally invariant, then it is a radial SLE_2 path, when parametrized by capacity. (See subsection 2.1 for a description of two alternative topologies on spaces of probability measures on curves, for which this convergence may be stated.) In broad strokes, the reason why it should be an SLE path is basically the same as the argument presented above for the percolation interface. Two important properties of the percolation interface scaling limit were crucial in the above argument: conformal invariance and the following Markovian property. If we condition on an initial segment of the path, the remainder is an instance of the path in the domain slitted by the initial segment starting from the endpoint of the initial segment. Conformal invariance was believed to hold for the LERW scaling limit, while the Markovian property does hold for the reversal of the LERW.

The identification of the correct value of the parameter κ as 2 is based on Kenyon's calculated LERW winding variance growth rate and a calculation of the variance of the winding number of the radial SLE_κ path truncated at distance ε from the interior target point. The latter grows like $(\kappa + o(1)) \log(1/\varepsilon)$.

It was also conjectured in [79] that the percolation interface discussed above converges to SLE_6. The identification of the parameter κ as 6 in this case was based on Cardy's formula [20] and the verification that the corresponding formula holds for SLE_κ if and only if $\kappa = 6$.

The percolation interface satisfies the following locality property. The evolution of the path (given its past) does not depend on the shape of the domain away from

the current location of the endpoint of the path. Though this is essentially obvious, it should be noted that other interesting paths (such as the LERW scaling limit) do not satisfy locality.

Another process that clearly satisfies locality is Brownian motion. Greg Lawler and Wendelin Werner [61], [62] studied the intersection exponents of planar Brownian motion and the relations between them. An example of an intersection exponent is the unique number $\xi(1, 1)$ such that the probability that the paths of two independent Brownian motions started at distance 1 apart within the unit disk $\mathbb{U}$ and stopped when they first hit the circle $R\,\partial\mathbb{U}$ do not intersect one another is $R^{-\xi(1,1)+o(1)}$ as $R \to \infty$. At the time, there were conjectures [27] for the values of many of these exponents, which were rational numbers, but only two of these could be proved rigorously (not accidentally, those had values 1 and 2). These exponents encode many fundamental properties of Brownian motion. For example, Lawler [50] showed that the dimension of the outer boundary of planar Brownian motion stopped at time $t = 1$, say, is $2(1 - \alpha)$ for a certain intersection exponent α. Lawler and Werner [61], [62] have proved certain relations between the intersection exponents, and have shown that any process which like Brownian motion satisfies conformal invariance and a certain version of the locality property necessarily has intersection exponents that are very simply related to the Brownian exponents.

Since SLE_6 was believed to be the scaling limit of the percolation interface, it should satisfy locality. It is also conformally invariant by definition. Thus, the Brownian exponents should apply to SLE_6. Indeed, in a series of papers [53], [54], [55] Lawler, Werner and the present author proved the conjectured values of the Brownian exponents by calculating the corresponding exponents for SLE_6 (and using the previous work by Lawler and Werner). Very roughly, one can say that the reason why the exponents of SLE are easier to calculate than the Brownian exponents is that the SLE path, though it may hit itself, does not cross itself. Thus, the outer boundary of the SLE path is drawn essentially in chronological order.

Later [58] it became clear that the relation between SLE_6 and Brownian motion is even closer than previously apparent: the outer boundary of Brownian motion started from 0 and stopped on hitting the unit circle $\partial\mathbb{U}$ has the same distribution as the outer boundary of a variant of SLE_6.

Lennart Carleson observed that, assuming conformal invariance, Cardy's formula is equivalent to the statement that $Q(D, \partial_1, \partial_2) = \mathrm{length}(\partial_2)$ when D is an equilateral triangle of sidelength 1, ∂_1 is its base, and $\partial_2 \subset \partial D$ is a line segment having the vertex opposite to ∂_1 as one of its endpoints. Smirnov [87] proved Carleson's form of Cardy's formula for critical site percolation on the triangular lattice (that is, the same percolation model we have described above) and showed that crossing probabilities between two arcs on the boundary of a simply connected domain are asymptotically conformally invariant. As a corollary, Smirnov concluded that the scaling limit of the percolation interface exists and is equal to the SLE_6 path. This connection enabled proving many conjectures about this percolation model. For example, the prediction [24], [73] that the probability that the cluster of the origin has diameter larger

than R decays like

$$\mathbf{P}\big[\text{the origin is in a cluster of diameter} \geq R\big] = R^{-5/48+o(1)} \tag{2}$$

as $R \to \infty$ was proved [56]. This value $5/48$ is an example of what is commonly referred to as a critical exponent. Building on earlier work by Kesten and others, as well as on Smirnov's theorem and SLE, Smirnov and Werner [88] were able to determine many useful percolation exponents. Julien Dubédat [25] has used SLE to prove Watts' [92] formula for the asymptotic probability that in a given rectangle there are both a white horizontal and vertical crossing (for the above percolation model at $p = p_c = 1/2$).

The next process for which conformal invariance and convergence to SLE was established is the LERW [59]. Contrary to Smirnov's proof for percolation, where convergence to SLE was a consequence of conformal invariance, in the case of the LERW the proof establishes conformal invariance as a consequence of the convergence to SLE_2. More specifically, the argument in [59] proceeds by considering the Loewner driving term of the discrete LERW (before passing to the limit) and proving that the driving term converges to an appropriately time-scaled Brownian motion. The same paper also shows that the uniform spanning tree scaling limit is conformally invariant, and the Peano curve associated with it (essentially, the boundary of a thickened uniform spanning tree) converges to SLE_8. Another difference between the results of [87] and [59] is that while the former is restricted to site percolation on the triangular lattice, the results in [59] are essentially lattice independent. Figure 5 above shows a fine LERW, which gives an idea of what an SLE_2 looks like. Likewise, Figure 6 shows a sample of an initial segment of the uniform spanning tree Peano curve in a rectangular domain. Note that the curve is space filling, as is SLE_8.

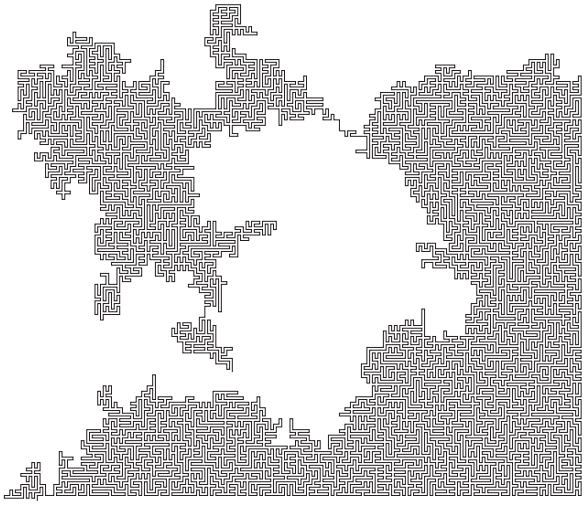


Figure 6. An initial segment of the uniform spanning tree Peano path.

Meanwhile, Gady Kozma [47] came up with a different proof that the LERW scaling limit exists. Although Kozma's proof does not identify the limit, it has the advantage of generalizing to three dimensions [48].

There are two discrete models for which convergence to SLE_4 has been established by Scott Sheffield and the present author. These models are the harmonic explorer [80] and the interface of the discrete Gaussian free field [81]. The discrete and continuous Gaussian free fields (a.k.a. the harmonic crystal) play an important role in the heuristic physics analysis of various statistical physics models. The discrete Gaussian free field is a probability measure on real valued functions defined on a graph, often a piece of a lattice. If, for example, the graph is a triangulation of a domain in the plane, an interface is a curve in the dual graph separating vertices where the function is positive from vertices where the function is negative. See [85] or [81] for further details, and see Figure 7 for a simulation of the harmonic explorer, and therefore an approximation of SLE_4.

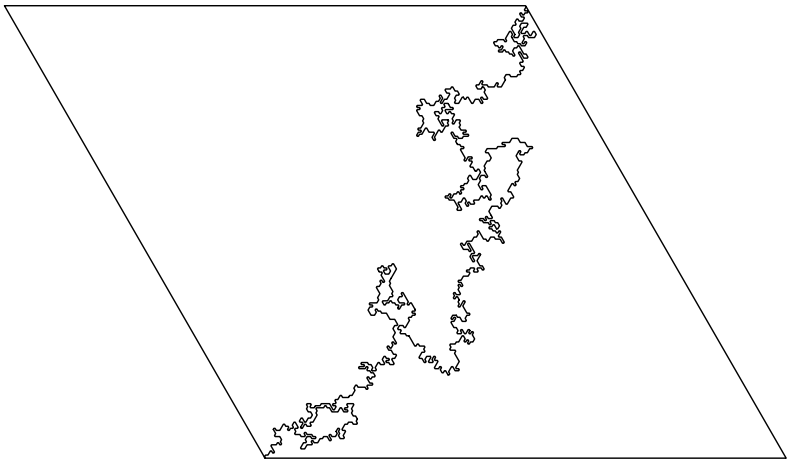


Figure 7. The harmonic explorer path.

Sheffield also announced work in progress connecting the Gaussian free field with SLE_κ for other values of κ. The basic idea is that while SLE_4 may be thought of as a curve solving the equation $h = 0$, where h is the Gaussian free field, for other κ, the SLE_κ curve may be considered as a solution of

$$c\,\mathrm{winding}(\gamma[0,t]) = h(\gamma(t)), \tag{3}$$

where c is a constant depending on κ. When $\kappa = 4$, the corresponding constant c is zero, which reduces to the setting of [81]. Alternatively, (3) can be heuristically written as $c\,\gamma'(s) = \exp(i\,h(\gamma(t))$, where s is the length parameter of γ. However, we stress that it is hard to make sense of these equations, for the Gaussian free field

is not a smooth function (in fact, it is not even a function but rather a distribution). Likewise, the SLE path is not rectifiable and its winding at most points is infinite.

As mentioned above, there are several different variants of SLE in simply connected domains: chordal, radial, as well as a few others, which we have not mentioned. These variants are rather closely related to one another [83]. There are also variants defined in the multiply-connected setting [101], [6], [5], [7]. One motivation for this study comes from statistical physics models, which are easy to define on multiply connected domains. Since one can easily vary the boundary conditions on different boundary components of the domain, it is clear that there is often more than one reasonable choice for the definition of the SLE path.

Finally, we mention an intriguing connection between Brownian motion and SLE_κ for $\kappa \in (8/3, 4]$. There is the notion of the Brownian loop soup [63], which is a Poisson measure on the space of Brownian motion loops. According to [93], the boundaries of clusters of a sample from the loop soup measure with intensity c are SLE_κ-like paths, where $\kappa = \kappa(c) \in (8/3, 4]$. The proof is to appear in a future joint work of Sheffield and Werner.

The above account describes some of the highlights of the developments in the field in the past several years. The rest of the paper will be devoted to a description of some problems where we hope to see some future progress. Some of these problems are obvious to anyone working in the field (though the solution is not obvious), while others are borrowed from several different sources. A few of the problems appear here for the first time. The paper [76] contains some additional problems.

2. Random processes converging to SLE

As we have seen, paths associated with several random processes have been proved to converge to various SLE paths. However, the list of processes where the convergence is expected but not proved yet is longer. This section will present questions of this sort, most of which have previously appeared in the literature.

The strategy of the proofs of convergence to SLE in the papers [59], [80], [81] is very similar. In these papers, a collection of martingales with respect to the filtration given by the evolution of the curve is used to gain information about the Loewner driving term of the discrete curve. Although such a proof is also possible for the percolation interface (using Cardy's formula), this technique was not available at the time, and Smirnov used instead an argument which uses the independence properties of percolation in an essential way and is therefore not likely to be applicable to many other models. Thus, it seems that presently the most promising technique is the martingale technique from [59].

2.1. Notions of convergence. To be precise, we must describe the meaning of these scaling limits. In fact, there are at least two distinct reasonable notions of convergence, which we now describe. Suppose that γ_n are random paths in the closed upper half

plane $\overline{\mathbb{H}}$ starting from 0. Consider the one-point compactification $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ of $\mathbb{C} = \mathbb{R}^2$, which may be thought of as the sphere S^2. The law of γ_n may be thought of as a Borel probability measure on the Hausdorff space of closed nonempty subsets of $\hat{\mathbb{C}}$. Since that Hausdorff space is compact, the space of Borel probability measures on it is compact with respect to weak convergence of measures [26]. We may say that γ_n converges in the Hausdorff sense to a random set $\gamma \subset \overline{\mathbb{H}} \cup \{\infty\}$ if the law of γ_n converges weakly to the law of γ. A similar definition applies to curves in the closure of a bounded domain $D \subset \mathbb{C}$. The above stated instances of convergence to SLE hold with respect to this notion. However, in the case of convergence to SLE_8, this does not mean very much, for SLE_8 fills up the domain.

The second notion of convergence is stronger. Suppose that each γ_n is a.s. continuous with respect to the half-plane capacity parametrization from ∞. (This holds, in particular, if γ_n is a.s. a (continuous) simple path.) If d is a metric on $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ compatible with its topology, then we may consider the metric

$$d^*(\beta_1, \beta_2) := \sup_{t \in [0,\infty)} d\big(\beta_1(t), \beta_2(t)\big)$$

on the space of continuous paths defined on $[0, \infty)$. We may say that γ_n converges to a random path γ weakly-uniformly if the law of γ_n converges weakly to the law of γ in the space of Borel measures with respect to the metric d^*. This implies Hausdorff convergence. Since d^* is finer than the Hausdorff metric, there are more functions from the space of paths to $\mathbb{R}$ that are continuous with respect to d^* than with respect to the Hausdorff metric. Consequently, weakly-uniform convergence is stronger than Hausdorff convergence. In all the results stated above saying that some random path converges to SLE, the convergence is weakly-uniform when the paths are parametrized by capacity or half-plane capacity (depending on whether the convergence is to radial or chordal SLE, respectively).

In the following, when we ask for convergence to SLE, we will mean weakly-uniform convergence. However, weaker nontrivial forms of convergence would also be very interesting.

2.2. Self avoiding walk. Let G be either the square, the hexagonal or the triangular grid in the plane, positioned so that 0 is some vertex in G. For $n \in \mathbb{N}$ consider the uniform measures on all self avoiding n-step walks in G that start at 0 and stay in the upper half plane. It has been shown in [60] that when $G = \mathbb{Z}^2$ the limiting measure as $n \to \infty$ exists. (The same proof probably applies for the other alternatives for G, provided that G is positioned so that horizontal lines through vertices in G do not intersect the relative interior of edges of G which they do not contain.)

Problem 2.1 ([60]). Let γ be a sample from the $n \to \infty$ limit of the uniform measure on n-step self avoiding paths in the upper half plane described above. Prove that the limit as $s \searrow 0$ of the law of $s\,\gamma$ exists and that it is $\mathrm{SLE}_{8/3}$.

The convergence may be considered with respect to either of the two topologies discussed in subsection 2.1.

In [60] some consequences of this convergence are indicated, as well as support for the conjecture.

There are some indications that the setting of the hexagonal lattice is easier: the rate of growth of the number of self avoiding paths on the hexagonal grid is predicted [72] to be $\left(2+\sqrt{2}+o(1)\right)^{n/2}$; no such prediction exists for the square grid or triangular lattice.

In dimensions $d > 4$ Takashi Hara and Gordon Slade [32] proved that the scaling limit of self-avoiding random walk is Brownian motion. This is also believed to be the case for $d = 4$. See [67] for references and further background on the self-avoiding walk.

2.3. Height models. There is a vast collection of height model interfaces that should converge to SLE_4. The one theorem in this regard is the convergence of the interface of the Gaussian free field [81]. This was motivated by Kenyon's theorem stating that the domino tiling height function converges to the Gaussian free field [42] and by Kenyon's conjecture that the double domino interface converges to SLE_4 (see [76] for a statement of this problem).

The domino height function is a function on $\mathbb{Z}^2$ associated with a domino tiling (see [42]). Its distribution is roughly (ignoring boundary issues) the uniform measure on functions $h\colon \mathbb{Z}^2 \to \mathbb{Z}$ such that $h(0,0) = 0$,

$$h(x,y) \mod 4 = \begin{cases} 0 & x, y \text{ even}, \\ 1 & x \text{ odd } y \text{ even}, \\ 2 & x, y \text{ odd}, \\ 3 & x \text{ even } y \text{ odd}, \end{cases}$$

and $|h(z) - h(z')| \in \{1,3\}$ if $|z - z'| = 1$, $z, z' \in \mathbb{Z}^2$.

Let D be a bounded domain in the plane whose boundary is a simple path in the triangular lattice, say. Let ∂_+ and ∂_- be complementary arcs in ∂D such that the two common endpoints of these arcs are midpoints of edges. Consider the uniform measure on functions h taking odd integer values on vertices in $\bar{D}$ such that $h = 1$ on ∂_+, $h = -1$ on ∂_-, and $|h(v) - h(u)| \in \{0,2\}$ for neighbors v, u. We may extend such a function h to $\bar{D}$ by affine interpolation within each triangle, and this interpolation is consistent along the edges. There is then a unique connected path γ that is the connected component of $h^{-1}(0)$ that contains the two endpoints of each of the two arcs $\partial_\pm$.

Problem 2.2. Is it true that the path γ tends to SLE_4? Does the law of h converge to the Gaussian free field?

The convergence we expect for h is in the same sense as in [42].

Note that if we restrict in the above the image of h to be $\{1,-1\}$, we obtain critical site percolation on the triangular grid, and the limit of the corresponding interface is in this case SLE_6.

Now suppose that $(D, \partial_+, \partial_-)$ is as above. Let $\lambda \in (0, 1/2]$ be some constant and consider the uniform measure on functions h taking real values on vertices in $\overline{D}$ such that $h = \lambda$ on ∂_+, $h = -\lambda$ on ∂_- and $|h(v) - h(u)| \leq 1$ for every edge $[v, u]$.

Problem 2.3. Is it true that for some value of λ the corresponding interface converges to SLE_4? Does the law of h converge in some sense to the Gaussian free field?

In the case of the corresponding questions for the discrete Gaussian free field, there is just one constant λ such that the interface converges to SLE_4. For other choices of λ the interface converges to a well-known variant of SLE_4 [81].

There are some restricted classes of height models for which convergence to the Gaussian free field is known [71]. It may still be very hard to prove that the corresponding interface converges to SLE_4. One interesting problem of this sort is the following.

Problem 2.4 ([81]). If we project the Gaussian free field onto the subspace spanned by the eigenfunctions of the Dirichlet Laplacian with eigenvalues in $[-r, r]$ and add the harmonic function with boundary values $\pm\lambda$ on $\partial_\pm$, does the corresponding interface converge to SLE_4 as $r \to \infty$ when λ is chosen appropriately?

The problem is natural, because the Gaussian free field is related to the Dirichlet Laplacian. In particular, the projections of the field onto the spaces spanned by eigenfunctions with eigenvalues in two disjoint intervals are independent.

2.4. The Ising, FK, and $O(n)$ loop models. The Ising model is a fundamental physics model for magnetism. Consider again a domain D adapted to the triangular lattice and a partition $\partial D = \partial_+ \cup \partial_-$ as in subsection 2.3. Now consider a function h that take the values ± 1 on vertices in $\overline{D}$ such that h is 1 on ∂_+ and -1 on ∂_-. On the collection of all such functions we put a probability measure such that the probability for a given h is proportional to $e^{-2\beta k}$, where β is a parameter and k is the number of edges $[v, u]$ such that $h(v) \neq h(u)$. This is known as the Ising model and the value associate to a vertex is often called a spin. It is known that the critical value β_c (which we do not define here in the context of the Ising model) for β satisfies $e^{2\beta} = \sqrt{3}$ (see [69], [35]). Again, the interface at the critical $\beta = \beta_c$ is believed to converge to an SLE path, this time SLE_3. For $\beta \in [0, \beta_c)$ fixed, the interface should converge to SLE_6. Note that when $\beta = 0$, the model is again identical to critical site percolation on the triangular grid, and the interface does converge to SLE_6.

Problem 2.5. Prove that when $\beta = \beta_c$, the interface converges to SLE_3 and when $\beta \in (0, \beta_c)$ to SLE_6.

When $\beta > \beta_c$ we do not expect convergence to SLE, and do not expect conformal invariance. The interface scaling limit is in this case a straight line segment if the domain is convex [75] (see also [29]).

The Fortuin–Kasteleyn [28] (FK) model (a.k.a. the random cluster model) is a probability measure on the collection of all subsets of the set of edges E of a finite

graph $G = (V, E)$. In the FK model, the measure of each $\omega \subset E$ is proportional to $\big(p/(1-p)\big)^{|\omega|}\, q^c$, where $q > 0$ and $p \in (0, 1)$ are parameters, $|\omega|$ is the cardinality of ω, and c is the number of connected components of the subgraph (V, ω). The FK model is very closely related to the well known Potts model [8], which is a generalization of the Ising model. Many questions about the Potts model can be translated to questions about the FK model and vice versa.

On the grid $\mathbb{Z}^2$, when $p = \sqrt{q}/(1+\sqrt{q})$ the FK model satisfies a form of self-duality.

Problem 2.6 ([76]). Prove that when $q \in (0, 4)$ and $p = \sqrt{q}/(1+\sqrt{q})$, the interface of the FK model on $\mathbb{Z}^2$ with appropriate boundary conditions converges to SLE_κ, where $\kappa = 4\pi/\cos^{-1}\big(-\sqrt{q}/2\big)$. (See [76] for further details.)

The $O(n)$ loop model on a finite graph $G = (V, E)$ is a measure on the collection of subgraphs of G where the degree of every vertex in the subgraph is 2. (The subgraph does not need to contain all the vertices.) The probability of each such subgraph is proportional to $x^e\, n^c$, where c is the number of connected components, e is the number of edges in the subgraph, and $x, n > 0$ are parameters. When n is a positive integer, the $O(n)$ loop model is derived from the $O(n)$ spin model, which is a measure on the set of functions which associate to every vertex a unit vector in $\mathbb{R}^n$.

In order to pin down a specific long path in the $O(n)$ loop model, we pick two points on the boundary of the domain and require that in the random subgraph the degrees of two boundary vertices near these two points be 1, while setting the degrees of all other boundary vertices to 0, say. Then the measure is supported on configurations with one simple path and a collection of loops.

Now we specialize to the hexagonal lattice. Set $x_c(n) := \big(2+\sqrt{2-n}\big)^{-1/2}$, which is the conjectured critical parameter [72].

Problem 2.7 ([36]). Prove that when $n \in [0, 2]$ and $x = x_c(n)$ (respectively, $x > x_c(n)$) the scaling limit of the path containing the two special boundary vertices is chordal SLE_κ, where $\kappa \in [8/3, 4]$ (respectively, $\kappa \in [4, 8]$) and $n = -2\cos(4\pi/\kappa)$.

When $x < x_c(n)$, we expect the scaling limit to be a straight line segment (if the domain is convex). The fact that at $n = 1$ we get the same limits as for the Ising model is no accident. It is not hard to see that the $O(1)$ loop measure coincides with the law of boundaries of Ising clusters. See [36] for further details.

Similar conjectures should hold in other lattices. However, the values of the critical parameters are expected to be different.

2.5. Lattice trees. We now present an example of a discrete model where we suspect that perhaps conformal invariance might hold. However, we do not presently have a candidate for the scaling limit.

Fix $n \in \mathbb{N}_+$, and consider the collection of all trees contained in the grid G that contain the origin and have n vertices. Select a tree T from this measure, uniformly at random.

Problem 2.8. What is the growth rate of the expected diameter of such a tree? If we rescale the tree so that the expected (or median) diameter is 1, is there a limit for the law of the tree as $n \to \infty$? What are its geometric and topological properties? Can the limit be determined?

It would be good to be able to produce some pictures. However, we presently do not know how to sample from this measure.

Problem 2.9. Produce an efficient algorithm which samples lattice trees approximately uniformly, or prove that such an algorithm does not exist.

See [86] for background on lattice trees and for results in high dimensions and [17] for an analysis of a related continuum model.

2.6. Percolation interface. It is natural to try to extend the understanding of percolation at p_c to percolation at a parameter p tending to p_c. One possible framework is as follows. Fix a parameter $q \in (0, 1)$. Suppose that in Figure 3 with small mesh $\varepsilon > 0$ we choose $p(\varepsilon)$ so that the probability to have a left to right crossing of white hexagons in some fixed 1×1 square in the upper half plane is q at percolation parameter $p = p(\varepsilon)$. The corresponding interface will still be an unbounded path starting at 0, but its distribution will be different from the interface at $p = 1/2$ if $q \neq 1/2$. Thus, it is natural to ask

Problem 2.10 (Lincoln Chayes (personal communication)). What is the scaling limit of the interface as $\varepsilon \searrow 0$ and $p = p(\varepsilon)$ if $q \neq 1/2$ is fixed?

This problem is also very closely related to a problem formulated by F. Camia, L. Fontes and C. Newman [18].

Site percolation on the triangular lattice is only one of several different models for percolation in the plane. Among discrete models, widely studied is bond percolation on the square grid. As for site percolation on the triangular lattice, the critical probability is again $p_c = 1/2$.

At present, Smirnov's proof does not work for bond percolation on the square grid. The proof uses the invariance of the model under rotation by $2\pi/3$. Thus, the following problem presents itself.

Problem 2.11. Prove Smirnov's theorem for critical bond percolation on $\mathbb{Z}^2$.

Some progress on this problem has been reported by Vincent Beffara [9].

There are other natural percolation models which have been studied. Among them we mention Voronoi percolation and the boolean model. In Voronoi percolation one has two independent Poisson point processes in the plane, W and B, with intensities p and $1-p$, respectively. Let $\hat{W}$ be the closure of the set of points in $\mathbb{R}^2$ closer to W than to B, and let $\hat{B}$ be the closure of the set of points closer to B. The set $\hat{W}$ is a sample from Voronoi percolation at parameter p. Some form of conformal invariance was proved for Voronoi percolation [14], but the version proved does not imply convergence

to SLE. It is neither stronger nor weaker than the conformal invariance proved by Smirnov. Notable recent progress has been made for Voronoi percolation by Bollobás and Riordan [15], who established the very useful Russo–Seymour–Welsh theorem, as well as $p_c = 1/2$ for Voronoi percolation.

Problem 2.12. Prove Smirnov's theorem for Voronoi percolation.

The boolean percolation model (a.k.a. continuum percolation) can be defined by taking a Poisson set of points $W \subset \mathbb{R}^2$ of intensity 1 and letting $\hat{W}$ be the set of points in the plane at distance at most r from W. Here, r is the parameter of the model. (Alternatively, one may fix $r = 1$, say, and let the intensity of the Poisson process be the parameter, but this is essentially the same, by scaling.) The Russo–Seymour–Welsh theorem is known for this model [1], [77], but the critical value of the parameter has not been identified. A nice feature which the model shares with Voronoi percolation is invariance under rotations.

Problem 2.13. Prove Smirnov's theorem for boolean percolation.

3. Critical exponents

The determination of critical exponents has been one motivation to prove conformal invariance for discrete models. For example, den Nijs and Nienhuis predicted [24], [73] that the probability that the critical percolation cluster of the origin has diameter larger than R is $R^{-5/48+o(1)}$ as $R \to \infty$. Likewise, the probability that a given site in the square $[-R, R]^2$ is pivotal for a left-right crossing of the square $[-2R, 2R]^2$ was predicted to be $R^{-5/4+o(1)}$. (Here, pivotal means that the occurrence or non-occurrence of a crossing would be modified by flipping the status of the site.) These and other exponents were proved for site percolation on the triangular grid using Smirnov's theorem and SLE [56], [88]. The determination of the exponents is very useful for the study of percolation.

Richard Kenyon [39] calculated by enumeration techniques involving determinants the asymptotics of the probability that an edge belongs to a loop-erased random walk. The probability decays like $R^{-3/4+o(1)}$ when the distance from the edge to the endpoints of the walk is R. However, Kenyon's estimate is much more precise; he shows that, in a specific domain, $R^{3/4}$ times the probability is bounded away from zero and infinity, and in fact estimates the probability as $f\, R^{-3/4}\left(1 + o(1)\right)$ as $R \to \infty$, where f is an explicit function of the position of the edge.

Thus, it is natural to ask for such precise estimates for the important percolation events as well. Namely,

Problem 3.1. Improve the estimates $R^{-5/48+o(1)}$ and $R^{-5/4+o(1)}$ mentioned above (as well as other similar estimates) to more precise formulas. It would be especially nice to obtain estimates that are sharp up to multiplicative constants.

In addition to the case of the loop-erased random walk mentioned above, estimates up to constants are known for events involving Brownian motions [57].

The difficulty in getting more precise estimates is not in the analysis of SLE. Rather, it is due to the passage between the discrete and continuous setting. Consequently, the above problem seems to be related to the following.

Problem 3.2. Obtain reasonable estimates for the speed of convergence of the discrete processes which are known to converge to SLE.

There are still critical exponents which do not seem accessible via an SLE analysis. For example, we may ask

Problem 3.3. Calculate the number α such that on the event that there is a left-right crossing in critical percolation in the square $[0, R]^2$, the expected length of the shortest crossing is $R^{\alpha+o(1)}$.

Ziff [102] predicts an exponent which is related to this α, but it seems that there is currently no prediction for the exact value of α.

4. Quantum gravity

Consider the uniform measure μ_n on equivalence classes of n-vertex triangulations of the sphere, where two triangulations are considered equivalent if there is a homeomorphism of the sphere taking one to the other. One may view a sample from this measure with the graph metric as a random geometry on the sphere. Such models go under the name "quantum gravity" in physics circles. One may also impose statistical physics models on such random triangulations. For example, the sample space may include such a triangulation (or rather, equivalence class of triangulations) together with a map h from the vertices to $\{-1, 1\}$. The measure of such a pair may be taken proportional to a^k, where k is the number of edges $[v, u]$ in the triangulation for which $h(v) \neq h(u)$ and $a > 0$ is a parameter. Thus, we are in effect considering a triangulation weighted by the Ising model partition function. (The partition function is in this case the sum of all the weights of such functions h on the given triangulation.) Likewise, one may weight the triangulation by other kinds of partition functions.

In some cases it is easier to make a heuristic analysis of such statistical physics models in the quantum gravity world than in the plane. The enigmatic KPZ formula of Knizhnik, Polyakov and Zamolodchikov [46] was used in physics to predict properties of statistical physics in the plane from the corresponding properties in quantum gravity. Basically, the KPZ formula is a formula relating exponents in quantum gravity to the corresponding exponents in plane geometry.

To date, there has been progress in the mathematical (as well as physical) understanding of the statistical physics in the plane as well as in quantum gravity [2], [3], [16]. However, there is still no mathematical understanding of the KPZ formula. In fact, the author's understanding of KPZ is too weak to even state a concrete problem.

However, we may ask about the scaling limit of μ_n. There has been significant progress lately describing some aspects of the geometry of samples from μ_n [2], [23]. In particular, it has been shown by Chassaing and Schaeffer [23] that if D_n is the graph-metric diameter of a sample from μ_n, then $D_n/n^{-1/4}$ converges in law to some random variable in $(0, \infty)$. However, the scaling limit of samples from μ_n is not known. On the collection of compact metric spaces, we may consider the Gromov–Hausdorff distance $d_{\mathrm{GH}}(X, Y)$, which is the infimum of the Hausdorff distance between subsets X^* and Y^* in a metric space Z^* over all possible triples (X^*, Y^*, Z^*) such that Z^* is a metric space, $X^*, Y^* \subset Z^*$, X is isometric with X^* and Y is isometric with Y^*. Let X_n be a sample from μ_n, considered as a metric space with the graph metric scaled by $n^{-1/4}$, and let μ_n^* denote the law of X_n.

Problem 4.1. Show that the weak limit $\lim_{n\to\infty} \mu_n^*$ with respect to the Gromov–Hausdorff metric exists. Determine the properties of the limit.

Note that [68] proves convergence of samples from μ_n, but the metric used there on the samples from μ_n is very different and consequently a solution of Problem 4.1 does not seem to follow.

5. Noise sensitivity, Fourier spectrum, and dynamical percolation

The indicator function of the event of having a percolation crossing in a domain between two arcs on the boundary is a boolean function of boolean variables. Some fundamental results concerning percolation are based on general theorems about boolean functions. (One can mention here the BK inequality, the Harris-FKG inequality and the Russo formula. See, e.g. [30].) Central to the theory of boolean functions is the Fourier expansion. Basically, if $f\colon \{-1, 1\}^n \to \mathbb{R}$ is any function of n bits, the Fourier–Walsh expansion of f is

$$f(x) = \sum_{S\subset[n]} \hat{f}(S)\, \chi_S(x),$$

where $\chi_S(x) = \prod_{j\in S} x_j$ for $S \subset [n] = \{1, \ldots, n\}$. When we consider $\{-1, 1\}^n$ with the uniform probability measure, the collection $\{\chi_S : S \subset [n]\}$ forms an orthonormal basis for $L^2(\{-1, 1\}^n)$. (Often other measures are also considered.) If we suppose that $\|f\|_2 = 1$ (in particular, this holds if $f\colon \{-1, 1\}^2 \to \{-1, 1\}$), then the Parseval identity gives $\sum_{S\subset[n]} \hat{f}(S)^2 = 1$. Thus, we get a probability measure μ_f on $2^{[n]} = \{S : S \subset [n]\}$ for which $\mu_f(\{S\}) = \hat{f}(S)^2$. The map $S \mapsto |S|$, assigning to each $S \subset [n]$ its cardinality pushes forward the measure μ_f to a measure $\tilde{\mu}_f$ on $\{0, 1, \ldots, n\}$. This measure $\tilde{\mu}_f$ may be called the Fourier spectrum of f. The Fourier spectrum encodes important information about f, and quite a bit of research on the subject exists [37]. For instance, one can read off from $\tilde{\mu}_f$ the sensitivity of f to noise (see [13]).

When f is a percolation crossing function (i.e., 1 if there is a crossing, -1 otherwise), the corresponding index set $[n]$ is identified with the collection of relevant sites or bonds, depending if it is a site or bond model. Though there is some partial understanding of the Fourier spectrum of percolation [82], the complete picture is unclear. For example, if the domain is approximately an $\ell \times \ell$ square in the triangular lattice, then for the indicator function f_ℓ of a crossing in critical site percolation it is known [82] that for every $\alpha < 1/8$

$$\tilde{\mu}_{f_\ell}([1, \ell^\alpha]) \to 0 \tag{4}$$

as $\ell \to \infty$. This is proved using the critical exponents for site percolation as well as an estimate for the Fourier coefficients of general functions (based on the existence of an algorithm computing the function which is unlikely to examine any specific input variable). On the other hand, using the percolation exponents one can show that (4) fails if $\alpha > 3/4$. This is based on calculating the expected number of sites pivotal for a crossing (i.e., a change of the value of the corresponding input variable would change the value of the function) as well as showing that the second moment is bounded by a constant times the square of the expectation. The expected number of pivotals is known [88] to be $\ell^{3/4+o(1)}$ as $\ell \to \infty$. It is reasonable to conjecture that (4) holds for every $\alpha < 3/4$.

Problem 5.1. Is it true that $\lim_{\ell\to\infty} \tilde{\mu}_{f_\ell}([\ell^{\alpha_1}, \ell^{\alpha_2}]) = 1$ if $\alpha_1 < 3/4 < \alpha_2$? Determine the asymptotic behavior of $\tilde{\mu}_{f_\ell}([\ell^{\alpha_1}, \ell^{\alpha_2}])$ as $\ell \to \infty$ for arbitrary $0 \le \alpha_1 < \alpha_2 \le 2$.

Estimates on the Fourier coefficients of percolation crossings (in an annulus) play a central part in the proof [82] that dynamical percolation has exceptional times. Dynamical percolation (introduced in [31]) is a model in which at each fixed time one sees an ordinary percolation configuration, but the random bits determining whether or not a site (or bond) is open undergo random independent flips at a uniform rate, according to independent Poisson processes. The main result of [82] is that dynamical critical site percolation on the triangular lattice has exceptional times at which there is an infinite percolation component. These set of times are necessarily of zero Lebesgue measure. A better understanding of the Fourier coefficients may lead to sharper results about dynamical percolation, such as the determination of the dimension of exceptional times. Some upper and lower bounds for the dimension are known [82].

One would hope to understand the measure μ_f geometrically. Gil Kalai (personal communication) has suggested the problem of determining the scaling limit of μ_f. More specifically, the Fourier index set S for critical percolation crossing of a square is naturally identified with a subset of the plane. If we rescale the square to have edge length 1 while refining the mesh, then μ_f may be thought of as a probability measure on the Hausdorff space $\mathcal{H}$ of closed subsets of the square. It is reasonable to expect that μ_f converges weakly to some probability measure μ on $\mathcal{H}$. We really do not know what samples from μ look like. Could it be that μ is supported on singletons? Alternatively, is it possible that $\mu[S = \text{entire square}] = 1$? Is S a Cantor set μ-a.s.?

Problem 5.2 (Gil Kalai, personal communication). Prove that the limiting measure μ exists and determine properties of samples from μ.

Kalai suspects (personal communication) that the set S is similar to the set of pivotal sites (which is a.s. a Cantor set in the scaling limit). This is supported by the easily verified fact that $\mathbf{P}\big[i \in S\big] = \mathbf{P}\big[i \text{ pivotal}\big]$ and $\mathbf{P}\big[i, j \in S\big] = \mathbf{P}\big[i, j \text{ pivotal}\big]$ hold for arbitrary boolean functions. Examples of functions where the scaling limit of S has been determined are provided by Tsirelson [90], [91].

One may try to study a scaling limit of dynamical percolation. Consider dynamical critical site percolation on a triangular lattice of mesh ε, where the rate at which the sites flip is $\lambda > 0$. We choose $\lambda = \lambda(\varepsilon)$ so that the correlation between having a left-right crossing of a fixed square at time 0 and at time 1 is $1/2$, say. Noise sensitivity of percolation [13] shows that $\lim_{\varepsilon \searrow 0} \lambda(\varepsilon) = 0$ and the results of [82] imply that $\lambda(\varepsilon) = \varepsilon^{O(1)}$ and $\varepsilon = \lambda(\varepsilon)^{O(1)}$ for $\varepsilon \in (0, 1]$. It is not hard to invent (several different) notions in which to take the limit of dynamical percolation as $\varepsilon \searrow 0$.

Problem 5.3. Prove that the scaling limit of dynamical critical percolation exists. Prove that correlations between crossing events at different times $t_1 < t_2$ decay to zero as $t_2 - t_1 \to \infty$ and that a change in a crossing event becomes unlikely if $t_2 - t_1 \to 0$.

Since the correlation between events occurring at different times can be expressed in terms of the Fourier coefficients [13], [82], it follows that the second statement in Problem 5.3 is very much related to strong concentration of the measure $\tilde{\mu}_{f_\ell}$, in the spirit of Problem 5.1.

Because of the dependence of λ on ε, it is not reasonable to expect the dynamical percolation scaling limit to be invariant under maps of the form $f \times$ identity, where $f\colon D \to D'$ is conformal and the identity map is applied to the time coordinate. In particular, in the case where $f(z) = a\,z, a > 0$, one should expect dynamical percolation to be invariant under the map $f \times (t \mapsto a^\beta\, t)$, where $\beta := -\lim_{\varepsilon \searrow 0} \log \lambda(\varepsilon)/\log \varepsilon$ (and this limit is expected to exist). It is not too hard to see that $\beta = 3/4$ if the answer to the first question in Problem 5.1 is yes.

This suggests a modified form of conformal invariance for dynamical percolation. Suppose that $F(z, t)$ has the form $F(z, t) = \big(f(z), g(z, t)\big)$, where $f\colon D \to D'$ is conformal and g satisfies $\partial_t g(z, t) = |f'(z)|^\beta$, with the above value of β. Is dynamical percolation invariant under such maps? If such invariance is to hold, it would be in a "relativistic" framework, in which one does not consider crossings occurring at a specific time slice, but rather inside a space-time set. It is not clear if one can make good sense of that.

6. LERW and UST

The loop-erased random walk and the uniform spanning tree are models where very detailed knowledge exists. They may be studied using random walks and electrical

network techniques, and in the two-dimensional setting also by SLE as well as domino tiling methods. (See [66] and the references cited there.) However, some open problems still remain.

One may consider the random walk in a fine mesh lattice in the unit disk, which is stopped when it hits the boundary of the disk. The random walk converges to Brownian motion while its loop-erasure converges to SLE_2. It is therefore reasonable to expect that the law of the pair (random walk, its loop-erasure) converges to a coupling of Brownian motion and SLE_2. (If not, a subsequential limit will converge.)

Problem 6.1. In this coupling, is the SLE_2 determined by the Brownian motion?

It seems that this question occurred to several researchers independently, including Wendelin Werner (personal communication).

Of course, one cannot naively loop-erase the Brownian motion path, because there is no first loop to erase and there are cases where the erasure of one loop eliminates some of the other loops.

It is also interesting to try to extend some of the understanding of probabilistic statistical physics models beyond the planar setting to higher genus. The following problem in this direction was proposed by Russell Lyons (personal communication).

Consider the uniform spanning tree on a fine square grid approximation of a torus. There is a random graph dual to the tree, which consists of the dual edges perpendicular to primal edges not in the tree. It is not hard to see that this random dual of the tree contains precisely three edge-simple closed paths (i.e., no repeating edges), and that these paths are not null-homotopic.

Problem 6.2. Determine the distribution of the triple of homotopy classes containing these three closed paths.

The problem would already be interesting for a square torus, but one could hope to get the answer as a function of the geometry of the torus.

7. Non-discrete problems

In this section we mention some problems about the behavior of SLE itself, which may be stated without relation to any particular discrete model.

The parametrization of the SLE path by capacity is very convenient for many calculations. However, in some situations, for example when you consider the reversal of the path, this parametrization is not so useful. It would be great if we had an understanding of a parametrization by a kind of Hausdorff measure. Thus we are led to

Problem 7.1. Define a Hausdorff measure on the SLE path which is σ-finite.

We would expect the measure to be a.s. finite on compact subsets of the plane.

That the Hausdorff dimension of the SLE path is $\min\{2, 1+\kappa/8\}$ has been established by Vincent Beffara [10]. When $\kappa < 8$ (in which case the path has zero area), we expect the σ-finite Hausdorff measure to be the Hausdorff measure with respect to the gauge function $\phi(r) = r^d \log\log(1/r)$, where $d = 1+\kappa/8$ is the Hausdorff dimension. This is based on past experience with similar random paths [89]. However, in order to prove that this Hausdorff measure is σ-finite, one should probably find alternative constructions of the measure. In the case $\kappa \leq 4$, where the SLE path is a simple path a.s., one could try to use conformal maps from the unit disk to the two components in the complement of the curve in the upper half plane. If f is such a map, it might be possible to show that the limit of the length measure of the image of the circle $r\,\partial\mathbb{U}$, rescaled appropriately, has a limit as $r \nearrow 1$. Another approach, which was discussed by Tom Kennedy [38], would be to study the α-variation of the SLE path, though this seems hard to handle.

One may also consider other measures of growth for the SLE path. For example, when $\kappa > 4$, we may study the area of the SLE hull. It would be interesting to study the various relations between different measures of growth.

It is also natural to ask what kind of sets are visited by the SLE path. More precisely:

Problem 7.2. Fix $\kappa < 8$. Find necessary or sufficient conditions on a deterministic compact set $K \subset \overline{\mathbb{H}}$ to satisfy $\mathbf{P}\big[K \cap \gamma \neq \emptyset\big] > 0$, where γ is the SLE_κ path.

The case $K \subset \mathbb{R}$ is of particular interest.

When $\kappa = 8/3$ and $\mathbb{H} \setminus K$ is simply connected, there is a simple explicit formula [58] for $\mathbf{P}\big[\gamma \cap K \neq \emptyset\big]$. It is not clear if such formulas are also available for other values of κ. Wendelin Werner [96] proved the existence of a random collection of $\mathrm{SLE}_{8/3}$-like loops with some wonderful properties. In particular, the expected number of loops which separate two boundary components of an annulus is conformally invariant, and therefore a function of the conformal modulus of the annulus. However, this function is not known explicitly.

Many of the random interfaces which are known or believed to converge to SLE are reversible, in the sense that the reversed path has the same law as the original path (with respect to a slightly modified setup). This motivates the following problem from [76].

Problem 7.3. Let γ be the chordal SLE_κ path, where $\kappa \leq 8$. Prove that up to reparametrization, the image of γ under inversion in the unit circle (that is, the map $z \mapsto 1/\bar{z}$) has the same law as γ itself.

The reason that we restrict to the case $\kappa \leq 8$ is that this is false when $\kappa > 8$ (as will be proved in a forthcoming joint paper with Steffen Rohde). Indeed, there are no known models from physics that are believed to be related to SLE_κ when $\kappa > 8$. Sheffield (personal communication) expects that at least in the case $\kappa < 4$ Problem 7.3 can be answered by studying the relationship between the Gaussian free field and SLE.

Acknowledgments. Greg Lawler, Wendelin Werner and Steffen Rohde have collaborated with me during the early stages of the development of SLE. Without them the subject would not be what it is today. I wish to thank Itai Benjamini, Gil Kalai, Richard Kenyon, Scott Sheffield, Jeff Steif and David Wilson for numerous inspiring conversations. Thanks are also due to Yuval Peres for useful advice, especially concerning Problem 7.1.

References

[1] Alexander, K. S., The RSW theorem for continuum percolation and the CLT for Euclidean minimal spanning trees. *Ann. Appl. Probab.* **6** (2) (1996), 466–494.

[2] Angel, O., Growth and percolation on the uniform infinite planar triangulation. *Geom. Funct. Anal.* **13** (5) (2003), 935–974.

[3] ——, Scaling of Percolation on Infinite Planar Maps, I. Preprint, 2005; arXiv:math.Pr/0501006.

[4] Barlow, M. T., Fractals, and diffusion-limited aggregation. *Bull. Sci. Math.* **117** (1) (1993), 161–169.

[5] Bauer, R. O., and Friedrich, R. M., On radial stochastic Loewner evolution in multiply connected domains. *J. Funct. Anal.* **237** (2) (2006), 565–588.

[6] ——, Stochastic Loewner evolution in multiply connected domains. *C. R. Math. Acad. Sci. Paris* **339** (8) (2004), 579–584.

[7] ——, On Chordal and Bilateral SLE in multiply connected domains. Preprint, 2005; arXiv:math.Pr/0503178.

[8] Baxter, R. J., Kelland, S. B., and Wu, F. Y., Equivalence of the Potts model or Whitney polynomial with an ice-type model. *J. Phys. A* **9** (1976), 397–406.

[9] Beffara, V., Critical percolation on other lattices. Talk at the Fields Institute, 2005; http://www.fields.utoronto.ca/audio/05-06/.

[10] ——, The dimension of the SLE curves. Preprint, 2002; arXiv:math.Pr/0211322.

[11] ——, Cardy's formula on the triangular lattice, the easy way. Preprint, 2005; http://www.umpa.ens-lyon.fr/˜vbeffara/files/Proceedings-Toronto.pdf.

[12] Beffara, V., and Sidoravicius, V., Percolation theory. Preprint, 2005; arXiv:math.Pr/0507220.

[13] Benjamini, I., Kalai, G., and Schramm, O., Noise sensitivity of Boolean functions and applications to percolation. *Inst. Hautes Études Sci. Publ. Math.* **90** (1999), 5–43.

[14] Benjamini, I., and Schramm, O., Conformal invariance of Voronoi percolation. *Comm. Math. Phys.* **197** (1) (1998), 75–107.

[15] Bollobás, B., and Riordan, O., The critical probability for random Voronoi percolation in the plane is 1/2. *Probab. Theory Related Fields* **136** (2006), 417–468.

[16] Bousquet-Melou, M., and Schaeffer, G., The degree distribution in bipartite planar maps: applications to the Ising model. Preprint, 2002; arXiv:math.CO/0211070.

[17] Brydges, D. C., and Imbrie, J. Z., Branched polymers and dimensional reduction. *Ann. of Math.* (2) **158** (3) (2003), 1019–1039.

[18] Camia, F., Fontes, L. R. G., and Newman, C. M., The Scaling Limit Geometry of Near-Critical 2D Percolation. Preprint, 2005; cond-mat/0510740.

[19] Camia, F., and Newman, C. M., The Full Scaling Limit of Two-Dimensional Critical Percolation. Preprint, 2005; arXiv:math.Pr/0504036.

[20] Cardy, J., Critical percolation in finite geometries. *J. Phys. A* **25** (4) (1992), L201–L206.

[21] ——, SLE for theoretical physicists. *Ann. Physics* **318** (1) (2005), 81–118.

[22] Carleson, L., and Makarov, N., Aggregation in the plane and Loewner's equation. *Comm. Math. Phys.* **216** (3) (2001), 583–607.

[23] Chassaing, P., and Schaeffer, G., Random planar lattices and integrated superBrownian excursion. *Probab. Theory Related Fields* **128** (2) (2004), 161–212.

[24] den Nijs, M., A relation between the temperature exponents of the eight-vertex and the q-state potts model. *J. Phys. A* **12** (1979), 1857–1868.

[25] Dubédat, J., Excursion decompositions for SLE and Watts' crossing formula. *Probab. Theory Related Fields* **134** (3) (2006), 453–488.

[26] Dudley, R. M., *Real analysis and probability*. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1989.

[27] Duplantier, B., and Kwon, K.-H., Conformal invariance and intersection of random walks. *Phys. Rev. Lett.* **61** (1988), 2514–2517.

[28] Fortuin, C. M., and Kasteleyn, P. W., On the random-cluster model. I. Introduction and relation to other models. *Physica* **57** (1972), 536–564.

[29] Greenberg, L., and Ioffe, D., On an invariance principle for phase separation lines. *Ann. Inst. H. Poincaré Probab. Statist.* **41** (5) (2005), 871–885.

[30] Grimmett, G., *Percolation*. Second ed., Grundlehren Math. Wiss. 321, Springer-Verlag, Berlin 1999.

[31] Häggström, O., Peres, Y., and Steif, J. E., Dynamical percolation. *Ann. Inst. H. Poincaré Probab. Statist.* **33** (4) (1997), 497–528.

[32] Hara, T., and Slade, G., Self-avoiding walk in five or more dimensions. I. The critical behaviour. *Comm. Math. Phys.* **147** (1) (1992), 101–136.

[33] Harris, T. E., A lower bound for the critical probability in a certain percolation process. *Proc. Cambridge Philos. Soc.* **56** (1960), 13–20.

[34] Hastings, M. B., and Levitov, L. S., Laplacian growth as one-dimensional turbulence. *Physica D* **116** (1998), 244–252.

[35] Itzykson, C., and Drouffe, J.-M., *Statistical field theory.* Vol. 1. From Brownian motion to renormalization and lattice gauge theory, Cambridge Monogr. Math. Phys., Cambridge University Press, Cambridge 1989.

[36] Kager, W., and Nienhuis, B., A guide to stochastic Löwner evolution and its applications. *J. Statist. Phys.* **115** (5–6) (2004), 1149–1229.

[37] Kalai, G., and Safra, S., Threshold phenomena and influence. In *Computational Complexity and Statistical Physics* (A. G. Percus, G. Istrate and C. Moore, eds.), St. Fe Inst. Stud. Sci. Complex., Oxford University Press, New York 2006, 25–60.

[38] Kennedy, T., Monte Carlo comparisons of the self-avoiding walk and SLE as parameterized curves. Preprint, 2005; arXiv:math.Pr/0510604.

[39] Kenyon, R., The asymptotic determinant of the discrete Laplacian. *Acta Math.* **185** (2) (2000), 239–286.

[40] ——, Conformal invariance of domino tiling. *Ann. Probab.* **28** (2) (2000), 759–795.

[41] ——, Long-range properties of spanning trees. Probabilistic techniques in equilibrium and nonequilibrium statistical physics. *J. Math. Phys.* **41** (3) (2000), 1338–1363.

[42] ——, Dominos and the Gaussian free field. *Ann. Probab.* **29** (3) (2001), 1128–1137.

[43] Kesten, H., The critical probability of bond percolation on the square lattice equals $1/2$. *Comm. Math. Phys.* **74** (1) (1980), 41–59.

[44] ——, Upper bounds for the growth rate of DLA. *Phys. A* **168** (1) (1990), 529–535.

[45] ——, Some highlights of percolation. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. I, Higher Ed. Press, Beijing 2002, 345–362.

[46] Knizhnik, V. G., Polyakov, A. M., and Zamolodchikov, A. B., Fractal structure of 2D-quantum gravity. *Modern Phys. Lett. A* **3** (8) (1988), 819–826.

[47] Kozma, G., Scaling limit of loop erased random walk – a naive approach. Preprint 2002, arXiv:math.Pr/0212338.

[48] ——, The scaling limit of loop-erased random walk in three dimensions. Preprint 2005, arXiv:math.Pr/0508344.

[49] Langlands, R., Pouliot, P., and Saint-Aubin, Y., Conformal invariance in two-dimensional percolation. *Bull. Amer. Math. Soc.* (*N.S.*) **30** (1) (1994), 1–61.

[50] Lawler, G. F., The dimension of the frontier of planar Brownian motion. *Electron. Comm. Probab.* **1** (5) (1996), 29–47 (electronic).

[51] ——, A self-avoiding random walk. *Duke Math. J.* **47** (3) (1980), 655–693.

[52] ——, *Conformally invariant processes in the plane*. Math. Surveys Monogr. 114, Amer. Math. Soc., Providence, RI, 2005.

[53] Lawler, G. F., Schramm, O., and Werner, W., Values of Brownian intersection exponents. I. Half-plane exponents. *Acta Math.* **187** (2) (2001), 237–273.

[54] ——, Values of Brownian intersection exponents. II. Plane exponents. *Acta Math.* **187** (2) (2001), 275–308.

[55] ——, Values of Brownian intersection exponents. III. Two-sided exponents. *Ann. Inst. H. Poincaré Probab. Statist.* **38** (1) (2002), 109–123.

[56] ——, One-arm exponent for critical 2D percolation. *Electron. J. Probab.* **7** (2) (2002), 13 pp. (electronic).

[57] ——, Sharp estimates for Brownian non-intersection probabilities. *In and out of equilibrium* (Mambucaba, 2000), Progr. Probab. 51, Birkhäuser Boston, Boston, MA, 2002, pp. 113–131.

[58] ——, Conformal restriction: the chordal case. *J. Amer. Math. Soc.* **16** (4) (2003), 917–955 (electronic).

[59] ——, Conformal invariance of planar loop-erased random walks and uniform spanning trees. *Ann. Probab.* **32** (1B) (2004), 939–995.

[60] ——, On the scaling limit of planar self-avoiding walk. In *Fractal geometry and applications: a jubilee of Benoît Mandelbrot*, Part 2, Proc. Sympos. Pure Math. 72, Amer. Math. Soc., Providence, RI, 2004, 339–364.

[61] Lawler, G. F., and Werner, W., Intersection exponents for planar Brownian motion. *Ann. Probab.* **27** (4) (1999), 1601–1642.

[62] ——, Universality for conformally invariant intersection exponents. *J. Eur. Math. Soc.* (*JEMS*) **2** (4) (2000), 291–328.

[63] ——, The Brownian loop soup. *Probab. Theory Related Fields* **128** (4) (2004), 565–588.

[64] Lévy, P., *Processus Stochastiques et Mouvement Brownien. Suivi d'une note de M. Loève*. Gauthier-Villars, Paris 1948.

[65] Löwner, K. (C. Loewner), Untersuchungen über schlichte konforme Abbildungen des Einheitskreises, I. *Math. Ann.* **89** (1923), 103–121.

[66] Lyons, R., A bird's-eye view of uniform spanning trees and forests. In *Microsurveys in discrete probability* (Princeton, NJ, 1997), Amer. Math. Soc., Providence, RI, 1998, 135–162.

[67] Madras, N., and Slade, G., *The self-avoiding walk*. Probab. Appl., Birkhäuser, Boston, MA, 1993.

[68] Marckert, J. F., and Mokkadem, A., Limit of Normalized Quadrangulations: the Brownian map. *Ann. Probab.* **34** (2006), 2144–2202.

[69] McCoy, B. M., and Wu, T. T., *The two-dimensional Ising model*. Harvard University Press, Cambridge, Mass., 1973.

[70] Meester, R., and Roy, R., *Continuum percolation*. Cambridge Tracts in Math. 119, Cambridge University Press, Cambridge 1996.

[71] Naddaf, A., and Spencer, T., On homogenization and scaling limit of some gradient perturbations of a massless free field. *Comm. Math. Phys.* **183** (1) (1997), 55–84.

[72] Nienhuis, B., Exact critical point and critical exponents. *Phys. Rev. Lett.* **49** (1982), 1062–1065.

[73] ——, Coulomb gas description of 2-d critical behaviour. *J. Statist. Phys.* **34** (1984), 731–761.

[74] Pemantle, R., Choosing a spanning tree for the integer lattice uniformly. *Ann. Probab.* **19** (4) (1991), 1559–1574.

[75] Pfister, C.-E., and Velenik, Y., Interface, surface tension and reentrant pinning transition in the 2D Ising model. *Comm. Math. Phys.* **204** (2) (1999), 269–312.

[76] Rohde, S., and Schramm, O., Basic properties of SLE. *Ann. of Math.* (2) **161** (2) (2005), 883–924.

[77] Roy, R., The Russo-Seymour-Welsh theorem and the equality of critical densities and the "dual" critical densities for continuum percolation on $\mathbf{R}^2$. *Ann. Probab.* **18** (4) (1990), 1563–1575.

[78] Russo, L., A note on percolation. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **43** (1) (1978), 39–48.

[79] Schramm, O., Scaling limits of loop-erased random walks and uniform spanning trees. *Israel J. Math.* **118** (2000), 221–288.

[80] Schramm, O., and Sheffield, S., Harmonic explorer and its convergence to SLE_4. *Ann. Probab.* **33** (6) (2005), 2127–2148.

[81] ——, Contour lines of the 2D Gaussian free field. In preparation, 2006.

[82] Schramm, O., and Steif, J. E., Quantitative noise sensitivity and exceptional times for percolation. Preprint, 2005; arXiv:math.Pr/0504586.

[83] Schramm, O., and Wilson, D. B., SLE coordinate changes. *New York J. Math.* **11** (2005), 659–669.

[84] Seymour, P. D., and Welsh, D. J. A., Percolation probabilities on the square lattice. Advances in graph theory (Cambridge Combinatorial Conf., Trinity College, Cambridge, 1977); *Ann. Discrete Math.* **3** (1978), 227–245.

[85] Sheffield, S., Gaussian free fields for mathematicians. Preprint, 2003; arXiv:math. Pr/0312099.

[86] Slade, G., Lattice trees, percolation and super-Brownian motion. In *Perplexing problems in probability*, Progr. Probab. 44, Birkhäuser, Boston, MA, 1999, 35–51.

[87] Smirnov, S., Critical percolation in the plane: conformal invariance, Cardy's formula, scaling limits. *C. R. Acad. Sci. Paris Sér. I Math.* **333** (3) (2001), 239–244.

[88] Smirnov, S., and Werner, W., Critical exponents for two-dimensional percolation. *Math. Res. Lett.* **8** (5–6) (2001), 729–744.

[89] Taylor, S. J., The measure theory of random fractals. *Math. Proc. Cambridge Philos. Soc.* **100** (3) (1986), 383–406.

[90] Tsirelson, B., Fourier-Walsh coefficients for a coalescing flow (discrete time). TAU RP-SOR-99-02, 1999; arXiv:math.Pr/9903068.

[91] ——, Scaling limit of Fourier-Walsh coefficients (a framework). TAU RP-SOR-99-04, 1999; arXiv:math.Pr/9903121.

[92] Watts, G. M. T., A crossing probability for critical percolation in two dimensions. *J. Phys. A* **29** (14) (1996), L363–L368.

[93] Werner, W., SLEs as boundaries of clusters of Brownian loops. *C. R. Math. Acad. Sci. Paris* **337** (7) (2003), 481–486.

[94] ——, Random planar curves and Schramm-Loewner evolutions. In *Lectures on probability theory and statistics*, Lecture Notes in Math. 1840, Springer-Verlag, Berlin 2004, 107–195.

[95] ——, Conformal restriction and related questions. *Probab. Surv.* **2** (2005), 145–190 (electronic).

[96] ——, The conformally invariant measure on self-avoiding loops. Preprint, 2005; arXiv:math. Pr/0511605.

[97] ——, Conformal restriction properties. In *Proceedings of the International Congress of Mathematicians* (Madrid, 2006), Volume III, EMS Publishing House, Zürich 2006, 741–762.

[98] Wierman, J. C., Bond percolation on honeycomb and triangular lattices. *Adv. in Appl. Probab.* **13** (2) (1981), 298–313.

[99] Wilson, D. B., Generating random spanning trees more quickly than the cover time. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing* (Philadelphia, PA, 1996), ACM , New York 1996, 296–303.

[100] Witten, T. A., and Sander, L. M., Diffusion-limited aggregation. *Phys. Rev. B* (3) **27** (9) (1983), 5686–5697.

[101] Zhan, D., Stochastic Loewner evolution in doubly connected domains. *Probab. Theory Related Fields* **129** (3) (2004), 340–380.

[102] Ziff, R. M., Exact critical exponent for the shortest-path scaling function in percolation. *J. Phys. A* **32** (43) (1999), L457–L459.

Microsoft Corporation, Redmond, Washington, U.S.A.

Increasing and decreasing subsequences and their variants

Richard P. Stanley

Abstract. We survey the theory of increasing and decreasing subsequences of permutations. Enumeration problems in this area are closely related to the RSK algorithm. The asymptotic behavior of the expected value of the length $\mathrm{is}(w)$ of the longest increasing subsequence of a permutation w of $1, 2, \ldots, n$ was obtained by Vershik–Kerov and (almost) by Logan–Shepp. The entire limiting distribution of $\mathrm{is}(w)$ was then determined by Baik, Deift, and Johansson. These techniques can be applied to other classes of permutations, such as involutions, and are related to the distribution of eigenvalues of elements of the classical groups. A number of generalizations and variations of increasing/decreasing subsequences are discussed, including the theory of pattern avoidance, unimodal and alternating subsequences, and crossings and nestings of matchings and set partitions.

Mathematics Subject Classification (2000). Primary 05A05, 05A06; Secondary 60C05.

Keywords. Increasing subsequence, decreasing subsequence, Young tableau, RSK algorithm, Tracy–Widom distribution, GUE model, pattern avoidance, unimodal subsequence, alternating subsequence, matching, oscillating tableau.

1. Introduction

Let $\mathfrak{S}_n$ denote the symmetric group of all permutations of $[n] := \{1, 2, \ldots, n\}$. We write permutations $w \in \mathfrak{S}_n$ as *words*, i.e., $w = a_1 a_2 \ldots a_n$, where $w(i) = a_i$. An *increasing subsequence* of w is a subsequence $a_{i_1} \ldots a_{i_k}$ satisfying $a_{i_1} < \cdots < a_{i_k}$, and similarly for *decreasing subsequence*. For instance, if $w = 5642713$, then 567 is an increasing subsequence and 543 is a decreasing subsequence. Let $\mathrm{is}(w)$ (respectively, $\mathrm{ds}(w)$) denote the length (number of terms) of the longest increasing (respectively, decreasing) subsequence of w. If $w = 5642713$ as above, then $\mathrm{is}(w) = 3$ (corresponding to 567) and $\mathrm{ds}(w) = 4$ (corresponding to 5421 or 6421). A nice interpretation of increasing subsequences in terms of the one-person card game *patience sorting* is given by Aldous and Diaconis [4]. Further work on patience sorting was undertaken by Burstein and Lankham [33], [34], [35]. Connections between patience sorting and airplane boarding times were found by Bachmat et al. [12], [13] and between patience sorting and disk scheduling by Bachmat [11].

The subject of increasing and decreasing subsequences began in 1935, and there has been much recent activity. There have been major breakthroughs in understanding

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

the distribution of $\mathrm{is}(w)$, $\mathrm{ds}(w)$, and related statistics on permutations, and many unexpected and deep connections have been obtained with such areas as representation theory and random matrix theory. A number of excellent survey papers have been written on various aspects of these developments, e.g., [4], [40], [60], [108], [115]; the present paper will emphasize the connections with combinatorics.

In Section 2 we give some basic enumerative results related to increasing/decreasing subsequences and show their connection with the RSK algorithm from algebraic combinatorics. The next two sections are devoted to the distribution of $\mathrm{is}(w)$ for $w \in \mathfrak{S}_n$, a problem first raised by Ulam. In Section 3 we deal with the expectation of $\mathrm{is}(w)$ for $w \in \mathfrak{S}_n$, culminating in the asymptotic formula of Logan–Shepp and Vershik–Kerov. We turn to the entire limiting distribution of $\mathrm{is}(w)$ in Section 4. The main result is the determination of this limiting distribution by Baik, Deift, and Johansson to be a (suitably scaled) Tracy–Widom distribution. The Tracy–Widom distribution originally arose in the theory of random matrices, so the result of Baik et al. opens up unexpected connections between increasing/decreasing subsequences and random matrices.

Much of the theory of increasing/decreasing subsequences of permutations in $\mathfrak{S}_n$ carries over to permutations in certain subsets of $\mathfrak{S}_n$, such as the set of involutions. This topic is discussed in Section 5. In particular, analogues of the Baik–Deift–Johansson theorem were given by Baik and Rains. In Section 6 we explain how the previous results are related to the distribution of eigenvalues in matrices belonging to the classical groups.

The remaining three sections are concerned with analogues and extensions of increasing/decreasing subsequences of permutations. Section 7 deals with pattern avoidance, where increasing/decreasing subsequence are replaced with other "patterns." In Section 8 we consider unimodal and alternating subsequences of permutations, and in Section 9 we replace permutations with (complete) matchings. For matchings the role of increasing and decreasing subsequences is played by crossings and nestings.

Acknowledgment. I am grateful to Percy Deift, Persi Diaconis, Craig Tracy and Herb Wilf for providing some pertinent references.

2. Enumeration and the RSK algorithm

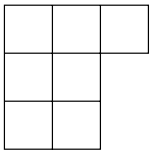
The first result on increasing and decreasing subsequences is a famous theorem of Erdős and Szekeres [43].

Theorem 1. *Let $p, q \geq 1$. If $w \in \mathfrak{S}_{pq+1}$, then either* $\mathrm{is}(w) > p$ *or* $\mathrm{ds}(w) > q$.

This result arose in the context of the problem of determining the least integer $f(n)$ so that any $f(n)$ points in general position in the plane contain an n-element subset S in convex position (i.e., every element of S is a vertex of the convex hull of S). A recent

survey of this problem was given by Morris and Soltan [77]. Seidenberg [92] gave an exceptionally elegant proof of Theorem 1 based on the pigeonhole principle which has been reproduced many times, e.g., Gardner [46, Ch. 11, §7]. For a mathematical game based on Theorem 1, see the papers [2], [55].

Theorem 1 is best possible in that there exists $w \in \mathfrak{S}_{pq}$ with $\mathrm{is}(w) = p$ and $\mathrm{ds}(w) = q$. Schensted [89] found a quantitative strengthening of this result based on his rediscovery of an algorithm of Robinson [84] which has subsequently become a central algorithm in algebraic combinatorics. To describe Schensted's result, let $\lambda = (\lambda_1, \lambda_2, \dots)$ be a partition of $n \geq 0$, denoted $\lambda \vdash n$ or $|\lambda| = n$. Thus $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ and $\sum \lambda_i = n$. The (*Young*) *diagram*) of a partition λ is a left-justified array of squares with λ_i squares in the ith row. For instance, the Young diagram of (3, 2, 2) is given by



A *standard Young tableau* (SYT) of shape $\lambda \vdash n$ is obtained by placing the integers $1, 2, \dots, n$ (each appearing once) into the squares of the diagram of λ (with one integer in each square) such that every row and column is increasing. For example, an SYT of shape (3, 2, 2) is given by

$$\begin{array}{ccc} 1 & 3 & 6 \\ 2 & 5 & \\ 4 & 7 & . \end{array}$$

Let f^λ denote the number of SYT of shape λ. The quantity f^λ has a number of additional combinatorial interpretations [99, Prop. 7.10.3]. It also has a fundamental algebraic interpretation which suggests (via equation (9) below) a close connection between representation theory and increasing/decreasing subsequences. Namely, the (complex) irreducible representations F^λ of $\mathfrak{S}_n$ are indexed in a natural way by partitions $\lambda \vdash n$, and then

$$f^\lambda = \dim F^\lambda. \tag{1}$$

In particular (by elementary representation theory),

$$\sum_{\lambda \vdash n} (f^\lambda)^2 = n!. \tag{2}$$

See Section 6 for more on the connections between increasing/decreasing subsequences and representation theory. MacMahon [74, p. 175] was the first to give a formula for f^λ (in the guise of counting "lattice permutations" rather than SYT), and later Frame, Robinson, and Thrall [45] simplified MacMahon's formula, as follows. Let u be a square of the diagram of λ, denoted $u \in \lambda$. The *hook length* $h(u)$ of (or

at) u is the number of squares directly to the right or directly below u, counting u itself once. For instance, if $\lambda = (3, 2, 2)$ then the hook lengths are given by

$$\begin{array}{ccc} 5 & 4 & 1 \\ 3 & 2 & \\ 2 & 1 & . \end{array}$$

The *hook-length formula* of Frame, Robinson, and Thrall asserts that if $\lambda \vdash n$, then

$$f^\lambda = \frac{n!}{\prod_{u \in \lambda} h(u)}. \tag{3}$$

For instance,

$$f^{(3,2,2)} = \frac{7!}{5 \cdot 4 \cdot 1 \cdot 3 \cdot 2 \cdot 2 \cdot 1} = 21.$$

The *RSK algorithm* gives a bijection between $\mathfrak{S}_n$ and pairs (P, Q) of SYT of the same shape $\lambda \vdash n$. This algorithm is named after Gilbert de Beauregard Robinson, who described it in a rather vague form [84, §5] (subsequently analyzed by van Leeuwen [70, §7]), Craige Schensted [89], and Donald Knuth [65]. For further historical information see [99, Notes to Ch. 7]. The basic operation of the RSK algorithm is *row insertion*, i.e., inserting an integer i into a tableau T with distinct entries and with increasing rows and columns. (Thus T satisfies the conditions of an SYT except that its entries can be any distinct integers, not just $1, 2, \ldots, n$.) The process of row inserting i into T produces another tableau, denoted $T \leftarrow i$, with increasing rows and columns. If S is the set of entries of T, then $S \cup \{i\}$ is the set of entries of $T \leftarrow i$. We define $T \leftarrow i$ recursively as follows.

- If the first row of T is empty or the largest entry of the first row of T is less than i, then insert i at the end of the first row.
- Otherwise, i replaces (or *bumps*) the smallest element j in the first row satisfying $j > i$. We then insert j into the second row of T by the same procedure.

For further details concerning the definition and basic properties of $T \leftarrow i$ see e.g. [88, Ch. 3], [99, §7.11].

Let $w = a_1 a_2 \ldots a_n \in \mathfrak{S}_n$, and let $\emptyset$ denote the empty tableau. Define

$$P_i = P_i(w) = (\cdots((\emptyset \leftarrow a_1) \leftarrow a_2) \leftarrow \cdots \leftarrow a_i.$$

That is, we start with the empty tableau and successively row insert $a_1, a_2, \ldots, a_i$. Set $P = P(w) = P_n(w)$. Define $Q_0 = \emptyset$, and once Q_{i-1} is defined let $Q_i = Q_i(w)$ be obtained from Q_{i-1} by inserting i (without changing the position of any of the entries of Q_{i-1}) so that Q_i and P_i have the same shape. Set $Q = Q(w) = Q_n(w)$,

and finally define the output of the RSK algorithm applied to w to be the pair (P, Q), denoted $w \xrightarrow{\text{rsk}} (P, Q)$. For instance, if $w = 31542 \in \mathfrak{S}_5$, then we obtain

$$P_1(w) = 3, \quad P_2(w) = \begin{array}{ll} 1 \\ 3\,, \end{array} \quad P_3(w) = \begin{array}{lll} 1 & 5 \\ 3\,, \end{array}$$

$$P_4(w) = \begin{array}{ll} 1 & 4 \\ 3 & 5\,, \end{array} \quad P = P_5(w) = \begin{array}{ll} 1 & 2 \\ 3 & 4 \\ 5\,. \end{array}$$

It follows that

$$Q = \begin{array}{ll} 1 & 3 \\ 2 & 4 \\ 5\,. \end{array}$$

Note. By a theorem of Schützenberger [90], [99, §7.13] we have

$$Q(w) = P(w^{-1}), \tag{4}$$

so we could have in fact taken this formula as the definition of $Q(w)$.

If $w \xrightarrow{\text{rsk}} (P, Q)$ and P, Q have shape λ, then we also call λ the *shape* of w, denoted $\lambda = \text{sh}(w)$. The *conjugate* partition $\lambda' = (\lambda'_1, \lambda'_2, \dots)$ of λ is the partition whose diagram is the transpose of the diagram of λ. Equivalently, j occurs exactly $\lambda_j - \lambda_{j+1}$ times as a part of λ'. The *length* $\ell(\lambda)$ is the number of (nonzero) parts of λ, so $\ell(\lambda) = \lambda'_1$. The fundamental result of Schensted [89] connecting RSK with increasing and decreasing subsequences is the following.

Theorem 2. *Let $w \in \mathfrak{S}_n$, and suppose that* $\text{sh}(w) = \lambda$. *Then*

$$\text{is}(w) = \lambda_1, \tag{5}$$

$$\text{ds}(w) = \lambda'_1. \tag{6}$$

Equation (5) is easy to prove by induction since we need only analyze the effect of the RSK algorithm on the first row of the P_i's. On the other hand, equation (6) is based on the following symmetry property of RSK proved by Schensted. If $w = a_1 a_2 \dots a_n$ then let $w^r = a_n \dots a_2 a_1$, the *reverse* of w. We then have

$$w \xrightarrow{\text{rsk}} (P, Q) \implies w^r \xrightarrow{\text{rsk}} (P^t, \text{evac}(Q)^t), \tag{7}$$

where ^{t} denotes transpose and $\text{evac}(Q)$ is a certain tableau called the *evacuation* of Q (first defined by Schützenberger [91]) which we will not define here. Equation (7) shows that if $\text{sh}(w) = \lambda$, then $\text{sh}(w^r) = \lambda'$. Since clearly $\text{is}(w^r) = \text{ds}(w)$, equation (6) follows from (5).

Theorem 2 has several immediate consequences. The first corollary is the Erdős–Szekeres theorem (Theorem 1), for if $\text{sh}(w) = \lambda$, $\text{is}(w) \le p$, and $\text{ds}(w) \le q$, then $\lambda_1 \le p$ and $\lambda'_1 \le q$. Thus the diagram of λ is contained in a $q \times p$ rectangle, so $|\lambda| \le pq$. By the same token we get a quantitative statement that Theorem 1 is best possible.

Corollary 3. *The number of permutations $w \in \mathfrak{S}_{pq}$, where say $p \le q$, satisfying* $\mathrm{is}(w) = p$ *and* $\mathrm{ds}(w) = q$ *is given by*

$$(f^{(p^q)})^2 = \left(\frac{(pq)!}{1^1 2^2 \cdots p^p (p+1)^p \cdots q^p (q+1)^{p-1} \cdots (p+q-1)^1} \right)^2, \qquad (8)$$

where (p^q) denotes the partition with q parts equal to p.

Proof. Let $\lambda = \mathrm{sh}(w)$. If $\mathrm{is}(w) = p$ and $\mathrm{ds}(w) = q$, then $\lambda_1 = p$ and $\lambda_1' = q$. Since $\lambda \vdash pq$, we must have $\lambda = (p^q)$. The number of $v \in \mathfrak{S}_n$ with a fixed shape μ is just $(f^\mu)^2$, the number of pairs (P, Q) of SYT of shape μ. Hence the left-hand side of equation (8) follows. The right-hand side is then a consequence of the hook-length formula (3). □

An interesting result concerning the extremal permutations in the case $p = q$ in Corollary 3 was obtained by Romik [85, Thm. 5]. It can be stated informally as follows. Pick a random permutation $w \in \mathfrak{S}_{p^2}$ satisfying $\mathrm{is}(w) = \mathrm{ds}(w) = p$. Let P_w be the $p^2 \times p^2$ permutation matrix corresponding to w, drawn in the plane so that its corners occupy the points $(\pm 1, \pm 1)$. Then almost surely as $p \to \infty$ the limiting curve enclosing most of the 1's in P_w is given by

$$\{(x, y) \in \mathbb{R}^2 \,:\, (x^2 - y^2)^2 + 2(x^2 + y^2) = 3\}.$$

See Figure 1. In particular, this curve encloses a fraction $\alpha = 0.94545962\ldots$ of the entire square with vertices $(\pm 1, \pm 1)$. The number α can be expressed in terms of elliptic integrals as

$$\alpha = 2 \int_0^1 \frac{1}{\sqrt{(1-t^2)(1-(t/3)^2)}} dt - \frac{3}{2} \int_0^1 \sqrt{\frac{1-(t/3)^2}{1-t^2}} dt.$$

Compare with the case of *any* $w \in \mathfrak{S}_n$, when clearly the limiting curve encloses the entire square with vertices $(\pm 1, \pm 1)$. For further information related to permutations $w \in \mathfrak{S}_{p^2}$ satisfying $\mathrm{is}(w) = \mathrm{ds}(w) = p$, see the paper [80] of Pittel and Romik.

Clearly Corollary 3 can be extended to give a formula [99, Cor. 7.23.18] for the number

$$g_{pq}(n) = \#\{w \in \mathfrak{S}_n \,:\, \mathrm{is}(w) = p,\ \mathrm{ds}(w) = q\},$$

namely,

$$g_{pq}(n) = \sum_{\substack{\lambda \vdash n \\ \lambda_1 = p,\ \lambda_1' = q}} (f^\lambda)^2. \qquad (9)$$

The usefulness of this formula may not be readily apparent, but Theorem 7 below is an example of its utility.

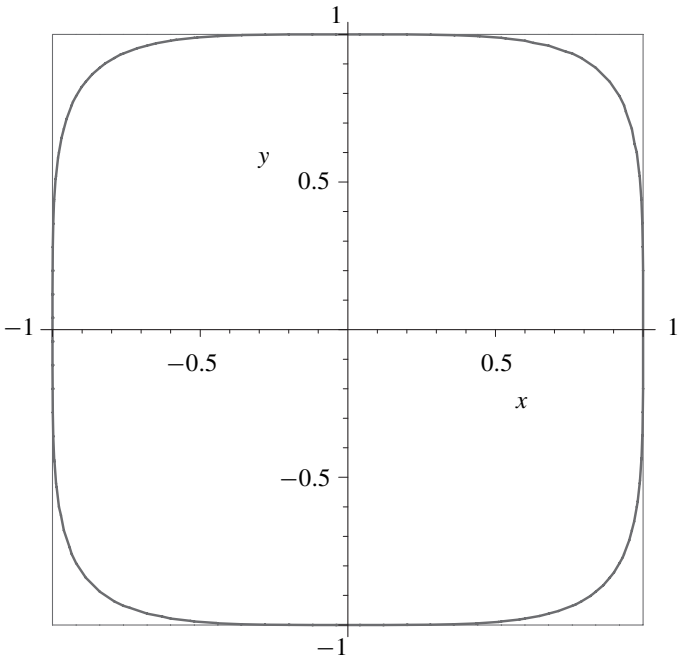


Figure 1. The curve $(x^2 - y^2)^2 + 2(x^2 + y^2) = 3$.

3. Expectation of is(w)

A further application of Theorem 2 concerns the distribution of the function is(w) as w ranges over $\mathfrak{S}_n$. The problem of obtaining information on this distribution was first raised by Ulam [109, §11.3] in the context of Monte Carlo calculations. In particular, one can ask for information on the expectation $E(n)$ of is(w) for $w \in \mathfrak{S}_n$, i.e.,

$$E(n) = \frac{1}{n!} \sum_{w \in \mathfrak{S}_n} \mathrm{is}(w).$$

Ulam mentions the computations of E. Neighbor suggesting that $E(n)$ is about $1.7\sqrt{n}$. Numerical experiments by Baer and Brock [14] suggested that $E(n) \sim 2\sqrt{n}$ might be closer to the truth. The Erdős–Szekeres theorem (Theorem 1) implies immediately that $E(n) \geq \sqrt{n}$, since

$$\frac{1}{2}(\mathrm{is}(w) + \mathrm{is}(w^r)) \geq \sqrt{\mathrm{is}(w)\,\mathrm{is}(w^r)} = \sqrt{\mathrm{is}(w)\,\mathrm{ds}(w)} \geq \sqrt{n}.$$

Hammersley [56] was the first person to seriously consider the question of estimating $E(n)$. He showed that if

$$c = \lim_{n \to \infty} \frac{E(n)}{\sqrt{n}},$$

then c exists and satisfies

$$\frac{\pi}{2} \leq c \leq e.$$

He also gave a heuristic argument that $c = 2$, in agreement with the experiments of Baer and Brock.

The next progress on Ulam's problem was based on Schensted's theorem (Theorem 2). It follows from this result that

$$E(n) = \frac{1}{n!} \sum_{\lambda \vdash n} \lambda_1 (f^\lambda)^2. \tag{10}$$

Now the RSK algorithm itself shows that

$$n! = \sum_{\lambda \vdash n} (f^\lambda)^2, \tag{11}$$

in agreement with (2). Since the number of terms in the sum on the right-hand side of (11) is very small compared to $n!$, the maximum value of f^λ for $\lambda \vdash n$ is close to $\sqrt{n!}$. Let λ^n be a value of $\lambda \vdash n$ for which f^λ is maximized. Then by (10) we see that a close approximation to $E(n)$ is given by

$$\begin{aligned} E(n) &\approx \frac{1}{n!} (\lambda^n)_1 (f^{\lambda^n})^2 \\ &\approx (\lambda^n)_1. \end{aligned}$$

This heuristic argument shows the importance of determining the partition λ^n maximizing the value of f^λ for $\lambda \vdash n$.

We are only really interested in the behavior of λ^n as $n \to \infty$, so let us normalize the Young diagram of any partition λ to have area one. Thus each square of the diagram has length $1/\sqrt{n}$. Let the upper boundary of (the diagram of) λ be the y-axis directed to the right, and the left boundary be the x-axis directed down. As $n \to \infty$ it is not unreasonable to expect that the boundary of the partition λ^n will approach some limiting curve $y = \Psi(x)$. If this curve intersects the x-axis at $x = b$, then it is immediate that

$$c := \lim_{n \to \infty} \frac{E(n)}{\sqrt{n}} \geq b.$$

We cannot be sure that $b = c$ since conceivably the first few parts of λ^n are much larger than the other parts, so these parts would "stretch out" the curve $y = \Psi(x)$ along the x-axis.

It was shown independently by Vershik–Kerov [110] and Logan–Shepp [71] that $y = \Psi(x)$ indeed does exist and is given parametrically by

$$\begin{aligned} x &= y + 2\cos\theta, \\ y &= \frac{2}{\pi}(\sin\theta - \theta\cos\theta), \end{aligned}$$

for $0 \le \theta \le \pi$. See Figure 2, where we have placed the coordinate axes in their customary locations.

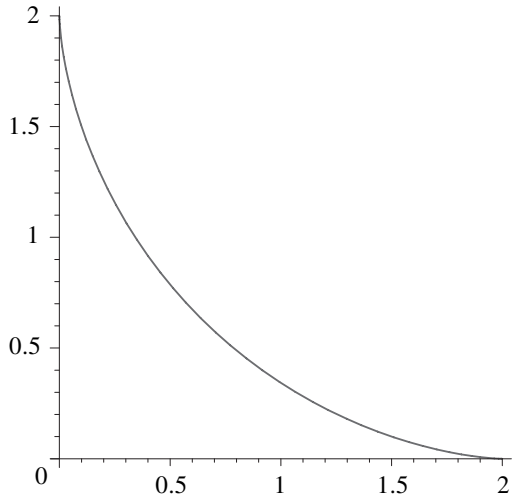


Figure 2. The curve $y = \Psi(x)$.

Logan–Shepp and Vershik–Kerov obtain the curve $\Psi(x)$ as a solution to a variational problem. If (x, y) is a point in the region A enclosed by the curve and the coordinate axes, then the (normalized) hook-length at (x, y) is $f(x) - y + f^{-1}(y) - x$. By equation (3) we maximize f^λ by minimizing $\prod_{u\in\lambda} h(u)$. Hence in the limit we wish to minimize $I(f) = \iint_A \log(f(x) - y + f^{-1}(y) - x)dx\,dy$, subject to the normalization $\iint_A dx\,dy = 1$. It is shown in [71] and [110] that $f = \Psi$ is the unique function minimizing $I(f)$ (and moreover $I(\Psi) = -1/2$).

Note. If we extend the curve $y = \Psi(x)$ to include the x-axis for $x \ge 2$ and the y-axis for $y \ge 2$, and then rotate it 45° counterclockwise, then we obtain the curve

$$\Omega(x) = \begin{cases} \frac{2}{\pi}(x \arcsin(x/2) + \sqrt{4 - x^2}), & |x| \le 2, \\ |x|, & |x| \ge 2. \end{cases}$$

This form of the limiting curve is more convenient for some purposes [62], [63], [64], such as surprising connections with the separation of zeros of orthogonal polynomials.

We see immediately from the equations for $\Psi(x)$ that it intersects the x-axis at $x = 2$, so $c \ge 2$. By a simple but clever use of the RSK algorithm Vershik and Kerov show in their paper that $c \le 2$, so we conclude that

$$E(n) \sim 2\sqrt{n}. \tag{12}$$

Different proofs that $E(n) \sim 2\sqrt{n}$ were later given by Aldous and Diaconis [4], Groeneboom [51], Johansson [58], and Sepäläinen [93]. The proof of Aldous and Diaconis is based on an interacting particle process for which the number of particles remaining after n steps has the same distribution as is_n. Their proof is known in the language of statistical physics as a *hydrodynamic limit* argument. See [5, §3] for a brief survey.

We should remark that the curve $y = \Psi(x)$ is not merely the limiting curve for the partition *maximizing* f^λ; it is also the limiting curve for the *typical* shape of a permutation $w \in \mathfrak{S}_n$. A remarkable refinement of this fact is due to Kerov [57], [61], [64, §0.3.4], who shows that the deviation of a Young diagram from the expected limit converges in probability to a certain Gaussian process. A different kind of refinement is due to Borodin, Okounkov, and Olshanski [31, Thm. 1], who obtain more detailed local information about a typical shape λ than is given by $\Psi(x)$.

4. Distribution of is(w)

A major breakthrough in understanding the behavior of is(w) was achieved in 1999 by Baik, Deift, and Johansson [15]. They determined the entire limiting distribution of is(w) as $n \to \infty$. It turns out to be given by the (suitably scaled) Tracy–Widom distribution, which had first appeared in connection with the distribution of the largest eigenvalue of a random hermitian matrix.

To describe these results, write is_n for the function $\mathrm{is}\colon \mathfrak{S}_n \to \mathbb{Z}$. Let $u(x)$ denote the unique solution to the nonlinear second order differential equation

$$u''(x) = 2u(x)^3 + xu(x), \tag{13}$$

subject to the condition

$$u(x) \sim -\frac{e^{-\frac{2}{3}x^{3/2}}}{2\sqrt{\pi}x^{1/4}}, \quad \text{as } x \to \infty.$$

Equation (13) is known as the *Painlevé II equation*, after Paul Painlevé (1863–1933). Painlevé completely classified differential equations (from a certain class of second order equations) whose "bad" singularities (branch points and essential singularities) were independent of the initial conditions. Most of the equations in this class were already known, but a few were new, including equation (13).

Now define the *Tracy–Widom distribution* to be the probability distribution on $\mathbb{R}$ given by

$$F(t) = \exp\left(-\int_t^\infty (x-t)u(x)^2\,dx\right). \tag{14}$$

It is easily seen that $F(t)$ is indeed a probability distribution, i.e., $F(t) \geq 0$ and $\int_{-\infty}^{\infty} F'(t)dt = 1$. We can now state the remarkable results of Baik, Deift, and Johansson.

Theorem 4. *We have for random (uniform) $w \in \mathfrak{S}_n$ and all $t \in \mathbb{R}$ that*

$$\lim_{n\to\infty} \text{Prob}\left(\frac{\text{is}_n(w) - 2\sqrt{n}}{n^{1/6}} \le t\right) = F(t).$$

The above theorem is a vast refinement of the Vershik–Kerov and Logan–Shepp results concerning $E(n)$, the expectation of $\text{is}(w)$. It gives the entire limiting distribution (as $n \to \infty$) of $\text{is}_n(w)$. Baik, Deift, and Johansson also determine all the limiting moments of $\text{is}_n(w)$. In particular, we have the following formula for the variance $\text{Var}(\text{is}_n)$ of is_n as $n \to \infty$.

Corollary 5. *We have*

$$\begin{aligned}\lim_{n\to\infty} \frac{\text{Var}(\text{is}_n)}{n^{1/3}} &= \int t^2\, dF(t) - \left(\int t\, dF(t)\right)^2 \\ &= 0.8131947928\ldots,\end{aligned}$$

and

$$\begin{aligned}\lim_{n\to\infty} \frac{E(n) - 2\sqrt{n}}{n^{1/6}} &= \int t\, dF(t) \\ &= -1.7710868074\ldots.\end{aligned} \tag{15}$$

Note that equation (15) may be rewritten

$$E(n) = 2\sqrt{n} + \alpha n^{1/6} + o(n^{1/6}),$$

where $\alpha = \int t\, dF(t)$, thereby giving the second term in the asymptotic behavior of $E(n)$.

We will say only a brief word on the proof of Theorem 4, explaining how combinatorics enters into the picture. Some kind of analytic expression is needed for the distribution of $\text{is}_n(w)$. Such an expression is provided by the following result of Ira Gessel [47], later proved in other ways by various persons; see [15, §1] for references. Define

$$\begin{aligned} u_k(n) &= \#\{w \in \mathfrak{S}_n : \text{is}_n(w) \le k\}, \\ U_k(x) &= \sum_{n\ge 0} u_k(n) \frac{x^{2n}}{n!^2}, \quad k \ge 1, \\ I_i(2x) &= \sum_{n\ge 0} \frac{x^{2n+i}}{n!\,(n+i)!}, \quad i \in \mathbb{Z}. \end{aligned} \tag{16}$$

The function I_i is the *hyperbolic Bessel function* of the first kind of order i. Note that $I_i(2x) = I_{-i}(2x)$.

Theorem 6. *We have*

$$U_k(x) = \det\left(I_{i-j}(2x)\right)_{i,j=1}^{k}.$$

Example 1. We have (using $I_1 = I_{-1}$)

$$U_2(x) = \begin{vmatrix} I_0(2x) & I_1(2x) \\ I_1(2x) & I_0(2x) \end{vmatrix} = I_0(2x)^2 - I_1(2x)^2.$$

From this expression it is easy to deduce that

$$u_2(n) = \frac{1}{n+1}\binom{2n}{n}, \tag{17}$$

a Catalan number. This formula for $u_2(n)$ was first stated by Hammersley [56] in 1972, with the first published proofs by Knuth [67, §5.1.4] and Rotem [86]. There is a more complicated expression for $u_3(n)$ due to Gessel [47, §7], [99, Exer. 7.16(e)], namely,

$$u_3(n) = \frac{1}{(n+1)^2(n+2)} \sum_{j=0}^{n} \binom{2j}{j}\binom{n+1}{j+1}\binom{n+2}{j+2}, \tag{18}$$

while no "nice" formula for $u_k(n)$ is known for fixed $k > 3$. It is known, however, that $u_k(n)$ is a P-recursive function of n, i.e., satisfies a linear recurrence with polynomial coefficients [47, §7]. For instance,

$$\begin{aligned}(n+4)(n+3)^2 u_4(n) = {} & (20n^3 + 62n^2 + 22n - 24)u_4(n-1) \\ & - 64n(n-1)^2 u_4(n-2),\end{aligned}$$

$$\begin{aligned}(n+6)^2(n+4)^2 u_5(n) = {} & (375 - 400n - 843n^2 - 322n^3 - 35n^4)u_5(n-1) \\ & + (259n^2 + 622n + 45)(n-1)^2 u_5(n-2) \\ & - 225(n-1)^2(n-2)^2 u_5(n-3).\end{aligned}$$

A number of conjectures about the form of the recurrence satisfied by $u_k(n)$ were made by Bergeron, Favreau, and Krob [23], reformulated in [24] with some progress toward a proof.

Gessel's theorem (Theorem 6) reduces the theorem of Baik, Deift, and Johansson to "just" analysis, viz., the Riemann–Hilbert problem in the theory of integrable systems, followed by the method of steepest descent to analyze the asymptotic behavior of integrable systems. For further information see the survey [40] of Deift mentioned above.

The asymptotic behavior of $\mathrm{is}_n(w)$ (suitably scaled) turned out to be identical to the Tracy–Widom distribution $F(t)$ of equation (14). Originally the Tracy–Widom distribution arose in connection with the *Gaussian Unitary Ensemble* (GUE). GUE is

a certain natural probability density on the space of all $n \times n$ hermitian matrices $M = (M_{ij})$, namely,

$$Z_n^{-1} e^{-\mathrm{tr}(M^2)} dM,$$

where Z_n is a normalization constant and

$$dM = \prod_i dM_{ii} \cdot \prod_{i<j} d(\mathrm{Re}\, M_{ij}) d(\mathrm{Im}\, M_{ij}).$$

Let the eigenvalues of M be $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. The following result marked the eponymous appearance [106] of the Tracy–Widom distribution:

$$\lim_{n\to\infty} \mathrm{Prob}\big((\alpha_1 - \sqrt{2n})\sqrt{2}n^{1/6} \leq t\big) = F(t). \tag{19}$$

Thus as $n \to \infty$, $\mathrm{is}_n(w)$ and α_1 have the same distribution (after scaling).

It is natural to ask, firstly, whether there is a result analogous to equation (19) for the other eigenvalues α_k of the GUE matrix M, and, secondly, whether there is some connection between such a result and the behavior of increasing subsequences of random permutations. A generalization of (19) to all α_k was given by Tracy and Widom [106] (expressed in terms of the Painlevé II function $u(x)$). The connection with increasing subsequences was conjectured in [15] and proved independently by Borodin–Okounkov–Olshanski [31], Johannson [59], and Okounkov [78], after first being proved for the second largest eigenvalue by Baik, Deift, and Johansson [16]. Given $w \in \mathfrak{S}_n$, define integers $\lambda_1, \lambda_2, \ldots$ by letting $\lambda_1 + \cdots + \lambda_k$ be the largest number of elements in the union of k increasing subsequences of w. For instance, let $w = 247951368$. The longest increasing subsequence is 24568, so $\lambda_1 = 5$. The largest union of two increasing subsequences is 24791368 (the union of 2479 and 1368), so $\lambda_1 + \lambda_2 = 8$. (Note that it is impossible to find a union of length 8 of two increasing subsequences that contains an increasing subsequence of length $\lambda_1 = 5$.) Finally w itself is the union of the three increasing subsequences 2479, 1368, and 5, so $\lambda_1 + \lambda_2 + \lambda_3 = 9$. Hence $(\lambda_1, \lambda_2, \lambda_3) = (5, 3, 1)$ (and $\lambda_i = 0$ for $i > 3$). Readers familiar with the theory of the RSK algorithm will recognize the sequence $(\lambda_1, \lambda_2, \ldots)$ as the shape $\mathrm{sh}(w)$ as defined preceding Theorem 2, a well-known result of Curtis Greene [50], [99, Thm. A1.1.1]. (In particular, $\lambda_1 \geq \lambda_2 \geq \cdots$, a fact which is by no means obvious.) The result of [31], [59], [78] asserts that as $n \to \infty$, λ_k and α_k are equidistributed, up to scaling. In particular, the paper [78] of Okounkov provides a direct connection, via the topology of random surfaces, between the two seemingly unrelated appearances of the Tracy–Widom distribution in the theories of random matrices and increasing subsequences. A very brief explanation of this connection is the following: a surface can be described either by gluing together polygons along their edges or by a ramified covering of a sphere. The former description is related to random matrices via the theory of quantum gravity, while the latter can be formulated in terms of the combinatorics of permutations.

We have discussed how Gessel's generating function $U_k(x)$ for $u_k(n)$ is needed to find the limiting distribution of is_n. We can also ask about the behavior of $u_k(n)$ itself for fixed k. The main result here is due to Regev [82].

Theorem 7. *For fixed k and for $n \to \infty$ we have the asymptotic formula*

$$u_k(n) \sim 1!\,2!\,\ldots(k-1)!\left(\frac{1}{\sqrt{2\pi}}\right)^{k-1}\left(\frac{1}{2}\right)^{(k^2-1)/2} k^{k^2/2}\frac{k^{2n}}{n^{(k^2-1)/2}}.$$

Idea of proof. From the RSK algorithm we have

$$u_k(n) = \sum_{\substack{\lambda\vdash n\\ \ell(\lambda)\le k}} (f^\lambda)^2. \tag{20}$$

Write f^λ in terms of the hook-length formula, factor out the dominant term from the sum (which can be determined via Stirling's formula), and interpret what remains in the limit $n \to \infty$ as a k-dimensional integral. This integral turns out to be a special case of *Selberg's integral* (e.g., [7, Ch. 8]), which can be explicitly evaluated. □

An immediate corollary of Theorem 7 (which can also be easily proved directly using RSK) is the formula

$$\lim_{n\to\infty} u_k(n)^{1/n} = k^2. \tag{21}$$

5. Symmetry

Previous sections dealt with properties of general permutations in $\mathfrak{S}_n$. Much of the theory carries over for certain classes of permutations. There is a natural action of the dihedral group D_4 of order 8 on $\mathfrak{S}_n$, best understood by considering the permutation matrix P_w corresponding to $w \in \mathfrak{S}_n$. Since P_w is a square matrix, D_4 acts on P_w as the usual symmetry group of the square. In particular, reflecting through the main diagonal transforms P_w to its transpose $P_w^t = P_{w^{-1}}$. Reflecting about a horizontal line produces P_{w^r}, where w^r is the reverse of w as used in equation (7). These two reflections generate the entire group D_4.

Let G be a subgroup of D_4, and let

$$\mathfrak{S}_n^G = \{w \in \mathfrak{S}_n \,:\, \sigma \cdot w = w \text{ for all } \sigma \in G\}.$$

Most of the results of the preceding sections can be carried over from $\mathfrak{S}_n$ to $\mathfrak{S}_n^G$. The general theory is due to Baik and Rains [17], [18], [19]. Moreover, for certain G we can add the condition that no entry of P_w equal to 1 can be fixed by G, or more strongly we can specify the number of 1's in P_w fixed by G. For instance, if G is the group of order 2 generated by reflection through the main diagonal, then we are specifying the number of fixed points of w. For convenience we will consider here only two special

cases, viz., (a) G is the group of order 2 generated by reflection through the main diagonal. In this case $\mathfrak{S}_n^G = \{w \in \mathfrak{S}_n : w^2 = 1\}$, the set of *involutions* in $\mathfrak{S}_n$, which we also denote as $\mathfrak{I}_n$. (b) The modification of (a) where we consider fixed-point free involutions only. Write $\mathfrak{I}_n^*$ for this set, so $\mathfrak{I}_n^* = \emptyset$ when n is odd.

The RSK algorithm is well-behaved with respect to inversion, viz., it follows from equation (4) that if $w \xrightarrow{\text{rsk}} (P, Q)$ then $w^{-1} \xrightarrow{\text{rsk}} (Q, P)$. Hence

$$w^2 = 1 \quad \text{if and only if} \quad P = Q. \tag{22}$$

Let

$$y_k(n) = \#\{w \in \mathfrak{I}_n : \text{is}_n(w) \le k\}.$$

By Schensted's theorem (Theorem 2) we conclude

$$y_k(n) = \sum_{\substack{\lambda \vdash n \\ \lambda_1 \le k}} f^\lambda,$$

the "involution analogue" of (20). From this formula or by other means one can obtain formulas for $y_k(n)$ for small k analogous to (17) and (18). In particular (see [99, Exer. 7.16(b)] for references),

$$\begin{aligned}
y_2(n) &= \binom{n}{\lfloor n/2 \rfloor}, \\
y_3(n) &= \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} C_i, \\
y_4(n) &= C_{\lfloor (n+1)/2 \rfloor} C_{\lceil (n+1)/2 \rceil}, \\
y_5(n) &= 6 \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} C_i \frac{(2i+2)!}{(i+2)!(i+3)!},
\end{aligned}$$

where as usual C_i is a Catalan number.

The RSK algorithm is also well-behaved with respect to fixed points of involutions. It was first shown by Schützenberger [90, p. 127], [99, Exer. 7.28(a)] that if $w^2 = 1$ and $w \xrightarrow{\text{rsk}} (P, P)$, then the number of fixed points of w is equal to the number of columns of P of odd length. Let

$$\begin{aligned}
v_{2k}(n) &= \#\{w \in \mathfrak{I}_n^* : \text{ds}(w) \le 2k\}, \\
z_k(n) &= \#\{w \in \mathfrak{I}_n^* : \text{is}(w) \le k\}.
\end{aligned}$$

(It is easy to see directly that if $w \in \mathfrak{I}_n^*$ then $\text{ds}(w)$ is even, so there is no need to deal

with $v_{2k+1}(n)$.) It follows that

$$v_{2k}(n) = \sum_{\substack{\lambda \vdash n \\ \lambda_1 \le k}} f^{2\lambda'},$$
$$z_k(n) = \sum_{\substack{\lambda \vdash n, \\ \lambda'_1 \le k}} f^{2\lambda'},$$

where $2\lambda' = (2\lambda'_1, 2\lambda'_2, \dots)$, the general partition with no columns of odd length. Note that for fixed-point free involutions $w \in \mathfrak{I}_n^*$ we no longer have a symmetry between $\mathrm{is}(w)$ and $\mathrm{ds}(w)$, as we do for arbitrary permutations or arbitrary involutions.

There are also "involution analogues" of Gessel's determinant (Theorem 6). Equations (23) and (24) below were first obtained by Gessel [47, §6], equation (25) by Goulden [48], and equations (26) and (27) by Baik and Rains [17, Cor. 5.5]. Let

$$Y_k(x) = \sum_{n \ge 0} y_k(n) \frac{x^n}{n!},$$
$$V_{2k}(x) = \sum_{n \ge 0} v_{2k}(n) \frac{x^n}{n!},$$
$$Z_k(x) = \sum_{n \ge 0} z_k(n) \frac{x^n}{n!}.$$

Write $I_i = I_i(2x)$.

Theorem 8. *We have*

$$Y_{2k}(x) = \det(I_{i-j} + I_{i+j-1})_{i,j=1}^k, \tag{23}$$
$$Y_{2k+1}(x) = e^x \det(I_{i-j} - I_{i+j})_{i,j=1}^k, \tag{24}$$
$$V_{2k}(x) = \det(I_{i-j} - I_{i+j})_{i,j=1}^k, \tag{25}$$
$$Z_{2k}(x) = \frac{1}{4}\det(I_{i-j} + I_{i+j-2})_{i,j=1}^k + \frac{1}{2}\det(I_{i-j} - I_{i+j})_{i,j=1}^{k-1}, \tag{26}$$
$$Z_{2k+1}(x) = \frac{1}{2}e^x \det(I_{i-j} - I_{i+j-1})_{i,j=1}^k + \frac{1}{2}e^{-x}\det(I_{i-j} + I_{i+j-1})_{i,j=1}^k. \tag{27}$$

Once we have the formulas of Theorem 8 we can use the techniques of Baik, Deift, and Johansson to obtain the limiting behavior of $\mathrm{ds}(w)$ for $w \in \mathfrak{I}_n$ and $w \in \mathfrak{I}_n^*$. These results were first obtained by Baik and Rains [18], [19].

Theorem 9. (a) We have for random (uniform) $w \in \mathfrak{I}_n$ and all $t \in \mathbb{R}$ that

$$\lim_{n\to\infty} \mathrm{Prob}\left(\frac{\mathrm{is}_n(w) - 2\sqrt{n}}{n^{1/6}} \le t\right) = F(t)^{1/2} \exp\left(\frac{1}{2}\int_t^\infty u(s)ds\right),$$

where $F(t)$ denotes the Tracy–Widom distribution and $u(s)$ the Painlevé II function. (By (22) we can replace $\mathrm{is}_n(w)$ with $\mathrm{ds}_n(w)$.)

(b) We have for random (uniform) $w \in \mathfrak{I}_{2n}^*$ and all $t \in \mathbb{R}$ that

$$\lim_{n\to\infty} \mathrm{Prob}\left(\frac{\mathrm{ds}_{2n}(w) - 2\sqrt{2n}}{(2n)^{1/6}} \le t\right) = F(t)^{1/2} \exp\left(\frac{1}{2}\int_t^\infty u(s)ds\right).$$

(c) We have for random (uniform) $w \in \mathfrak{I}_{2n}^*$ and all $t \in \mathbb{R}$ that

$$\lim_{n\to\infty} \mathrm{Prob}\left(\frac{\mathrm{is}_{2n}(w) - 2\sqrt{2n}}{(2n)^{1/6}} \le t\right) = F(t)^{1/2} \cosh\left(\frac{1}{2}\int_t^\infty u(s)ds\right).$$

There are orthogonal and symplectic analogues of the GUE model of random hermitian matrices, known as the GOE and GSE models. The GOE model replaces hermitian matrices with real symmetric matrices, while the GSE model concerns hermitian self-dual matrices. (A $2n \times 2n$ complex matrix is *hermitian self-dual* if is composed of 2×2 blocks of the form $\left[\begin{smallmatrix} a+bi & c+di \\ -c+di & a-bi \end{smallmatrix}\right]$ which we identify with the quaternion $a+bi+cj+dk$, such that if we regard the matrix as an $n \times n$ matrix M of quaternions, then $\overline{M}_{ji} = M_{ij}$ where the bar is quaternion conjugation.) The limiting distribution of $\mathrm{ds}_{2n}(w)$ for $w \in \mathfrak{I}_{2n}^*$ coincides (after scaling) with the distribution of the largest eigenvalue of a random real symmetric matrix (under the GOE model), while the limiting distribution of $\mathrm{is}_{2n}(w)$ for $w \in \mathfrak{I}_{2n}^*$ coincides (after scaling) with the distribution of the largest eigenvalue of a random hermitian self-dual matrix (under the GSE model) [107].

6. Connections with the classical groups

In equation (9) we expressed $g_{pq}(n)$, the number of permutations $w \in \mathfrak{S}_n$ satisfying $\mathrm{is}(w) = p$ and $\mathrm{ds}(w) = q$, in terms of the degrees f^λ of irreducible representations of $\mathfrak{S}_n$. This result can be restated via Schur–Weyl duality as a statement about the distribution of eigenvalues of matrices in the unitary group $U(n)$. The results of Section 5 can be used to extend this statement to other classical groups.

Let $U(k)$ denote the group of $k \times k$ complex unitary matrices. For a function $f : U(k) \to \mathbb{C}$, let $E(f)$ denote expectation with respect to Haar measure, i.e.,

$$E(f) = \int_{M\in U(k)} f(M)dM,$$

where $\int$ is the Haar integral. The following result was proved by Diaconis and Shahshahani [42] for $n \ge k$ and by Rains [81] for general k. Note that if M has eigenvalues $\theta_1, \ldots, \theta_k$ then

$$|\mathrm{tr}(M)^n|^2 = (\theta_1 + \cdots + \theta_k)^n(\bar{\theta}_1 + \cdots + \bar{\theta}_k)^n.$$

Theorem 10. *We have* $E(|\mathrm{tr}(M)^n|^2) = u_k(n)$, *where* $u_k(n)$ *is defined in equation* (16).

Proof. The proof is based on the theory of symmetric functions, as developed e.g. in [72] or [99, Ch. 7]. If $f(x_1, \ldots, x_k)$ is a symmetric function, then write $f(M)$ for $f(\theta_1, \ldots, \theta_k)$, where $\theta_1, \ldots, \theta_k$ are the eigenvalues of $M \in U(k)$. The Schur functions s_λ for $\ell(\lambda) \leq k$ are the irreducible characters of $U(k)$, so by the orthogonality of characters we have for partitions λ, μ of length at most k that

$$\int_{M \in U(k)} s_\lambda(M)\, \overline{s_\mu(M)} dM = \delta_{\lambda\mu}. \tag{28}$$

Now $\mathrm{tr}(M)^n = p_1(M)^n$, where $p_1(x_1, \ldots, x_k) = x_1 + \cdots + x_k$. The symmetric function $p_1(x_1, \ldots, x_k)^n$ has the expansion [72, Exam. 1.5.2], [99, Cor. 7.12.5]

$$p_1(x_1, \ldots, x_k)^n = \sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq k}} f^\lambda s_\lambda(x_1, \ldots, x_k),$$

where f^λ is the number of SYT of shape λ as in Section 2. (This formula is best understood algebraically as a consequence of the Schur–Weyl duality between $\mathfrak{S}_n$ and $U(k)$ [99, Ch. 7, Appendix 2], although it can be proved without any recourse to representation theory.) Hence from equation (28) we obtain

$$\begin{aligned} E(|\mathrm{tr}(M)^n|^2) &= \int_{M \in U(k)} p_1(M)^n\, \overline{p_1(M)}^n dM \\ &= \sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq k}} \left(f^\lambda\right)^2. \end{aligned}$$

Comparing with equation (20) completes the proof. □

Many variations of Theorem 10 have been investigated. For instance, we can replace $\mathrm{tr}(M)^n$ by more general symmetric functions of the eigenvalues, such as $\mathrm{tr}(M^m)^n$, or we can replace $U(k)$ with other classical groups, i.e., $O(k)$ and $\mathrm{Sp}(2k)$. For further information, see Rains [81].

7. Pattern avoidance

In this and the following two sections we consider some generalizations of increasing and decreasing subsequences of permutations. In this section and the next we look at other kinds of subsequences of permutations, while in Section 9 we generalize the permutations themselves.

We have defined $u_k(n)$ to be the number of permutations in $\mathfrak{S}_n$ with no increasing subsequence of length $k + 1$. We can instead prohibit other types of subsequences of a fixed length, leading to the currently very active area of *pattern avoidance*.

Given $v = b_1 \dots b_k \in \mathfrak{S}_k$, we say that a permutation $w = a_1 \dots a_n \in \mathfrak{S}_n$ *avoids* v if it contains no subsequence $a_{i_1} \dots a_{i_k}$ in the same relative order as v, i.e., no subsequence $a_{i_1} \dots a_{i_k}$ satisfies the condition:

$$\text{For all } 1 \le r < s \le k, a_{i_r} < a_{i_s} \Longleftrightarrow b_r < b_s.$$

Thus a permutation w satisfies $\mathrm{is}(w) < k$ if and only if it is $12 \dots k$-avoiding, and similarly satisfies $\mathrm{ds}(w) < k$ if and only if it is $k(k-1) \dots 1$-avoiding. What can be said about the set $\mathfrak{S}_n(v)$ of permutations $w \in \mathfrak{S}_n$ that are v-avoiding? In particular, when are there formulas and recurrences for $s_n(v) := \#\mathfrak{S}_n(v)$ similar to those of Theorem 6 and Example 1?

The vast subject of pattern avoidance, as a generalization of avoiding long increasing and decreasing subsequences, began in 1968 with Knuth [66, Exer. 2.2.1.5]. He showed in connection with a problem on stack sorting that $s_n(312)$ is the Catalan number C_n. (See also [99, Exer. 6.19(ff)].) By obvious symmetries this result, together with equation (17), shows that $s_n(v) = C_n$ for all $v \in \mathfrak{S}_3$. A fundamental paper directly connecting 321-avoiding and 231-avoiding permutations was written by Simion and Schmidt [94].

Wilf first raised the question of investigating $s_n(v)$ for $v \in \mathfrak{S}_k$ when $k \ge 4$. Here is a brief summary of some highlights in this burgeoning area. For further information, see e.g. [30, Chs. 4, 5] and the special issue [9]. Call two permutations $u, v \in \mathfrak{S}_k$ *equivalent*, denoted $u \sim v$, if $s_n(u) = s_n(v)$ for all n. Then there are exactly three equivalence classes of permutations $u \in \mathfrak{S}_4$. One class contains 1234, 1243, and 2143 (and their trivial symmetries), the second contains 3142 and 1342, and the third 1324. The values of $s_n(1234)$ are given by equation (18) and of $s_n(1342)$ are given by the generating function

$$\sum_{n \ge 0} s_n(1342) x^n = \frac{32x}{1 + 20x - 8x^2 - (1-8x)^{3/2}},$$

a result of Bóna [28].The enumeration of 1324-avoiding permutations in $\mathfrak{S}_n$ remains open.

Let us mention one useful technique for showing the equivalence of permutations in $\mathfrak{S}_k$, the method of *generating trees* introduced by Chung, Graham, Hoggatt and Kleiman [38] and further developed by West [111], [112], [113] and others. Given $u \in \mathfrak{S}_k$, the *generating tree* $\mathcal{T}_u$ is the tree with vertex set $\bigcup_{n \ge 1} \mathfrak{S}_n(u)$, and with y a descendent of w if w is a subsequence of y (an actual subsequence, not the pattern of a subsequence). For many pairs $u, v \in \mathfrak{S}_k$ we have $\mathcal{T}_u \cong \mathcal{T}_v$, showing in particular that $s_n(u) = s_n(v)$ for all n, i.e., $u \sim v$. In many cases in fact the two trees will have no automorphisms, so the isomorphism $\mathcal{T}_u \to \mathcal{T}_v$ is unique, yielding a canonical bijection $\mathfrak{S}_n(u) \to \mathfrak{S}_n(v)$. A unique isomorphism holds for instance when $u = 123$ and $v = 132$. Figure 3 shows the first four levels of the trees $\mathcal{T}_{123} \cong \mathcal{T}_{132}$, labelled by elements of both $\mathcal{T}_{123}$ and $\mathcal{T}_{132}$ (boldface). This tree can also be defined recursively by the condition that the root has two children, and if vertex x has k children, then

the children of x have $2, 3, \ldots, k+1$ children. For further information about trees defined in a similar recursive manner, see Banderier et al. [20].

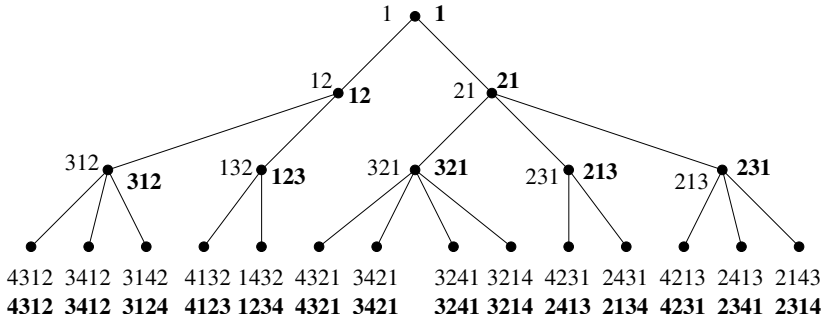


Figure 3. The generating tree for $\mathfrak{S}_n(123)$ and $\mathfrak{S}_n(132)$.

Given $v \in \mathfrak{S}_k$, let

$$F_v(x) = \sum_{n \geq 0} s_n(v) x^n.$$

It is not known whether $F_v(x)$ is always algebraic or even the weaker condition of being *D-finite*, which is equivalent to $s_n(v)$ being P-recursive [96], [99, §6.4]. A long-standing conjecture, known as the *Stanley–Wilf conjecture*, stated that for all $v \in \mathfrak{S}_k$ there is a $c > 1$ such that $s_n(v) < c^n$. In this case $L_v := \lim_{n\to\infty} s_n(v)^{1/n}$ exists and satisfies $1 < L_v < \infty$ [8]. For instance, equation (21) asserts that $L_{12\ldots k} = (k-1)^2$. The Stanley–Wilf conjecture was proved by Marcus and Tardos [76] by a surprisingly simple argument. It is known that for $k \geq 4$ the permutation $12\ldots k$ neither maximizes nor minimizes L_v for $v \in \mathfrak{S}_k$ [3], but it is not known which permutations do achieve the maximum or minimum.

An interesting aspect of pattern avoidance was considered by Albert [1]. Let X be a finite subset of $\mathfrak{S}_2 \cup \mathfrak{S}_3 \cup \cdots$, and let $s_n(X)$ denote the number of permutations $w \in \mathfrak{S}_n$ avoiding all permutations $v \in X$. We say that X is *proper* if it does not contain both the identity permutation $12\ldots j$ for some j and the "reverse identity" $k\ldots 21$ for some k. It is easy to see (using Theorem 1) that X is proper if and only if $s_n(X) > 0$ for all $n \geq 1$. For $w \in \mathfrak{S}_n$ let $\mathrm{is}^X(w)$ be the length of the longest subsequence of w avoiding all $v \in X$, and let $E_X(n)$ denote the expectation of $\mathrm{is}^X(w)$ for uniform $w \in \mathfrak{S}_n$, so

$$E_X(n) = \frac{1}{n!} \sum_{w \in \mathfrak{S}_n} \mathrm{is}^X(w).$$

Albert then makes the following intriguing conjecture.

Conjecture 11. If X is proper then

$$\lim_{n\to\infty} s_n(X)^{1/n} = \frac{1}{4} \left(\lim_{n\to\infty} \frac{E_X(n)}{\sqrt{n}} \right)^2. \tag{29}$$

(The limits on both sides are only conjectured to exist.)

Consider for instance the case $X = \{21\}$. Then $s_n(X) = 1$ for all $n \geq 1$, so the left-hand side of (29) is 1. On the other hand, $\mathrm{is}^X(w) = \mathrm{is}(w)$, so the right-hand side is also 1 by equation (12). More generally, Albert proves Conjecture 11 for $X = \{12\ldots k\}$ and hence (by symmetry) for $X = \{k\ldots 21\}$ [1, Prop. 4].

Let us mention that permutations avoiding a certain pattern v or a finite set of patterns have arisen naturally in a variety of contexts. For instance, an elementary result of Tenner [104] asserts that the interval $[0, w]$ in the Bruhat order of $\mathfrak{S}_n$ is a boolean algebra if and only if w is 321 and 3412-avoiding, and that the number of such permutations w is the Fibonacci number F_{2n-1}. The Schubert polynomial $\mathfrak{S}_w$ is a single monomial if and only if w is 132-avoiding [73, p. 46]. All reduced decompositions of $w \in \mathfrak{S}_n$ are connected by the Coxeter relations $s_i s_j = s_j s_i$ (i.e., $s_i s_{i+1} s_i$ does not appear as a factor in any reduced decomposition of w) if and only if w is 321-avoiding [25, Thm. 2.1]. *Vexillary permutations* may be defined as those permutations w such that the stable Schubert polynomial F_w is a single Schur function or equivalently, whose Schubert polynomial $\mathfrak{S}_w$ is a flag Schur function (or multi-Schur function). They turn out to be the same as 2143-avoiding permutations [73, (1.27)(iii), (7.24)(iii)], first enumerated by West [111, Cor. 3.17], [112, Cor. 3.11]. Similarly, permutations $w \in \mathfrak{S}_n$ for which the Schubert variety Ω_w in the complete flag variety $\mathrm{GL}(n, \mathbb{C})/B$ is smooth are those permutations that are 4231 and 3412-avoiding (implicit in Ryan [87], based on earlier work of Lakshmibai, Seshadri, and Deodhar, and explicit in Lakshmibai and Sandhya [69]). The enumeration of such "smooth permutations" in $\mathfrak{S}_n$ is due to Haiman [29], [52], [99, Exer. 6.47], viz.,

$$\sum_{n\geq 0} \mathfrak{S}_n(4231, 3412)x^n = \frac{1}{1 - x - \frac{x^2}{1-x}\left(\frac{2x}{1+x-(1-x)C(x)} - 1\right)},$$

where $C(x) = \sum_{n\geq 0} C_n x^n = (1 - \sqrt{1-4x})/2x$. See Billey and Lakshmibai [26] for further information. As a final more complicated example, Billey and Warrington [27] show that a permutation $w \in \mathfrak{S}_n$ has a number of nice properties related to the Kazhdan–Lusztig polynomials $P_{x,w}$ if and only if w avoids 321, 46718235, 46781235, 56718234, and 56781234. These permutations were later enumerated by Stankova and West [95]. A database of "natural occurrences" of pattern avoidance can be found at a website [105] maintained by B. Tenner.

The subjects of pattern avoidance and increasing/decreasing subsequences can be considered together, by asking for the distribution of $\mathrm{is}(w)$ or $\mathrm{ds}(w)$ where w ranges over a pattern-avoiding class $\mathfrak{S}_n(v)$. (For that matter, one can look at the distribution of $\mathrm{is}(w)$ or $\mathrm{ds}(w)$ where w ranges over *any* "interesting" subset of $\mathfrak{S}_n$.) For instance, Reifegerste [83, Cor. 4.3] shows that for $k \geq 3$,

$$\#\{w \in \mathfrak{S}_n(231) \,:\, \mathrm{is}(w) < k\} = \frac{1}{n}\sum_{i=1}^{k-1} \binom{n}{i}\binom{n}{i-1}, \tag{30}$$

a sum of *Narayana numbers* [99, Exer. 6.36]. Note that the left-hand side of (30) can also be written as $\#\{w \in \mathfrak{S}_n(231, 12\dots k)\}$, the number of permutations in $\mathfrak{S}_n$ avoiding both 231 and $12\dots k$. Asymptotic results were obtained by Deutsch, Hildebrand, and Wilf [41] for the distribution of $\mathrm{is}(w)$ when $v = 231$, 132, and 321. Their result for $v = 132$ is the following.

Theorem 12. *For $w \in \mathfrak{S}_n(132)$ the random variable $\mathrm{is}(w)$ has mean $\sqrt{\pi n} + O(n^{1/4})$ and standard deviation $\sqrt{\pi(\frac{\pi}{3} - 1)}\sqrt{n} + O(n^{1/4})$. Moreover, for any $t > -\sqrt{\pi}$ we have*

$$\lim_{n\to\infty} \mathrm{Prob}\left(\frac{\mathrm{is}(w) - \sqrt{\pi n}}{\sqrt{n}} \le t\right) = \sum_{j\in\mathbb{Z}} (1 - 2j^2(t + \sqrt{\pi})^2)e^{-(t+\sqrt{\pi})^2 j^2}.$$

The proof of Theorem 12 is considerably easier than its counterpart for $w \in \mathfrak{S}_n$ (Theorem 4) because there is a relatively simple formula for the number $f(n, k)$ of permutations $w \in \mathfrak{S}_n(132)$ satisfying $\mathrm{is}(w) < k$, viz.,

$$f(n, k) = 2 \sum_{i=\lceil -n/(k+1)\rceil}^{\lfloor (n+1)/(k+1)\rfloor} \left(\binom{2n}{n + i(k + 1)} - \frac{1}{4}\binom{2n + 2}{n + 1 + i(k + 1)}\right).$$

A number of variations and generalizations of pattern-avoiding permutations have been investigated. In particular, we can look at patterns where some of the terms must appear consecutively. This concept was introduced by Babson and Steingrímsson [10] and further investigated by Claesson [39] and others. For instance, the generalized pattern 1–32 indicates a subsequence $a_i a_j a_{j+1}$ of a permutation $w = a_1 a_2 \dots a_n$ such that $a_i < a_{j+1} < a_j$. The hyphen in the notation 1–32 means that the first two terms of the subsequence need not be consecutive. The permutations in $\mathfrak{S}_4$ avoiding 1–32 are all $C_4 = 14$ permutations avoiding 132 (in the previous sense, so avoiding 1–3–2 in the present context) together with 2413. A typical result, due to Claesson [39, Props. 2 and 5], asserts that

$$\#\mathfrak{S}_n(1\text{–}23) = \#\mathfrak{S}_n(1\text{–}32) = B(n),$$

the number of partitions of the set $[n]$ (a *Bell number* [98, §1.4]).

8. Unimodal and alternating subsequences

We briefly discuss two variations of increasing/decreasing subsequences of a different flavor from those considered above. There is considerable room for further work in this area.

Early work of Chung [37] and Steele [102] deals with k-unimodal subsequences. A sequence is *k-unimodal* if it is a concatenation of (at most) $k + 1$ monotone sequences. (In more traditional terminology, a sequence is k-unimodal if it has at most $k + 1$

alternating runs [30, §1.2].) Thus a 0-unimodal sequence is just an increasing or decreasing sequence, and every such sequence is k-unimodal for all k. The sequences 41235 and 24531 are 1-unimodal. Chung showed that every $w \in \mathfrak{S}_n$ has a 1-unimodal subsequence of length $\left\lceil \sqrt{2n + \frac{1}{4}} - \frac{1}{2} \right\rceil$, and that this result is best possible. She conjectured that if $E_k(n)$ is the expected length of the longest k-unimodal subsequence of a random permutation $w \in \mathfrak{S}_n$, then $E_k(n)/\sqrt{n}$ approaches a limit c_k as $n \to \infty$. Steele proved this conjecture and showed that $c_k = 2\sqrt{k+1}$ by deducing it from the monotone ($k = 0$) case.

A sequence $b_1 b_2 \dots b_k$ of integers is *alternating* if

$$b_1 > b_2 < b_3 > b_4 < \cdots b_k.$$

For instance, there are five alternating permutations in $\mathfrak{S}_4$, viz., 2143, 3142, 4132, 3241, 4231. If E_n denotes the number of alternating permutations in $\mathfrak{S}_n$, then a famous result of André [6], [99, §3.16] states that

$$\sum_{n \geq 0} E_n \frac{x^n}{n!} = \sec x + \tan x. \tag{31}$$

The numbers E_n were first considered by Euler (using (31) as their definition) and are known as *Euler numbers*. Sometimes E_{2n} is called a *secant number* and E_{2n-1} a *tangent number*.

We can try to extend the main results on increasing/decreasing subsequences to alternating subsequences. In particular, given $w \in \mathfrak{S}_n$ let $\mathrm{as}(w) = \mathrm{as}_n(w)$ denote the length of the longest alternating subsequence of w, and define

$$b_k(n) = \#\{w \in \mathfrak{S}_n \,:\, \mathrm{as}(w) \leq k\}.$$

Thus $b_1(n) = 1$ (corresponding to the permutation $12 \dots n$), $b_k(n) = n!$ if $k \geq n$, and $b_n(n) - b_{n-1}(n) = E_n$. Note that we can also define $b_k(n)$ in terms of pattern avoidance, viz., $b_k(n)$ is the number of $w \in \mathfrak{S}_n$ avoiding all E_{k+1} alternating permutations in $\mathfrak{S}_{k+1}$.

Unlike the situation for $u_k(n)$ (defined by (16)), there are "nice" explicit generating functions and formulas for $b_k(n)$. The basic reason for the existence of such explicit results is the following (easily proved) key lemma.

Lemma 13. *For any $w \in \mathfrak{S}_n$, there exists an alternating subsequence of w of maximum length that contains n.*

From Lemma 13 it is straightforward to derive a recurrence satisfied by $a_k(n) := b_k(n) - b_{k-1}(n)$, viz.,

$$a_k(n) = \sum_{j=1}^{n} \binom{n-1}{j-1} \sum_{2r+s=k-1} (a_{2r}(j-1) + a_{2r+1}(j-1)) a_s(n-j). \tag{32}$$

Now define

$$B(x,t) = \sum_{k,n\geq 0} b_k(n) t^k \frac{x^n}{n!}.$$

It follows from the recurrence (32) (after some work [101]) that

$$B(x,t) = \frac{1+\rho+2te^{\rho x}+(1-\rho)e^{2\rho x}}{1+\rho-t^2+(1-\rho-t^2)e^{2\rho x}}, \tag{33}$$

where $\rho = \sqrt{1-t^2}$. Alternatively (as pointed out by M. Bóna), let $G(n,k)$ denote the number of $w \in \mathfrak{S}_n$ with k alternating runs as defined at the beginning of this section. Then equation (33) is a consequence of the relation $a_k(n) = \frac{1}{2}(G(n,k-1)+G(n,k))$ and known facts about $G(n,k)$ summarized in [30, §1.2].

It can be deduced from equation (33) (shown with assistance from I. Gessel) that

$$b_k(n) = \frac{1}{2^{k-1}} \sum_{\substack{i+2j\leq k \\ i\equiv k \pmod 2}} (-2)^j \binom{k-j}{(k+i)/2} \binom{n}{j} i^n.$$

For instance,

$$b_1(n) = 1,\ \ b_2(n) = 2^{n-1},\ \ b_3(n) = \frac{1}{4}(3^n - 2n + 3),\ \ b_4(n) = \frac{1}{8}(4^n - (2n-4)2^n).$$

From equation (33) it is also easy to compute the moments

$$M_k(n) = \frac{1}{n!} \sum_{w\in\mathfrak{S}_n} \mathrm{as}_n(w)^k.$$

For instance,

$$\sum_{n\geq 1} M_1(n) x^n = \left.\frac{\partial B(x,t)}{\partial t}\right|_{t=1} = \frac{6x - 3x^2 + x^3}{6(1-x)^2},$$

from which we obtain

$$M_1(n) = \begin{cases} 1, & n = 1, \\ \dfrac{4n+1}{6}, & n > 1. \end{cases} \tag{34}$$

Similarly the variance of $\mathrm{as}_n(w)$ is given by

$$\mathrm{Var}(\mathrm{as}_n) = \frac{8}{45}n - \frac{13}{180}, \quad n \geq 4. \tag{35}$$

It is surprising that there are such simple explicit formulas, in contrast to the situation for $\mathrm{is}(w)$ (equation (10)).

It is natural to ask for the limiting distribution of as_n, analogous to Theorem 4 for is_n. The following result was shown independently by R. Pemantle [79] and H. Widom [114]. It can also be obtained by showing that the polynomials $\sum_k a_k(n)t^k$ have (interlacing) real zeros, a consequence of the connection between $a_k(n)$ and $G(n,k)$ mentioned above and a result of Wilf [30, Thm. 1.41].

Theorem 14. *We have for random (uniform) $w \in \mathfrak{S}_n$ and all $t \in \mathbb{R}$ that*

$$\lim_{n\to\infty} \text{Prob}\left(\frac{\text{as}_n(w) - 2n/3}{\sqrt{n}} \le t\right) = G(t),$$

where $G(t)$ is Gaussian with variance $8/45$:

$$G(t) = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{t\sqrt{45}/4} e^{-s^2} ds.$$

For further information on longest alternating subsequences, see the paper [101].

9. Matchings

The subject of pattern containment and avoidance discussed in Section 7 provides one means to extend the concept of increasing/decreasing subsequences of permutations. In this section we will consider a different approach, in which permutations are replaced with other combinatorial objects. We will be concerned mainly with (complete) *matchings* on $[2n]$, which may be defined as partitions $M = \{B_1, \ldots, B_n\}$ of $[2n]$ into n two-element blocks B_i. Thus $B_1 \cup B_2 \cup \cdots \cup B_n = [2n]$, $B_i \cap B_j = \emptyset$ if $i \ne j$, and $\#B_i = 2$. (These conditions are not all independent.) Alternatively, we can regard a matching M as a fixed-point free involution w_M of $[2n]$, viz., if $B_i = \{a, b\}$ then $w_M(a) = b$. We already considered increasing and decreasing subsequences of fixed-point free involutions in Section 5. In that situation, however, there is no symmetry interchanging increasing subsequences with decreasing subsequences. Here we consider two alternative statistics on matchings (one of which is equivalent to decreasing subsequences) which have the desired symmetry.

Write $\mathfrak{M}_n$ for the set of matchings on $[2n]$. We represent a matching $M \in \mathfrak{M}_n$ by a diagram of $2n$ vertices $1, 2, \ldots, 2n$ on a horizontal line in the plane, with an arc between vertices i and j and lying above the vertices if $\{i, j\}$ is a block of M. Figure 4 shows the diagram corresponding to the matching

$$M = \{\{1, 5\}, \{2, 9\}, \{3, 10\}, \{4, 8\}, \{6, 7\}\}.$$

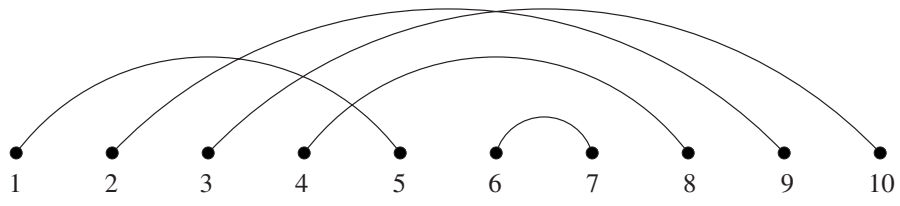


Figure 4. A matching on [10].

Let $M \in \mathfrak{M}_n$. A *crossing* of M consists of two arcs $\{i, j\}$ and $\{k, l\}$ with $i < k < j < l$. Similarly a *nesting* of M consists of two arcs $\{i, j\}$ and $\{k, l\}$ with $i < k < l < j$. The maximum number of mutually crossing arcs of M is called the *crossing number* of M, denoted $\mathrm{cr}(M)$. Similarly the *nesting number* $\mathrm{ne}(M)$ is the maximum number of mutually nesting arcs. For the matching M of Figure 4, we have $\mathrm{cr}(M) = 3$ (corresponding to the arcs $\{1, 5\}$, $\{2, 9\}$, and $\{3, 10\}$), while also $\mathrm{ne}(M) = 3$ (corresponding to $\{2, 9\}$, $\{4, 8\}$, and $\{6, 7\}$).

It is easy to see that $\mathrm{ds}(w_M) = 2 \cdot \mathrm{ne}(M)$, where w_M is the fixed-point free involution corresponding to M as defined above. However, it is not so clear whether $\mathrm{cr}(M)$ is connected with increasing/decreasing subsequences. To this end, define

$$f_n(i, j) = \#\{M \in \mathfrak{M}_n \,:\, \mathrm{cr}(M) = i,\ \mathrm{ne}(M) = j\}.$$

It is well-known that

$$\sum_j f_n(0, j) = \sum_i f_n(i, 0) = C_n. \tag{36}$$

In other words, the number of matchings $M \in \mathfrak{M}_n$ with no crossings (or with no nestings) is the Catalan number C_n. For crossings this result goes back to Errera [44], [99, Exer. 6.19(n,o)]; for nestings see [100]. Equation (36) was given the following generalization by Chen et al. [36].

Theorem 15. *For all i, j, n we have $f_n(i, j) = f_n(j, i)$.*

Theorem 15 is proved by using a version of RSK first defined by the author (unpublished) and then extended by Sundaram [103]. Define an *oscillating tableau* of shape $\lambda \vdash n$ and length k to be a sequence

$$\emptyset = \lambda^0, \lambda^1, \ldots, \lambda^k = \lambda$$

of partitions λ^i such that (the diagram of) λ^{i+1} is obtained from λ^i by either adding or removing a square. (Note that if we add a square each time, so $k = n$, then we obtain an SYT of shape λ.) Oscillating tableaux were first defined (though not with that name) by Berele [22] in connection with the representation theory of the symplectic group. Given a matching $M \in \mathfrak{M}_n$, define an oscillating tableau $\Phi(M) = (\lambda^0, \lambda^1, \ldots, \lambda^{2n})$ of length $2n$ and shape $\emptyset$ as follows. Label the right-hand endpoints of the arcs of M by $1, 2, \ldots, n$ from right-to-left. Label each left-hand endpoint with the same label as the right-hand endpoint. Begin with the empty tableau $T_0 = \emptyset$. Let $a_1, \ldots, a_{2n}$ be the sequence of labels, from left-to-right. Once T_{i-1} has been obtained, define T_i to be the tableau obtained by row-inserting a_i into T_{i-1} (as defined in Section 2) if a_i is the label of a left-hand endpoint of an arc; otherwise T_i is the tableau obtained by deleting a_i from T_{i-1}. Let λ^i be the shape of T_i, and set

$$\Phi(M) = (\emptyset = \lambda^0, \lambda^1, \ldots, \lambda^{2n} = \emptyset).$$

See Figure 5 for an example. It is easy to see that $\Phi(M)$ is an oscillating tableau of length $2n$ and shape $\emptyset$. With a little more work it can be shown that in fact the map $M \mapsto \Phi(M)$ is a *bijection* from $\mathfrak{M}_n$ to the set $\mathcal{O}_n$ of all oscillating tableaux of length $2n$ and shape $\emptyset$. As a consequence we have the enumerative formula

$$\#\mathcal{O}_n = (2n-1)!! := 1 \cdot 3 \cdot 5 \ldots (2n-1), \tag{37}$$

the number of matchings on $[2n]$. The key fact about the correspondence Φ for proving Theorem 15 is the following "oscillating analogue" of Schensted's theorem (Theorem 2).

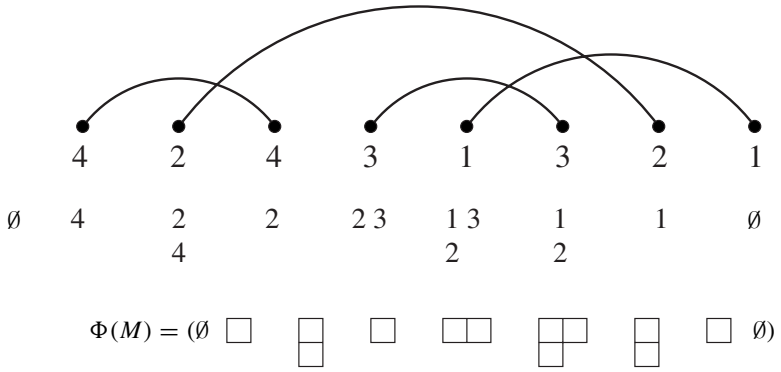


Figure 5. A correspondence between matchings and oscillating tableaux.

Theorem 16. *Let $M \in \mathfrak{M}_n$, and suppose that $\Phi(M) = (\lambda^0, \lambda^1, \ldots, \lambda^{2n})$. Then* $\mathrm{ne}(M)$ *is equal to the most number of columns of any λ^i, while* $\mathrm{cr}(M)$ *is equal to the most number of rows of any λ^i.*

Theorem 15 is an easy consequence of Theorem 16. For let $\Phi(M)'$ be the oscillating tableau obtained by conjugating all the partitions in $\Phi(M)$, and let M' be the matching satisfying $\Phi(M') = \Phi(M)'$. By Theorem 16 we have $\mathrm{cr}(M) = \mathrm{ne}(M')$ and $\mathrm{ne}(M) = \mathrm{cr}(M')$. Since the map $M \mapsto \Phi(M)$ is a bijection we have that the operation $M \mapsto M'$ is a bijection from $\mathfrak{M}_n$ to itself that interchanges cr and ne, and the proof follows.

The above argument and equation (7) show that the operation $M \mapsto M'$ on matchings is a natural analogue of the operation of reversal on permutations. Unlike the case of permutations, we do not know a simple "direct" operation on matchings that interchanges cr with ne.

Let $\tilde{f}_n^\lambda$ denote the number of oscillating tableaux of shape λ and length n, so $\tilde{f}_n^\lambda = 0$ unless $n \equiv |\lambda| \pmod 2$. A generalization for $\tilde{f}_n^\lambda$ of the hook-length formula (equation (3)) is due to Sundaram [103, Lemma 2.2], viz.,

$$\tilde{f}_n^\lambda = \binom{n}{k}(n-k-1)!!\, f^\lambda,$$

where $\lambda \vdash k$ and where of course f^λ is evaluated by the usual hook-length formula (3). (Set $(-1)!! = 1$ when $n = k$.) Note that an oscillating tableau $(\lambda^0, \lambda^1, \ldots, \lambda^{2n})$ of shape $\emptyset$ may be regarded as a pair (P, Q) of oscillating tableaux of the same shape $\lambda = \lambda^n$ and length n, viz.,

$$P = (\lambda^0, \lambda^1, \ldots, \lambda^n),$$
$$Q = (\lambda^{2n}, \lambda^{2n-1}, \ldots, \lambda^n).$$

Hence we obtain the following restatement of equation (37):

$$\sum_\lambda \left(\tilde{f}_n^\lambda\right)^2 = (2n-1)!!, \tag{38}$$

where λ ranges over all partitions. (The partitions λ indexing a nonzero summand are those satisfying $\lambda \vdash k \leq n$ and $k \equiv n \pmod 2$.)

Equation (38) suggests, in analogy to equations (1) and (2), a connection between $\tilde{f}_n^\lambda$ and representation theory. Indeed, there is a $\mathbb{C}$-algebra $\mathfrak{B}_n(x)$, where x is a real parameter, which is semisimple for all but finitely many x (and such that these exceptional x are all integers) and which has a basis that is indexed in a natural way by matchings $M \in \mathfrak{M}_n$. In particular, $\dim \mathfrak{B}_n(x) = (2n-1)!!$. This algebra was first defined by Brauer [32] and shown to be the centralizer algebra of the action of the orthogonal group $\mathrm{O}(V)$ on $V^{\otimes n}$ (the nth tensor power of V), where $\dim V = k$ and $x = k$. It is also the centralizer algebra of the action of the symplectic group $\mathrm{Sp}(2k)$ on $V^{\otimes n}$, where now $\dim V = 2k$ and $x = -2k$. When $\mathfrak{B}_n(x)$ is semisimple, its irreducible representations have dimension $\tilde{f}_n^\lambda$, so we obtain a representation-theoretic explanation of equation (38). For further information see e.g. Barcelo and Ram [21, App. B6]

Because $\mathrm{ds}(w_M) = 2 \cdot \mathrm{ne}(M)$ and because cr_n and ne_n have the same distribution by Theorem 15, the asymptotic distribution of cr_n and ne_n on $\mathfrak{M}_n$ reduces to that of ds_{2n} on $\mathfrak{I}_{2n}^*$, which is given by Theorem 9(b). We therefore obtain the following result.

Theorem 17. *We have for random (uniform) $M \in \mathfrak{M}_n$ and all $t \in \mathbb{R}$ that*

$$\lim_{n\to\infty} \mathrm{Prob}\left(\frac{\mathrm{ne}_n(M) - \sqrt{2n}}{(2n)^{1/6}} \leq \frac{t}{2}\right) = F(t)^{1/2} \exp\left(\frac{1}{2}\int_t^\infty u(s)ds\right).$$

The same result holds with ne_n *replaced with* cr_n.

We can also consider the effect of bounding *both* $\mathrm{cr}(M)$ and $\mathrm{ne}(M)$ as $n \to \infty$. The analogous problem for $\mathrm{is}(w)$ and $\mathrm{ds}(w)$ is not interesting, since by Theorem 1 there are no permutations $w \in \mathfrak{S}_n$ satisfying $\mathrm{is}(w) \leq p$ and $\mathrm{ds}(w) \leq q$ as soon as $n > pq$. Let

$$h_{p,q}(n) = \#\{M \in \mathfrak{M}_n : \mathrm{cr}(M) \leq p,\ \mathrm{ne}(M) \leq q\},$$
$$H_{p,q}(x) = \sum_{n\geq 0} h_{p,q}(n)x^n.$$

It follows from the bijection $\Phi\colon \mathfrak{M}_n \to \mathcal{O}_n$ and a simple application of the transfer-matrix method [98, §4.7] that $H_{p,q}(x)$ is a rational function of x [36, §5]. For instance,

$$H_{1,1}(x) = \frac{1}{1-x}, \quad H_{1,2}(x) = \frac{1-x}{1-2x}, \quad H_{1,3}(x) = \frac{1-2x}{1-3x+x^2}$$

$$H_{2,2}(x) = \frac{1-5x+2x^2}{(1-x)(1-5x)}, \quad H_{2,3}(x) = \frac{1-11x+30x^2-23x^3+4x^4}{(1-x)(1-3x)(1-8x+4x^2)}$$

$$H_{3,3}(x) = \frac{1-24x+186x^2-567x^3+690x^4-285x^5+15x^6}{(1-x)(1-19x+83x^2-x^3)(1-5x+6x^2-x^3)^2}.$$

Christian Krattenthaler pointed out that $h_{p,q}(n)$ can be interpreted as counting certain walks in an alcove of the affine Weyl group $\tilde{C}_n$. It then follows from a result of Grabiner [49, (23)] that all reciprocal zeros of the denominator of $H_{p,q}(x)$ are of the form

$$2(\cos(\pi r_1/m) + \cdots + \cos(\pi r_j/m)),$$

where each $r_i \in \mathbb{Z}$ and $m = p + q + 1$. All these numbers for fixed m belong to an extension of $\mathbb{Q}$ of degree $\phi(2m)/2$, where ϕ is the Euler phi-function. As a consequence, every irreducible factor (over $\mathbb{Q}$) of the denominator of $H_{p,q}(x)$ has degree dividing $\phi(2m)/2$.

Theorem 15 can be extended to objects other than matchings, in particular, arbitrary set partitions. (Recall that we have defined a matching to be a partition of $[2n]$ into n 2-element blocks.) In this situation oscillating tableaux are replaced by certain sequences of partitions known as *vacillating tableaux*. See [36] for further details. Vacillating tableaux were introduced implicitly (e.g., [54, (2.23)]) in connection with the representation theory of the *partition algebra* $\mathfrak{P}_n$, a semisimple algebra whose dimension is the Bell number $B(n)$. See Halverson and Ram [54] for a survey of the partition algebra. Vacillating tableaux and their combinatorial properties were made more explicit by Chen, et al. [36] and by Halverson and Lewandowski [53]. An alternative approach based on "growth diagrams" to vacillating tableaux and their nesting and matchings was given by Krattenthaler [68]. It remains open to find an analogue of Theorem 17 for the distribution of $\mathrm{cr}(\pi)$ or $\mathrm{ne}(\pi)$ (as defined in [36]) for arbitrary set partitions π.

References

[1] Albert, M. H., On the length of the longest subsequence avoiding an arbitrary pattern in a random permutation. Technical Report OUCS-2005-08, University of Otago, 2005; math.CO/0505485.

[2] Albert, M. H., Aldred, R. E. L., Atkinson, M. D., Handley, C. C., Holton, D. A., McCaughan, D. J., Sagan, B. E., Monotonic sequence games. In *Games of No Chance III*, submitted; math.CO/0602630.

[3] Albert, M. H., Elder, M., Rechnitzer, A., Westcott, P., Zabrocki, M., On the Stanley-Wilf limit of 4231-avoiding permutations and a conjecture of Arratia. *Adv. in Appl. Math.* **36** (2) (2006), 96–105.

[4] Aldous, D. J., Diaconis, P., Hammersley's interacting particle process and longest increasing subsequences. *Probab. Theory Related Fields* **103** (1995), 199–213.

[5] Aldous D. J., Diaconis, P., Longest increasing subsequences, from patience sorting to the Baik-Deift-Johansson theorem. *Bull. Amer. Math. Soc.* **36** (1999), 413–432.

[6] André, D., Développement de $\sec x$ and $\operatorname{tg} x$. *C. R. Math. Acad. Sci. Paris* **88** (1879), 965–979.

[7] Andrews, G. E., Askey, R., Roy, R., *Special Functions*. Encyclopedia of Mathematics and Its Applications 71, Cambridge University Press, Cambridge, New York 1999.

[8] Arratia, A. On the Stanley-Wilf conjecture for the number of permutations avoiding a given pattern. *Electron. J. Combin.* **6** (1) (1999), Article N1 (electronic).

[9] Atkinson, M., Holton, D. (eds.), Special volume on permutation patterns. *Electron. J. Combin.* **9** (2002–2003) (electronic).

[10] Babson, E., Steingrímsson, E., Generalized permutation patterns and a classification of the Mahonian statistics. *Sém. Lothar. Combin.* **44** (2000), Article B44b (electronic).

[11] Bachmat, E., Analysis of disk scheduling with linear seek function, increasing, subsequences, and space-time geometry. Preprint; math.OC/0601025.

[12] Bachmat, E., Berend, D., Sapir, L., Skiena, S., Stolyarov, N., Analysis of aeroplane boarding via spacetime geometry and random matrix theory. *J. Phys. A* **39** (2006), L453–L459.

[13] Bachmat, E., Berend, D., Sapir, L., Skiena, S., Stolyarov, N., Analysis of airplane boarding times. Preprint.

[14] Baer, R. M., Brock, P., Natural sorting over permutation spaces. *Math. Comp.* **22** (1968), 385–410.

[15] Baik, J., Deift, P., Johansson, K., On the distribution of the length of the longest increasing subsequence of random permutations. *J. Amer. Math. Soc.* **12** (1999), 1119–1178.

[16] Baik, J., Deift, P., Johansson, K., On the distribution of the length of the second row of a Young diagram under the Plancherel measure. *Geom. Funct. Anal.* **10** (2000), 702–731; Addendum, ibid. 1606–1607.

[17] Baik, J., Rains, E., Algebraic aspects of increasing subsequences. *Duke Math. J.* **109** (2001), 1–65.

[18] Baik, J., Rains, E., Symmetrized random permutations. In *Random Matrix Models and Their Applications*, Math. Sci. Res. Inst. Publ. 40, Cambridge University Press, Cambridge 2001, 1–19.

[19] Baik, J., Rains, E., The asymptotics of monotone subsequences of involutions. *Duke Math. J.* **109** (2001), 205–281.

[20] Banderier, C., Bousquet-Mélou, M., Denise, A., Flajolet, P., Gardy, D., Gouyou-Beauchamps, D., Generating functions for generating trees. *Discrete Math.* **246** (2002), 29–55.

[21] Barcelo, H., Ram, A., Combinatorial representation theory. In *New Perspectives in Algebraic Combinatorics* (Berkeley, CA, 1996–97) , Math. Sci. Res. Inst. Publ. 38, Cambridge University Press, Cambridge 1999, 23–90.

[22] Berele, A., A Schensted-type correspondence for the symplectic group. *J. Combin. Theory Ser. A* **43** (1986), 320–328.

[23] Bergeron, F., Favreau, L., Krob, D., Conjectures on the enumeration of tableaux of bounded height. *Discrete Math.* **139** (1995), 463–468.

[24] Bergeron, F., Gascon, F., Counting Young tableaux of bounded height. *J. Integer Seq.* **3** (2000), Article 00.1.7 (electronic).

[25] Billey, S. C., Jockusch, W., Stanley, R., Some combinatorial properties of Schubert polynomials. *J. Algebraic Combin.* **2** (1993), 345–374.

[26] Billey, S. C., Lakshmibai, V., *Singular Loci of Schubert Varieties*. Progr. Math. 182, Birkäuser, Boston, MA, 2000.

[27] Billey, S. C., Warrington, G. S., Kazhdan-Lusztig polynomials for 321-hexagon-avoiding permutations. *J. Algebraic Combin.* **13** (2001), 111–136.

[28] Bóna, M., Exact enumeration of 1342-avoiding permutations: a close link with labeled trees and planar maps. *J. Combin. Theory Ser. A* **80** (1997), 257–272.

[29] Bóna, M., The permutation classes equinumerous to the smooth class. *Electron. J. Combin.* **5** (1998), Article R31 (electronic).

[30] Bóna, M., *Combinatorics of Permutations*. Chapman & Hall/CRC, Boca Raton, FL, 2004.

[31] Borodin, A., Okounkov, A. Olshanski, G., Asymptotics of Plancherel measures for symmetric groups. *J. Amer. Math. Soc.* **13** (2000), 481–515.

[32] Brauer, R., On algebras which are connected with the semisimple continuous groups. *Ann. Math.* **38** (1937), 854–872.

[33] Burstein, A., Lankham, I., Combinatorics of patience sorting piles. In *Proc. Formal Power Series and Algebraic Combinatorics* (Taormina, Sicily, 2005), Sém. Lothar. Combin. 54A (2005/06), electronic.

[34] Burstein, A., Lankham, I., A geometric form for the extended patience sorting algorithm. *Adv. in Appl. Math.* **36** (2) (2006), 106–117.

[35] Burstein, A., and Lankham, I., Restricted patience sorting and barred pattern avoidance. In *Proc. Formal Power Series and Algebraic Combinatorics* (June 2006), to appear; math.CO/0512122.

[36] Chen, W. Y. C., Deng, E. Y. P., Du, R. R. X., Stanley, R., Yan, C. H., Crossings and nestings of matchings and partitions. *Trans. Amer. Math. Soc.* **359** (2007), 1555–1575.

[37] Chung, F., On unimodal subsequences. *J. Combin. Theory Ser. A* **29** (1980), 267–279.

[38] Chung, F. R. K., Graham, R. L., Hoggatt, V. E., Kleiman, M., The number of Baxter permutations. *J. Combin. Theory Ser. A* **24** (1978), 382–394.

[39] Claesson, A., Generalized pattern avoidance. *European J. Combin.* **22** (2001), 961–971.

[40] Deift, P., Integrable systems and combinatorial theory. *Notices Amer. Math. Soc.* **47** (2000), 631–640.

[41] Deutsch, E., Hildebrand, A. J., Wilf, H., The distribution of longest increasing subsequences in pattern-restricted permutations. *Electron. J. Combin.* **9** (2) (2002–2003), Article R12 (electronic).

[42] Diaconis, P., Shahshahani, M., On the eigenvalues of random matrices. *J. Appl. Prob.* **31** (1994), 49–61.

[43] Erdős, P., Szekeres, G., A combinatorial problem in geometry. *Composito Math.* **2** (1935), 463–470.

[44] Errera, A., Analysis situs. Un problème d'énumeration. *Mém. Acad. Roy. Belgique Coll.* 8^o (2) **11** (1931), 26 pp.

[45] Frame, J. S., Robinson, G. de B., Thrall, R. M., The hook graphs of S_n. *Canad. J. Math.* **6** (1954), 316–324.

[46] Gardner, M., *The Last Recreations*. Springer-Verlag, New York 1997; reprinted from *Scientific American* **216** (March 1967), 124–129, and **216** (April 1967), 116–123.

[47] Gessel, I. M., Symmetric functions and P-recursiveness. *J. Combin. Theory Ser. A* **53** (1990), 257–285.

[48] Goulden, I. P., A linear operator for symmetric functions and tableaux in a strip with given trace. *Discrete Math.* **99** (1992), 69–77.

[49] Grabiner, D., Random walk in an alcove of an affine Weyl group, and non-colliding random walks on an interval. *J. Combin. Theory Ser. A* **97** (2002), 285–306.

[50] Greene, C., An extension of Schensted's theorem. *Adv. Math.* **14** (1974), 254–265.

[51] Groeneboom, P., Ulam's problem and Hammersley's process. *Ann. Probab.* **29** (2001), 683–690.

[52] Haiman, M., unpublished.

[53] Halverson, T., Lewandowski, T., RSK insertion for set partitions and diagram algebras. *Electron. J. Combin.* **11** (2) (2004–2005), Article R24 (electronic).

[54] Halverson, T., Ram, A., Partition algebras. *European J. Combin.* **26** (2005), 869–921.

[55] Harary, F., Sagan, B., West, D, Computer-aided analysis of monotonic sequence games. *Atti Accad. Peloritana Cl. Sci. Fis. Mat. Natur.* **61** (1983), 67–78.

[56] Hammersley, J. M., A few seedlings of research. In *Proc. Sixth Berkeley Symposium on Mathematical Statistics and Probability* (Berkeley, 1970/1971), Vol. 1: *Theory of statistics*. University California Press, Berkeley, CA, 1972, 345–394.

[57] Ivanov, V., Olshanski, G., Kerov's central limit theorem for the Plancherel measure on Young diagrams. In *Symmetric Functions 2001: Surveys of Developments and Perspectives* (S. Fomin, ed.), NATO Sci. Ser. II Math. Phys. Chem. 74, Kluwer, Dordrecht 2002, 93–151.

[58] Johansson, K., The longest increasing subsequence in a random permutation and a unitary random matrix model. *Math. Res. Lett.* **5** (1998), 63–82.

[59] Johansson, K., Discrete orthogonal polynomial ensembles and the Plancherel measure. *Ann. Math.* **153** (2001), 259–296.

[60] Johansson, K., Toeplitz determinants, random growth and determinantal processes. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. III, Higher Ed. Press, Beijing 2002, 53–62.

[61] Kerov, S. V., Gaussian limit for the Plancherel measure of the symmetric group. *C. R. Acad. Sci. Paris Sér. I Math.* **316** (1993), 303–308.

[62] Kerov, S. V., Asymptotics of the separation of roots of orthogonal polynomials. *Algebra i Analiz* **5** (1993), 68–86; English translation: *St. Petersburg Math. J.* **5** (1994), 925–941.

[63] Kerov, S. V., The asymptotics of interlacing sequences and the growth of continual Young diagrams. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov.* (*POMI*) **205** (1993), *Differentsialnaya Geom. Gruppy Li i Mekh.* **13**, 21–29, 179; English translation: *J. Math. Sci.* **80** (1996), 1760–1767.

[64] Kerov, S. V., *Asymptotic Representation Theory of the Symmetric Group and Its Applications in Analysis*. Transl. Math. Monogr. 219, Amer. Math. Soc., Providence, RI, 2003.

[65] Knuth, D. E., Permutations, matrices, and generalized Young tableaux. *Pacific J. Math.* **34** (1970), 709–727.

[66] Knuth, D. E., *The Art of Computer Programming*, Vol. 1, *Fundamental Algorithms*. Addison-Wesley, Reading, MA, 1968; second edition, 1973.

[67] Knuth, D. E., *The Art of Computer Programming*, Vol. 3, *Sorting and Searching*. Addison-Wesley, Reading, MA, 1973; second edition, 1998.

[68] Krattenthaler, C., Growth diagrams, and increasing and decreasing chains in fillings of Ferrers shapes. *Adv. in Appl. Math.* **37** (2006), 404–431.

[69] Lakshmibai, V., Sandhya, B., Criterion for smoothness of Schubert varieties in $\mathrm{Sl}(n)/B$. *Proc. Indian Acad. Sci.* (*Math. Sci.*) **100** (1990), 45–52.

[70] van Leeuwen, M. A. A., The Robinson-Schensted and Schützenberger algorithms, an elementary approach. *Electron. J. Combin.* **3** (2) (1996), Article R15 (electronic).

[71] Logan, B. F., Shepp, L. A., A variational problem for random Young tableaux. *Adv. Math.* **26** (1977), 206–222.

[72] Macdonald, I. G., *Symmetric Functions and Hall Polynomials*. Second ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, Oxford 1995.

[73] Macdonald, I. G., *Notes on Schubert Polynomials*. Publ. Laboratoire de Combinatoire et d'Informatique Mathématique **6**, Université du Québec à Montréal, 1991.

[74] MacMahon, P. M., Memoir on the theory of the partitions of numbers — Part I. *Phil. Trans. Royal Soc. London Ser. A* **187** (1897), 619–673; *Collected Works*, Vol. 1 (G. E. Andrews, ed.), M.I.T. Press, Cambridge, MA, 1978, 1026–1080.

[75] Manivel, L., *Symmetric functions, Schubert polynomials and degeneracy loci*. SMF/AMS Texts and Monographs 6, Amer. Math. Soc., Providence, RI, and Soc. Math. France, Paris 2001.

[76] Marcus, A., Tardos, G., Excluded permutation matrices and the Stanley-Wilf conjecture. *J. Combin. Theory Ser. A* **107** (2004), 153–160.

[77] Morris, W., Soltan, V., The Erdős-Szekeres problem on points in convex position—a survey. *Bull. Amer. Math. Soc.* (*N.S.*) **37** (2000), 437–458.

[78] Okounkov, A., Random matrices and random permutations. *Internat. Math. Res. Notices* **2000** (2000), 1043–1095.

[79] Pemantle, R., private communications dated October 7 and October 9, 2005.

[80] Pittel, B., Romik, D., Limit shapes for random square Young tableaux and plane partitions. Preprint, 2004; arXiv.math.PR/0405190.

[81] Rains, E., Increasing subsequences and the classical groups. *Electron. J. Combin.* **5** (1998), Article R12 (electronic).

[82] Regev, A., Asymptotic values for degrees associated with strips of Young diagrams. *Adv. Math.* **41** (1981), 115–136.

[83] Reifegerste, A., On the diagram of 132-avoiding permutations. *European J. Combin.* **24** (2003), 759–776 (electronic).

[84] Robinson, G. de B., On the representations of S_n. *Amer. J. Math.* **60** (1938), 745–760.

[85] Romik, D., Permutations with short monotone subsequences. *Adv. Appl. Math.*, to appear; http://www.stat.berkeley.edu/∼romik/papers.html.

[86] Rotem, D., On a correspondence between binary trees and a certain type of permutation. *Information Processing Lett.* **4** (1975/76), 58–61.

[87] Ryan, K. M., On Schubert varieties in the flag manifold of $\mathrm{Sl}(n, C)$. *Math. Ann.* **276** (1987), 205–224.

[88] Sagan, B., *The Symmetric Group*. Second ed., Grad. Texts in Math. 203, Springer-Verlag, New York 2001.

[89] Schensted, C. E., Longest increasing and decreasing subsequences. *Canad. J. Math.* **13** (1961), 179–191.

[90] Schützenberger, M. P., Quelques remarques sur une construction de Schensted. *Math. Scand.* **12** (1963), 117–128.

[91] Schützenberger, M. P., Promotion des morphismes d'ensembles ordonnés. *Discrete Math.* **2** (1972), 73–94

[92] Seidenberg, A., A simple proof of a theorem of Erdős and Szekeres. *J. London Math. Soc.* **34** (1959), 352.

[93] Seppäläinen, T., Large deviations for increasing sequences on the plane. *Probab. Theory Related Fields* **112** (1998), 221–244.

[94] Simion, R., Schmidt, F., Restricted permutations. *European J. Combin.* **6** (1985), 383–406.

[95] Stankova, Z., West, J., Explicit enumeration of 321, hexagon-avoiding permutations. *Discrete Math.* **280** (2004), 165–189.

[96] Stanley, R., Differentiably finite power series. *European J. Combin.* **1** (1980), 175–188.

[97] Stanley, R., On the number of reduced decompositions of elements of Coxeter groups. *European J. Combin.* **5** (1984), 359–372.

[98] Stanley, R., *Enumerative Combinatorics*. Vol. 1, Wadsworth and Brooks/Cole, Pacific Grove, CA, 1986; second printing, Cambridge University Press, New York, Cambridge 1996.

[99] Stanley, R., *Enumerative Combinatorics*. Vol. 2. Cambridge University Press, New York, Cambridge 1999.

[100] Stanley, R., Catalan Addendum; http://www-math.mit.edu/∼rstan/ec/catadd.pdf.

[101] Stanley, R., Longest alternating subsequences of permutations. Preprint, 2005; arXiv:math.CO/0511419.

[102] Steele, M. J., Long unimodal subsequences: a problem of F. R. K. Chung. *Discrete Math.* **33** (1981), 223–225.

[103] Sundaram, S., The Cauchy identity for $\mathrm{Sp}(2n)$. *J. Combin. Theory Ser. A* **53** (1990), 209–238.

[104] Tenner, B. E., Pattern avoidance and the Bruhat order. *J. Combin. Theory Ser. A*, to appear.

[105] Tenner, B. E., Database of permutation pattern avoidance. http://www-math.mit.edu/∼bridget/cgi-bin/dppa.cgi.

[106] Tracy, C. A., Widom, H., Level-spacing distributions and the Airy kernel. *Comm. Math. Phys.* **159** (1994), 151–174.

[107] Tracy, C. A., Widom, H., On orthogonal and symplectic ensembles. *Comm. Math. Phys.* **177** (1996), 727–754.

[108] Tracy, C. A., Widom, H., Distribution functions for largest eigenvalues and their applications. In *Proc. International Congress of Mathematicians* (Beijing 2002), Vol. I, Higher Ed. Press, Beijing 2002, 587–596.

[109] Ulam, S. M., Monte Carlo calculations in problems of mathematical physics. In *Modern Mathematics for the Engineer: Second Series* (ed. by E. F. Beckenbach), McGraw-Hill, New York 1961, 261–281.

[110] Vershik, A. M., Kerov, S. V., Asymptotic behavior of the Plancherel measure of the symmetric group and the limit form of Young tableaux . *Dokl. Akad. Nauk SSSR* **223** (1977), 1024–1027; English translation: *Soviet Math. Dokl.* **233** (1977), 527–531.

[111] West, J., Permutations with forbidden subsequences; and, stack-sortable permutations. Ph.D. thesis, M.I.T., 1990.

[112] West, J., Generating trees and the Catalan and Schröder numbers. *Discrete Math.* **146** (1995), 247–262.

[113] West, J., Generating trees and forbidden subsequences. *Discrete Math.* **157** (1996), 363–374.

[114] Widom, H., On the limiting distribution for the longest alternating sequence in a random permutation. *Electron. J. Combin.* **13** (1) (2006), Article R25 (electronic).

[115] Wilf, H., The patterns of permutations. *Discrete Math.* **257** (2002), 575–583.

Richard Stanley, Massachusetts Institute of Technology, Department of Mathematics,
77 Massachessetts Avenue, Cambridge, MA 02139-4307, U.S.A.

E-mail: rstan@math.mit.edu

The dichotomy between structure and randomness, arithmetic progressions, and the primes

Terence Tao*

Abstract. A famous theorem of Szemerédi asserts that all subsets of the integers with positive upper density will contain arbitrarily long arithmetic progressions. There are many different proofs of this deep theorem, but they are all based on a fundamental dichotomy between structure and randomness, which in turn leads (roughly speaking) to a decomposition of any object into a structured (low-complexity) component and a random (discorrelated) component. Important examples of these types of decompositions include the Furstenberg structure theorem and the Szemerédi regularity lemma. One recent application of this dichotomy is the result of Green and Tao establishing that the prime numbers contain arbitrarily long arithmetic progressions (despite having density zero in the integers). The power of this dichotomy is evidenced by the fact that the Green–Tao theorem requires surprisingly little technology from analytic number theory, relying instead almost exclusively on manifestations of this dichotomy such as Szemerédi's theorem. In this paper we survey various manifestations of this dichotomy in combinatorics, harmonic analysis, ergodic theory, and number theory. As we hope to emphasize here, the underlying themes in these arguments are remarkably similar even though the contexts are radically different.

Mathematics Subject Classification (2000). Primary 11P32, 37A45, 05C65, 05C75, 42A99.

Keywords. Szemerédi's theorem, ergodic theory, graph theory, hypergraph theory, arithmetic combinatorics, arithmetic progressions, prime numbers.

1. Introduction

In 1975, Szemerédi [53] proved the following deep and enormously influential theorem:

Theorem 1.1 (Szemerédi's theorem). *Let A be a subset of the integers $\mathbb{Z}$ of positive upper density, thus* $\limsup_{N\to\infty} \frac{|A\cap[-N,N]|}{|[-N,N]|} > 0$. *Here $|A|$ denotes the cardinality of a set A, and $[-N, N]$ denotes the integers between $-N$ and N. Then for any $k \geq 3$, A contains infinitely many arithmetic progressions of length k.*

Several proofs of this theorem are now known. The original proof of Szemerédi [53] was combinatorial. A later proof of Furstenberg [11], [13] used ergodic theory and has led to many extensions. A more quantitative proof of Gowers [19], [20] was based on Fourier analysis and arithmetic combinatorics (extending a much older

*The author is supported by a grant from the Packard foundation.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

argument of Roth [50] handling the $k = 3$ case). A fourth proof by Gowers [21] and Rödl, Nagle, Schacht, and Skokan [46], [47], [48], [49] relied on the structural theory of hypergraphs. These proofs are superficially all very different (with each having their own strengths and weaknesses), but have a surprising number of features in common. The main difficulty in all of the proofs is that one *a priori* has no control on the behaviour of the set A other than a lower bound on its density; A could range from being a very random set, to a very structured set, to something in between. In each of these cases, A will contain many arithmetic progressions – but the *reason* for having these progressions varies from case to case. Let us illustrate this by informally discussing some representative examples:

- (Random sets) Let $0 < \delta < 1$, and let A be a random subset of $\mathbb{Z}$, which each integer n lying in A with an independent probability of δ. Then A almost surely has upper density δ, and it is easy to establish that A almost surely has infinitely many arithmetic progressions of length k, basically because each progression of length k in $\mathbb{Z}$ has a probability of δ^k of also lying in A. A more refined version of this argument also applies when A is *pseudorandom* rather than random – thus we allow A to be deterministic, but require that a suitable number of correlations (e.g. pair correlations, or higher order correlations) of A are negligible. The argument also extends to sparse random sets, for instance one where $\mathbf{P}(n \in A) \sim 1/\log n$.

- (Linearly structured sets) Consider a quasiperiodic set such as $A := \{n : \{\alpha n\} \leq \delta\}$, where $0 < \delta < 1$ is fixed, α is a real number (e.g. $\alpha = \sqrt{2}$) and $\{x\}$ denotes the fractional part of x. Such sets are "almost periodic" because there is a strong correlation between the events $n \in A$ and $n + L \in A$, thanks to the identity $\{\alpha(n + L)\} - \{\alpha n\} = \{\alpha L\} \mod 1$. An easy application of the Dirichlet approximation theorem (to locate an approximate period L with $\{\alpha L\}$ small) shows that such sets still have infinitely many progressions of any given length k. Note that this argument works regardless of whether α is rational or irrational.

- (Quadratically structured sets) Consider a "quadratically quasiperiodic" set of the form $A := \{n : \{\alpha n^2\} \leq \delta\}$. If α is irrational, then this set has upper density δ, thanks to Weyl's theorem on equidistribution of polynomials. (If α is rational, one can still obtain some lower bound on the upper density.) It is not linearly structured (there is no asymptotic correlation between the events $n \in A$ and $n + L \in A$ as $n \to \infty$ for any fixed non-zero L), however it has quadratic structure in the sense that there is a strong correlation between the events $n \in A$, $n + L \in A$, $n + 2L \in A$, thanks to the identity

$$\{\alpha n^2\} - 2\{\alpha(n + L)^2\} + \{\alpha(n + 2L)^2\} = 2\{\alpha L^2\} \mod 1.$$

  In particular A does not behave like a random set. Nevertheless, the quadratic structure still ensures that A contains infinitely many arithmetic progressions

of any length k, as one first locates a "quadratic period" L with $\{\alpha L^2\}$ small, and then for suitable $n \in A$ one locates a much smaller "linear period" M with $\{\alpha LMn\}$ small. If this is done correctly, the progression $n, n + LM, \ldots, n + (k-1)LM$ will be completely contained in A. The same arguments also extend to a more general class of quadratically structured sets, such as the "2-step nilperiodic" set $A = \{n : \{\lfloor\sqrt{2}n\rfloor\sqrt{3}n \leq \delta\}$, where $\lfloor x\rfloor$ is the greatest integer function.

- (Random subsets of structured sets) Continuing the previous example $A := \{n : \{\alpha n^2\} \leq \delta\}$, let A' be a random subset of A with each $n \in A$ lying in A' with an independent probability of δ' for some $0 < \delta' < 1$. Then this set A' almost surely has a positive density of $\delta\delta'$ if α is irrational. The set A' almost surely has infinitely many progressions of length k, since A already starts with infinitely many such progressions, and each such progression as a probability of $(\delta')^k$ of also lying in A'. One can generalize this example to random sets $\tilde{A}$ where the events $n \in \tilde{A}$ are independent as n varies, and the probability $\mathbf{P}(n \in \tilde{A})$ is a "quadratically almost periodic" function of n such as $\mathbf{P}(n \in \tilde{A}) = F(\{\alpha n^2\})$ for some nice (e.g. piecewise continuous) function F taking values between 0 and 1; the preceding example is the case where $F(x) := \delta' 1_{x<\delta}$. It is also possible to adapt this argument to (possibly sparse) pseudorandom subsets of structured sets, though one needs to take some care in defining exactly what "pseudorandom" means here.

- (Sets containing random subsets of structured sets) Let A'' be any set which contains the set A' (or $\tilde{A}$) of the previous example. Since A' contains infinitely many progressions of length k, it is trivial that A'' does also.

As the above examples should make clear, the reason for the truth of Szemerédi's theorem is very different in the cases when A is random, and when A is structured. These two cases can then be combined to handle the case when A is (or contains) a large (pseudo-)random subset of a structured set. Each of the proofs of Szemerédi's theorem now hinge on a *structure theorem* which, very roughly speaking, asserts that *every* set of positive density is (or contains) a large pseudorandom subset of a structured set; each of the four proofs obtains a structure theorem of this sort in a different way (and in a very different language). These remarkable structural results – which include the Furstenberg structure theorem and the Szemerédi regularity lemma as examples – are of independent interest (beyond their immediate applications to arithmetic progressions), and have led to many further developments and insights. For instance, in [27] a "weighted" structure theorem (which was in some sense a hybrid of the Furstenberg structure theorem and the Szemerédi regularity lemma) was the primary new ingredient in proving that the primes $P := \{2, 3, 5, 7, \ldots\}$ contained arbitrarily long arithmetic progressions. While that latter claim is ostensibly a number-theoretical result, the method of proof in fact uses surprisingly little from number theory, being much closer in spirit to the proofs of Szemerédi's theorem (and

in fact Szemerédi's theorem is a crucial ingredient in the proof). This can be seen from the fact that the argument in [27] in fact proves the following stronger result:

Theorem 1.2 (Szemerédi's theorem in the primes [27]). *Let A be a subset of the primes P of positive* relative *upper density, thus* $\limsup_{N\to\infty} \frac{|A\cap[-N,N]|}{|P\cap[-N,N]|} > 0$. *Then for any $k \geq 3$, A contains infinitely many arithmetic progressions of length k.*

This result was first established in the $k = 3$ case by Green [22], the key step again being a (Fourier-analytic) structure theorem, this time for subsets of the primes. The arguments used to prove this theorem do not directly address the important question of whether the primes P (or any subset thereof) have any pseudorandomness properties (but see Section 5 below). However, the structure theorem does allow one to (essentially) describe any dense subset of the primes as a (sparse) pseudorandom subset of some unspecified dense set, which turns out to be sufficient (thanks to Szemerédi's theorem) for the purpose of establishing the existence of arithmetic progressions.

There are now several expositions of Theorem 1.2; see for instance [42], [25], [55], [56], [37]. Rather than give yet another exposition of this result, we have chosen to take a broader view, surveying the collection of structural theorems which underlie the proof of such results as Theorem 1.1 and Theorem 1.2. These theorems have remarkably varied contexts – measure theory, ergodic theory, graph theory, hypergraph theory, probability theory, information theory, and Fourier analysis – and can be either qualitative (infinitary) or quantitative (finitary) in nature. However, their *proofs* tend to share a number of common features, and thus serve as a kind of "Rosetta stone" connecting these various fields. Firstly, for a given class of objects, one quantifies what it means for an object to be "(pseudo-)random" and an object to be "structured". Then, one establishes a *dichotomy between randomness and structure*, which typically looks something like this:

> *If an object is not* (*pseudo-*)*random, then it* (*or some non-trivial component of it*) *correlates with a structured object.*

One can then iterate this dichotomy repeatedly (e.g. via a stopping time argument, or by Zorn's lemma), to extract out all the correlations with structured objects, to obtain a *weak structure theorem* which typically looks as follows:

> *If A is an arbitrary object, then A* (*or some non-trivial component of A*) *splits as the sum of a structured object, plus a pseudorandom error.*

In many circumstances, we need to improve this result to a *strong structure theorem*:

> *If A is an arbitrary object, then A* (*or some non-trivial component of A*) *splits as the sum of a structured object, plus a small error, plus a* ***very*** *pseudorandom error.*

When one is working in an infinitary (qualitative) setting rather than a finitary (quantitative) one – which is for instance the case in the ergodic theory approach – one works instead with an *asymptotic structure theorem*:

If A is an arbitrary object, then A (or some non-trivial component of A) splits as the sum of a "compact" object (the limit of structured objects), plus an ***infinitely*** *pseudorandom error.*

The reason for the terminology "compact" to describe the limit of structured objects is in analogy to how a compact operator can be viewed as the limit of finite rank operators; see [12] for further discussion.

In many applications, the small or pseudorandom errors in these structure theorems are negligible, and one then reduces to the study of structured objects. One then exploits the structure of these objects to conclude the desired application.

Our focus here is on the structure theorems related to Szemerédi's theorem and related results such as Theorem 1.2; we will not have space to describe all the generalizations and refinements of these results here. However, these types of structural theorems appear in other contexts also, for instance the Komlós subsequence principle [40] in probability theory. The Lebesgue decomposition of a spectral measure into pure point, singular continuous, and absolutely continuous spectral components can also be viewed as a structure theorem of the above type. Also, the stopping time arguments which underlie the structural theorems here are also widely used in harmonic analysis, in particular obtaining fundamental decompositions such as the Calderón–Zygmund decomposition or the atomic decomposition of Hardy spaces (see e.g. [52]), as well as the tree selection arguments used in multilinear harmonic analysis (see e.g. [43]). It may be worth investigating whether there are any concrete connections between these disparate structural theorems.

2. Ergodic theory

We now illustrate the above general strategy in a number of contexts, beginning with the ergodic theory approach to Szemerédi's theorem, where the dichotomy between structure and randomness is particularly clean and explicit. Informally speaking, the ergodic theory approach seeks to understand the set A of integers by analyzing the asymptotic correlations of the shifts $A+n := \{a+n : a \in A\}$ (or of various asymptotic averages of these shifts), and treating these shifts as occurring on an abstract measure space. More formally, let X be a measure space with probability measure $d\mu$, and let $T\colon X \to X$ be a bijection such that T and T^{-1} are both measure-preserving maps. The associated shift operator $T\colon f \mapsto f \circ T^{-1}$ is thus a unitary operator on the Hilbert space $L^2(X)$ of complex-valued square-integrable functions with the usual inner product $\langle f, g\rangle := \int_X f\bar{g}\, d\mu$. A famous transference result known as the *Furstenberg correspondence principle*[1] (see [11], [13], [12]) shows that Szemerédi's

[1] Morally speaking, to deduce Szemerédi's theorem from Furstenberg's theorem, one takes X to be the integers $\mathbb{Z}$, T to be the standard shift $n \mapsto n+1$, and μ to be the density $\mu(A) = \lim_{N\to\infty} \frac{|A\cap[-N,N]|}{|[-N,N]|}$. This does not quite work because not all sets A have a well-defined density, however additional arguments (e.g. using the Hahn–Banach theorem) can fix this problem.

theorem is then equivalent to

Theorem 2.1 (Furstenberg recurrence theorem [11]). *Let X and T be as above, and let $f \in L^\infty(X)$ be any bounded non-negative function with $\int_X f\, d\mu > 0$. Then for any $k \geq 1$ we have*

$$\liminf_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X f T^n f \dots T^{(k-1)n} f\, d\mu > 0.$$

Here and in the sequel we use $\mathbf{E}_{n\in I} a_n$ as a shorthand for the average $\frac{1}{|I|}\sum_{n\in I} a_n$.

When $k = 2$ this is essentially the Poincaré recurrence theorem; by using the von Neumann ergodic theorem one can also show that the limit exists (thus the lim inf can be replaced with a lim). The $k = 3$ case can be proved by the following argument, as observed in [12]. We need to show that

$$\liminf_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X f T^n f T^{2n} f\, d\mu > 0 \tag{1}$$

whenever f is bounded, non-negative, and has positive integral.

The first key observation is that any sufficiently pseudorandom component of f will give a negligible contribution to (1) and can be dropped. More precisely, let us call f is *linearly pseudorandom* (or *weakly mixing*) with respect to the shift T if we have

$$\lim_{N\to\infty} \mathbf{E}_{1\leq n\leq N} |\langle T^n f, f\rangle|^2 = 0. \tag{2}$$

Such functions are negligible for the purpose of computing averages such as those in (1); indeed, if at least one of $f, g, h \in L^\infty(X)$ is linearly pseudorandom, then an easy application of van der Corput's lemma (which in turn is an application of Cauchy–Schwarz) shows that

$$\lim_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X f T^n g T^{2n} h\, d\mu = 0.$$

We shall refer to these types of results – that pseudorandom functions are negligible when averaged against other functions – as *generalized von Neumann theorems*.

In view of this generalized von Neumann theorem, one is now tempted to "quotient out" all the pseudorandom functions and work with a reduced class of "structured" functions. In this particular case, it turns out that the correct notion of structure is that of a *linearly almost periodic function*, which are in turn generated by the *linear eigenfunctions* of T. To make this more precise, we need the following dichotomy:

Lemma 2.2 (Dichotomy between randomness and structure). *Suppose that $f \in L^\infty(X)$ is not linearly pseudorandom. Then there exists an linear eigenfunction $g \in L^\infty(X)$ of T (thus $Tg = \lambda g$ for some $\lambda \in \mathbb{C}$) such that $\langle f, g\rangle \neq 0$.*

Remark 2.3. Observe that if g is a linear eigenfunction of T with $Tg = \lambda g$, then $|\lambda| = 1$ and $\lim_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X gT^n\bar{g}^2T^{2n}g\, d\mu = \int_X |g|^4$. Thus linear eigenfunctions can and do give nontrivial contributions to the expression in (1). One can view Lemma 2.2 as a converse to this observation.

The proof of this lemma follows easily from spectral theory and is omitted here. It has the following consequence. Let $\mathcal{Z}_1$ be the σ-algebra generated by all the eigenfunctions of T, this is known as the *Kronecker factor* of X, and roughly speaking encapsulates all the "linear structure" in the measure preserving system. Given every function $f \in L^2(X)$, we have the decomposition $f = f_{U^\perp} + f_U$, where $f_{U^\perp} := \mathbf{E}(f|\mathcal{Z}_1)$ is the conditional expectation of f with respect to the σ-algebra $\mathcal{Z}_1$ (i.e. the orthogonal projection from $L^2(X)$ to the $\mathcal{Z}_1$-measurable functions). By construction, $f_U := f - \mathbf{E}(f|\mathcal{Z}_1)$ is orthogonal to every eigenfunction of T, and is hence linearly pseudorandom by Lemma 2.2. In particular, we have established

Proposition 2.4 (Asymptotic structure theorem). *Let f be bounded and non-negative, with positive integral. Then we can split*[2] *$f = f_{U^\perp} + f_U$, where $f_{U^\perp}$ is bounded, non-negative, and $\mathcal{Z}_1$-measurable* (*and thus approximable in L^2 to arbitrary accuracy by finite linear combinations of linear eigenfunctions*)*, with positive integral, and f_U is linearly pseudorandom.*

This result is closely related to the Koopman–von Neumann theorem in ergodic theory. In the language of the introduction, it asserts (very roughly speaking) that any set A of integers can be viewed as a (linearly) pseudorandom set where the "probability" $f_{U^\perp}(n)$ that a given element n lies in A is a (linearly) almost periodic function of n.

Note that the linearly pseudorandom component f_U of f gives no contribution to (1), thanks to the generalized von Neumann theorem. Thus we may freely replace f by $f_{U^\perp}$ if desired; in other words, for the purposes of proving (1) we may assume without loss of generality that f is measurable with respect to the Kronecker factor $\mathcal{Z}_1$. In the notation of [14], we have just shown that the Kronecker factor is a *characteristic factor* for the recurrence in (1). (In fact it is essentially the universal factor for this recurrence, see [64], [39] for further discussion.)

We have reduced the proof of (1) to the case when f is structured, in the sense of being measurable in $\mathcal{Z}_2$. There are two ways to obtain the desired "structured recurrence" result. Firstly there is a "soft" approach, in which one observes that every $\mathcal{Z}_1$-measurable square-integrable function f is *almost periodic*, in the sense that for any $\varepsilon > 0$ there exists a set of integers n of positive density such that $T^n f$ is within ε of f in $L^2(X)$; from this it is easy to show that $\int_X fT^n fT^{2n} f\, d\mu$ is close to $\int_X f^3$ for a set of integers n of positive density, which implies (1). This almost periodicity can be verified by first checking it for polynomial combinations of linear eigenfunctions, and then extending by density arguments. There is also a "hard"

[2] The notation is from [27]; the subscript U stands for "Gowers uniform" (pseudorandom), and $U^\perp$ for "Gowers anti-uniform" (structured).

approach, in which one obtains algebraic and topological control on the Kronecker factor $\mathcal{Z}_1$. In fact, from a spectral analysis of T one can show that $\mathcal{Z}_1$ is the inverse limit of a sequence of σ-algebras, on each of which the shift T is isomorphic to a shift $x \mapsto x + \alpha$ on a compact abelian Lie group G. This gives a very concrete description of the functions f which are measurable in the Kronecker factor, and one can establish (1) by a direct argument similar to that used in the introduction for linearly structured sets. This "hard" approach gives a bit more information; for instance, it can be used to show that the limit in (1) actually converges, so one can replace the lim inf by a lim.

It turns out that these arguments extend (with some non-trivial effort) to the case of higher k. For sake of exposition let us just discuss the $k = 4$ case, though most of the assertions here extend to higher k. We wish to prove that

$$\liminf_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X f T^n f T^{2n} f T^{3n} f \, d\mu > 0 \tag{3}$$

whenever f is bounded, non-negative, and has positive integral. Here, it turns out that we must strengthen the notion of pseudorandomness (and hence generalize the notion of structure); linear pseudorandomness is no longer sufficient to imply negligibility. For instance, let f be a *quadratic eigenfunction*, in the sense that $Tf = \lambda f$, where λ is no longer constant but is itself a linear eigenfunction, thus $T\lambda = c\lambda$ for some constant c. As an example, if $X = (\mathbb{R}/\mathbb{Z})^2$ with the skew shift $T(x, y) = (x+\alpha, y+x)$ for some fixed number α, then the function $f(x, y) = e^{2\pi i y}$ is a quadratic eigenfunction but not a linear one. Typically such quadratic eigenfunctions will be linearly pseudorandom, but if $|\lambda| = |c| = 1$ (which is often the case) then we have the identity

$$\mathbf{E}_{1\leq n\leq N} \int_X f T^n \bar{f}^3 T^{2n} f^3 T^{3n} \bar{f} \, d\mu = \int_X |f|^8 \, d\mu \tag{4}$$

and so we see that these functions can give non-trivial contributions to expressions such as (1). The correct notion of pseudorandomness is now *quadratic pseudorandomness*, by which we mean that

$$\lim_{H\to\infty} \lim_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \mathbf{E}_{1\leq h\leq H} |\langle T^h f \bar{f}, T^n (T^h f \bar{f})\rangle|^2 = 0.$$

In other words, f is quadratically pseudorandom if and only if $T^h f \bar{f}$ is asymptotically linearly pseudorandom on the average as $h \to \infty$. Several applications of van der Corput's lemma give a generalized von Neumann theorem, asserting that

$$\lim_{N\to\infty} \mathbf{E}_{1\leq n\leq N} \int_X f_0 T^n f_1 T^{2n} f_2 T^{3n} f_3 \, d\mu = 0$$

whenever f_0, f_1, f_2, f_3 are bounded functions with at least one function quadratically pseudorandom.

One would now like to construct a factor $\mathcal{Z}_2$ (presumably larger than the Kronecker factor $\mathcal{Z}_2$) which will play the role of the Kronecker factor for the average (3); in particular, we would like a statement of the form

Lemma 2.5 (Dichotomy between randomness and structure). *Suppose that $f \in L^\infty(X)$ is not linearly pseudorandom. Then there exists a $\mathcal{Z}$-measurable function $g \in L^\infty(X)$ such that $\langle f, g\rangle \neq 0$.*

which would imply[3]

Proposition 2.6 (Asymptotic structure theorem). *Let f be bounded and non-negative, with positive integral. Then we can split $f = f_{U^\perp} + f_U$, where $f_{U^\perp}$ is bounded, non-negative, and $\mathcal{Z}_2$-measurable, with positive integral,and f_U is quadratically pseudorandom.*

This reduces the proof of (3) to that of $\mathcal{Z}_2$-measurable f. The existence of such a factor $\mathcal{Z}_2$ (which would be a *characteristic factor* for this average) is trivial to construct, as we could just take $\mathcal{Z}_2$ to be the entire σ-algebra, and it is in fact easy (via Zorn's lemma) to show the existence of a "best" such factor, which embed into all other characteristic factors for this average (see [64]). Of course, for the concept of characteristic factor to be useful we would like $\mathcal{Z}_2$ to be smaller than this, and specifically for the functions in this factor to enjoy some structural properties. An obvious guess for $\mathcal{Z}_2$ would be the σ-algebra generated by all the linear and quadratic eigenfunctions, but this factor turns out to be a bit too small (see [14]; this is related to the example of the 2-step nilperiodic set in the introduction). A more effective candidate for $\mathcal{Z}_2$, analogous to the "soft" description of the Kronecker factor, is the space of all "quadratically almost periodic functions". This concept is a bit tricky to define rigorously (see e.g. [13], [12], [54]), but roughly speaking, a function f is linearly almost periodic if the orbit $\{T^n f : n \in \mathbb{Z}\}$ is precompact in $L^2(X)$ viewed as a Hilbert space, while a function f is quadratically almost periodic if the orbit is precompact in $L^2(X)$ viewed as a Hilbert *module* over the Kronecker factor $L^\infty(\mathcal{Z}_1)$; this can be viewed as a matrix-valued (or more precisely compact operator-valued) extension of the concept of a quadratic eigenfunction. Another rough definition is as follows: a function f is linearly almost periodic if $T^n f(x)$ is close to $f(x)$ for many constants n, whereas a function f is quadratically almost periodic if $T^{n(x)} f(x)$ is close to $f(x)$ for a function $n(x)$ which is itself linearly almost periodic. It turns out that with this "soft" proposal for $\mathcal{Z}_2$, it is easy to prove Lemma 2.5 and hence Proposition 2.6, essentially by obtaining a "relative" version of the proof of Lemma 2.2. The derivation of (3) in this soft factor is slightly tricky though, requiring either van der Waerden's theorem, or the color focusing argument used to prove van der Waerden's theorem; see [11], [13], [12], [54].

More recently, a more efficient "hard" factor $\mathcal{Z}_2$ was constructed by Conze–Lesigne [7], Furstenberg–Weiss [14], and Host–Kra [38]; the analogous factors for

[3] One can generalize this structure theorem to obtain similar characteristic factors $\mathcal{Z}_3$, $\mathcal{Z}_4$ for cubic pseudorandomness, quartic pseudorandomness, etc. Applying Zorn's lemma, one eventually obtains the *Furstenberg structure theorem*, which decomposes any measure preserving system as a weakly mixing extension of a distal system, and thus decomposes any function as a distal function plus an "infinitely pseudorandom" error; see [13]. However this decomposition is not the most "efficient" way to prove Szemerédi's theorem, as the notion of pseudorandomness is too strong, and hence the notion of structure too general. It does illustrate however that one does have considerable flexibility in where to draw the line between randomness and structure.

higher k are more difficult to construct, but this was achieved by Host–Kra in [39], and also subsequently by Ziegler [64]. This factor yields more precise information, including convergence of the limit in (3). Here, the concept of a 2-*step nilsystem* is used to define structure. A 2-step nilsystem is a compact symmetric space G/Γ, with G a 2-step nilpotent Lie group and Γ is a closed subgroup, together with a shift element $\alpha \in G$, which generates a shift $T(x\Gamma) := \alpha x\Gamma$. The factor $\mathcal{Z}_2$ constructed in these papers is then the inverse limit of a sequence of σ-algebras, on which the shift is equivalent to a 2-step nilsystem. This should be compared with the "hard" description of the Kronecker factor, which is the 1-step analogue of the above result. Establishing the bound (3) then reduces to the problem of understanding the structure of arithmetic progressions $x\Gamma$, $\alpha x\Gamma$, $\alpha^2 x\Gamma$, $\alpha^3 x\Gamma$ on the nilsystem, which can be handled by algebraic arguments, for instance using the machinery of Hall–Petresco sequences [44].

The ergodic methods, while non-elementary and non-quantitative (though see [54]), have proven to be the most powerful and flexible approach to Szemerédi's theorem, leading to many generalizations and refinements. However, it seems that a purely "soft" ergodic approach is not quite capable by itself of extending to the primes as in Theorem 1.2, though it comes tantalizingly close. In particular, one can use Theorem 2.1 and a variant of the Furstenberg correspondence principle to establish Theorem 1.2 when the set of primes P is replaced by a random subset $\tilde{P}$ of the positive integers, with $n \in \tilde{P}$ with independent probability $1/\log n$ for $n > 1$; see [60]. Roughly speaking, if A is a subset of $\tilde{P}$, the idea is to construct an abstract measure-preserving system generated by a set $\tilde{A}$, in which $\mu(T^{n_1}\tilde{A} \cap \cdots \cap T^{n_k}\tilde{A})$ is the normalized density of $(A+n_1) \cap \cdots \cap (A+n_k)$ for any $n_1, \ldots, n_k$. Unfortunately, this approach requires the ambient space $\tilde{P}$ to be extremely pseudorandom and does not seem to extend easily to the primes.

3. Fourier analysis

We now turn to a more quantitative approach to Szemerédi's theorem, based primarily on Fourier analysis and arithmetic combinatorics. Here, one analyzes a set of integers A finitarily, truncating to a finite setting such as the discrete integral $\{1, \ldots, N\}$ or the cyclic group $\mathbb{Z}/N\mathbb{Z}$, and then testing the correlations of A with linear phases such as $n \mapsto e^{2\pi ikn/N}$, quadratic phases $n \mapsto e^{2\pi ikn^2/N}$, or similar objects. This approach has lead to the best known bounds on Szemerédi's theorem, though it has not yet been able to handle many of the generalizations of this theorem that can be treated by ergodic or graph-theoretic methods. In analogy with the ergodic arguments, the $k = 3$ case of Szemerédi's theorem can be handled by linear Fourier analysis (as was done by Roth [50]), while the $k = 4$ case requires quadratic Fourier analysis (as was done by Gowers [19]), and so forth for higher order k (see [20]). The Fourier analytic approach seems to be closely related to the theory of the "hard" characteristic

factors discovered in the ergodic theory arguments, although the precise nature of this relationship is still being understood.

It is convenient to work in a cyclic group $\mathbb{Z}/N\mathbb{Z}$ of prime order. It can be shown via averaging arguments (see [63]) that Szemerédi's theorem is equivalent to the following quantitative version:

Theorem 3.1 (Szemerédi's theorem, quantitative version). *Let $N > 1$ be a large prime, let $k \geq 3$, and let $0 < \delta < 1$. Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ be a function with $0 \leq f(x) \leq 1$ for all $x \in \mathbb{Z}/N\mathbb{Z}$ and $\mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} f(x) \geq \delta$. Then we have*

$$\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f(x)T^r f(x)\dots T^{(k-1)r} f(x) \geq c(k,\delta)$$

for some $c(k,\delta) > 0$ depending only on k and δ, where $T^r f(x) := f(x+r)$ is the shift operator on $\mathbb{Z}/N\mathbb{Z}$.

We remark that the Fourier-analytic arguments in Gowers [20] give the best known lower bounds on $c(k,\delta)$, namely $c(k,\delta) > 2^{-2^{1/\delta^{c_k}}}$ where $c_k := 2^{2^{k+9}}$. In the $k = 3$ case it is known that $c(3,\delta) \geq \delta^{C/\delta^2}$ for some absolute constant C, see [5]. A conjecture of Erdős and Turán [8] is roughly equivalent to asserting that $c(k,\delta) > e^{-C_k/\delta}$ for some C_k. In the converse direction, an example of Behrend shows that $c(3,\delta)$ cannot exceed $e^{c\log^2(1/\delta)}$ for some small absolute constant c, with similar results for higher values of k; in particular, $c(k,\delta)$ cannot be as large as any fixed power of δ. This already rules out a number of elementary approaches to Szemerédi's theorem and suggests that any proof must involve some sort of iterative argument.

Let us first describe (in more "modern" language) Roth's original proof [50] of Szemerédi's theorem in the $k = 3$ case. We need to establish a bound of the form

$$\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f(x)T^r f(x)T^{2r} f(x) \geq c(3,\delta) > 0 \tag{5}$$

when f takes values between 0 and 1 and has mean at least δ. As in the ergodic argument, we first look for a notion of pseudorandomness which will ensure that the average in (5) is negligible. It is convenient to introduce the *Gowers $U^2(\mathbb{Z}/N\mathbb{Z})$ uniformity norm* by the formula

$$\|f\|^4_{U^2(\mathbb{Z}/N\mathbb{Z})} := \mathbf{E}_{n\in\mathbb{Z}/N\mathbb{Z}}|\mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} T^n f(x)\,\overline{f(x)}|^2,$$

and informally refer to f as *linearly pseudorandom* (or *linearly Gowers-uniform*) if its U^2 norm is small; compare this with (2). The U^2 norm is indeed a norm; this can be verified either by several applications of the Cauchy–Schwarz inequality, or via the Fourier identity

$$\|f\|^4_{U^2(\mathbb{Z}/N\mathbb{Z})} = \sum_{\xi\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}(\xi)|^4, \tag{6}$$

where $\hat{f}(\xi) := \mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} f(x)e^{-2\pi i x\xi/N}$ is the usual Fourier transform. Some further applications of Cauchy–Schwarz (or Plancherel's theorem and Hölder's inequality)

yields the generalized von Neumann theorem

$$|\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f_0(x)T^r f_1(x)T^{2r} f_2(x)| \leq \min_{j=0,1,2} \|f_j\|_{U^2(\mathbb{Z}/N\mathbb{Z})} \tag{7}$$

whenever f_0, f_1, f_2 are bounded in magnitude by 1. Thus, as before, linearly pseudorandom functions give a small contribution to the average in (5), though now that we are in a finitary setting the contribution does not vanish completely.

The next step is to establish a dichotomy between linear pseudorandomness and some sort of usable structure. From (6) and Plancherel's theorem we easily obtain the following analogue of Lemma 2.2:

Lemma 3.2 (Dichotomy between randomness and structure). *Suppose that the function $f: \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ is bounded in magnitude by 1 with $\|f\|_{U^2(\mathbb{Z}/N\mathbb{Z})} \geq \eta$ for some $0 < \eta < 1$. Then there exists a linear phase function $\phi: \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ (thus $\phi(x) = \xi x/N + c$ for some $\xi \in \mathbb{Z}/N\mathbb{Z}$ and $c \in \mathbb{R}/\mathbb{Z}$) such that $|\mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} f(x)e^{-2\pi i\phi(x)}| \geq \eta^2$.*

The next step is to iterate this lemma to obtain a suitable structure theorem. There are two slightly different ways to do this. Firstly there is the original *density increment argument* approach of Roth [50], which we sketch as follows. It is convenient to work on a discrete interval $[1, N/3]$, which we identify with a subset of $\mathbb{Z}/N\mathbb{Z}$ in the obvious manner. Let $f: [1, N/3] \to \mathbb{R}$ be a non-negative function bounded in magnitude by 1, and let η be a parameter to be chosen later. If $f - \mathbf{E}_{1\leq x\leq N/3} f(x)$ is not linearly pseudorandom, in the sense that $\|f - \mathbf{E}_{1\leq x\leq N/3} f(x)\|_{U^2(\mathbb{Z}/N\mathbb{Z})} \geq \eta$, then we apply Lemma 3.2 to obtain a correlation with a linear phase ϕ. An easy application of the Dirichlet approximation theorem then shows that one can partition $[1, N/3]$ into arithmetic progressions (of length roughly $\eta^2\sqrt{N}$) on which ϕ is essentially constant (fluctuating by at most $\eta^2/100$, say). A pigeonhole argument (exploiting the fact that $f - \mathbf{E}_{1\leq x\leq N/3} f(x)$ has mean zero) then shows that on one of these progressions, say P, f has significantly higher density than on the average, in the sense that $\mathbf{E}_{x\in P} f(x) \geq \mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} f(x) + \eta^2/100$. One can then apply an affine transformation to convert this progression P into another discrete interval $\{1, \ldots, N'/3\}$, where N' is essentially the square root of N. One then iterates this argument until linear pseudorandomness is obtained (using the fact that the density of f cannot increase beyond 1), and one eventually obtains

Theorem 3.3 (Local structure theorem). *Let $f: [1, N/3] \to \mathbb{R}$ be a non-negative function bounded by 1, and let $\eta > 0$. Then there exists a progression P in $[1, N/3]$ of length at least $c(\eta)N^{c(\eta)}$ for some $c(\eta) > 0$, on which we have the splitting $f = f_{U^\perp} + f_U$, where $f_U^\perp := \mathbf{E}_{x\in P} f(x) \geq \mathbf{E}_{1\leq x\leq N/3} f(x)$ is the mean of f on P, and f_U is linearly pseudorandom in the sense that*

$$\|f_U\|_{U^2(\mathbb{Z}/M\mathbb{Z})} \leq \eta$$

where we identify P with a subset of a cyclic group $\mathbb{Z}/M\mathbb{Z}$ of cardinality $M \approx 3|P|$ in the usual manner.

More informally, any function will contain an arithmetic progression P of significant size on which f can be decomposed into a non-trivial structured component $f_{U^\perp}$ and a pseudorandom component f_U. In the language of the introduction, it is essentially saying that any dense set A of integers will contain components which are dense pseudorandom subsets of long progressions. Once one has this theorem, it is an easy matter to establish Szemerédi's theorem in the $k = 3$ case. Indeed, if $A \subseteq \mathbb{Z}$ has upper density greater than δ, then we can find arbitrarily large primes N such that $|A \cap [1, N/3]| \geq \delta N/3$. Applying Theorem 3.3 with $\eta := \delta^3/100$, and f equal to the indicator function of $A \cap [1, N/3]$, we can find a progression P in $\{1, \ldots, N/3\}$ of length at least $c(\delta)N^{c(\delta)}$ on which $\mathbf{E}_{x\in P} f(x) \geq \delta$ and $f - \mathbf{E}_{x\in P} f(x)$ is linearly pseudorandom in the sense of Theorem 3.3. It is then an easy matter to apply the generalized von Neumann theorem to show that $A \cap P$ contains many arithmetic progressions of length three (in fact it contains $\gg \delta^3|P|^3$ such progressions). Letting N (and hence $|P|$) tend to infinity we obtain Szemerédi's theorem in the $k = 3$ case. An averaging argument of Varnavides [63] then yields the more quantitative version in Theorem 3.1 (but with a moderately bad bound for $c(3, \delta)$, namely $c(3, \delta) = 2^{-2^{C/\delta^C}}$ for some absolute constant C).

A more refined structure theorem was given in [23] (see also [35]), which was termed an "arithmetic regularity lemma" in analogy with the Szemerédi regularity lemma which we discuss in the next section. That theorem has similar hypotheses to Theorem 3.3, but instead of constructing a single progression on P on which one has pseudorandomness, one partitions $[1, N/3]$ into *many* long progressions[4], where on most of which the function f becomes linearly pseudorandom (after subtracting the mean). A related structure theorem (with a more "ergodic" perspective) was also given in [56]. Here we give an alternate approach based on Fourier expansion and the pigeonhole principle. Observe that for any $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and any threshold λ we have the Fourier decomposition $f = f_{U^\perp} + f_U$, where the "structured" component $f_{U^\perp} := \sum_{\xi:|\hat{f}(\xi)|\geq\lambda} \hat{f}(\xi)e^{2\pi ix\xi/N}$ contains all the significant Fourier coefficients, and the "pseudorandom" component $f_U := \sum_{\xi:|\hat{f}(\xi)|\leq\lambda} \hat{f}(\xi)e^{2\pi ix\xi/N}$ contains all the small Fourier coefficients. Using Plancherel's theorem one can easily establish

Theorem 3.4 (Weak structure theorem). *Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ be a function bounded in magnitude by* 1*, and let $0 < \lambda < 1$. Then we can split $f = f_{U^\perp} + f_U$, where $f_{U^\perp}$ is the linear combination of at most $O(1/\lambda^2)$ linear phase functions $x \mapsto e^{2\pi ix\xi/N}$, and f_U is linearly pseudorandom in the sense that $\|f_U\|_{U^2(\mathbb{Z}/N\mathbb{Z})} \leq \lambda$.*

This theorem asserts that an arbitrary bounded function only has a bounded amount of significant linear Fourier-analytic structure; after removing this bounded amount of structure, the remainder is linearly pseudorandom.

This theorem, while simple to state and prove, has two weaknesses which make it unsuitable for such tasks as counting progressions of length three. Firstly, even

[4]Actually, for technical reasons it is more efficient to replace the notion of an arithmetic progression by a slightly different object known as a *Bohr set*; see [23], [35] for details.

though f is bounded by 1, the components $f_{U^\perp}$, f_U need not be. Related to this, if f is non-negative, there is no reason why $f_{U^\perp}$ should be non-negative also. Secondly, the pseudorandomness control on f_U is not very good when compared against the complexity of $f_{U^\perp}$ (i.e. the number of linear exponentials needed to describe $f_{U^\perp}$). In practice, this means that any control one obtains on the structured component of f will be dominated by the errors one has to concede from the pseudorandom component. Fortunately, both of these defects can be repaired, the former by a Fejér summation argument, and the latter by a pigeonhole argument (which introduces a second error term f_S, which is small in L^2 norm). More precisely, we have

Theorem 3.5 (Strong structure theorem). *Let $f: \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ be a non-negative function bounded by* 1*, and let $0 < \varepsilon < 1$. Let $F: \mathbb{N} \to \mathbb{N}$ be an arbitrary increasing function (e.g. $F(n) = 2^{2^n}$). Then there exists an integer $T = O_{F,\varepsilon}(1)$ and a decomposition $f = f_{U^\perp} + f_S + f_U$, where $f_{U^\perp}$ is the linear combination of at most T linear phase functions, f_U is linearly pseudorandom in the sense that $\|f_U\|_{U^2(\mathbb{Z}/N\mathbb{Z})} = O(1/F(T))$, and f_S is small in the sense that $\|f_S\|_{L^2(\mathbb{Z}/N\mathbb{Z})} := (\mathbf{E}_{n\in\mathbb{Z}/N\mathbb{Z}}|f_S(n)|^2)^{1/2} = O(\varepsilon)$. Furthermore, $f_{U^\perp}$, f_U are bounded in magnitude by* 1*. Also, $f_{U^\perp}$ and $f_{U^\perp} + f_S$ are non-negative with the same mean as f.*

This theorem can be proven by adapting arguments from [26], [35], or [56]; we omit the details. Note that we have the freedom to set the growth function F arbitrarily fast in the above proposition; this corresponds roughly speaking to the fact that in the ergodic counterpart to this structure theorem (Proposition 2.4) the pseudorandom error f_U has asymptotically *vanishing* Gowers U^2 norm. One can view $f_{U^\perp}$ as a "coarse" Fourier approximation to f, and $f_{U^\perp} + f_S$ as a "fine" Fourier approximation to f; this perspective links this proposition with the graph regularity lemmas that we discuss in the next section.

Theorem 3.5 can be used to deduce the structure theorems in [23], [56], [35], while a closely related result was also established in [4]. It can also be used to directly derive the $k = 3$ case of Theorem 3.1, as follows. Let f be as in that proposition, and let $\varepsilon := \delta^3/100$. We apply Theorem 3.5 to decompose $f = f_{U^\perp} + f_S + f_U$. Because $f_{U^\perp}$ has only T Fourier exponentials, it is easy to see that $f_{U^\perp}$ is almost periodic, in the sense that $\|T^n f_{U^\perp} - f_{U^\perp}\|_{L^2(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon$ for at least $\sigma(\varepsilon, T)N$ values of $n \in \mathbb{Z}/N\mathbb{Z}$, for some $\sigma(\varepsilon, T) > 0$. For such values of n, one can easily verify that

$$\mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} f_{U^\perp}(x) T^n f_{U^\perp}(x) T^{2n} f_{U^\perp}(x) \geq \delta^3/2.$$

Because f_S is small, we can also deduce that

$$\mathbf{E}_{x\in\mathbb{Z}/N\mathbb{Z}} (f_{U^\perp} + f_S)(x) T^n (f_{U^\perp} + f_S)(x) T^{2n} (f_{U^\perp} + f_S)(x) \geq \delta^3/4$$

for these values of n. Averaging in n (and taking advantage of the non-negativity of $f_{U^\perp} + f_S$) we conclude that

$$\mathbf{E}_{x,n\in\mathbb{Z}/N\mathbb{Z}} (f_{U^\perp} + f_S)(x) T^n (f_{U^\perp} + f_S)(x) T^{2n} (f_{U^\perp} + f_S)(x) \geq \delta^3 \sigma(\varepsilon, T)/4.$$

Adding in the pseudorandom error f_U using the generalized von Neumann theorem (7), we conclude that

$$\mathbf{E}_{x,n\in\mathbb{Z}/N\mathbb{Z}} f(x)T^n f(x)T^{2n} f(x) \geq \delta^3\sigma(\varepsilon, T)/4 - O(1/F(T)).$$

If we choose F to be sufficiently rapidly growing depending on δ and ε, we can absorb the error term in the main term and conclude that

$$\mathbf{E}_{x,n\in\mathbb{Z}/N\mathbb{Z}} f(x)T^n f(x)T^{2n} f(x) \geq \delta^3\sigma(\varepsilon, T)/8.$$

Since $T = O_{F,\varepsilon}(1) = O_\delta(1)$, we obtain the $k = 3$ case of Theorem 3.1 as desired.

Roth's original Fourier-analytic argument was published in 1953. But the extension of this Fourier argument to the $k > 3$ case was not achieved until the work of Gowers [19], [20] in 1998. For simplicity we once again restrict attention to the $k = 4$ case, where the theory is more complete. Our objective is to show

$$\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f(x)T^r f(x)T^{2r} f(x)T^{3r} f(x) \geq c(4,\delta) > 0 \tag{8}$$

whenever f is non-negative, bounded by 1, and has mean at least δ. There are some significant differences between this case and the $k = 3$ case (5). Firstly, linear pseudorandomness is not enough to guarantee that a contribution to (8) is negligible: for instance, if $f(x) := e^{2\pi i\xi x^2/N}$, then

$$\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f(x)T^r \bar{f}^3(x)T^{2r} f^3(x)T^{3r} \bar{f}(x) = 1$$

despite f being very linearly pseudorandom (the U^2 norm of f is $N^{-1/4}$); compare this example with (4). One must now utilize some sort of "quadratic Fourier analysis" in order to capture the correct concept of pseudorandomness and structure. Secondly, the Fourier-analytic arguments must now be supplemented by some results from arithmetic combinatorics (notably the Balog–Szemerédi theorem, and results related to Freiman's inverse sumset theorem) in order to obtain a usable notion of quadratic structure. Finally, as in the ergodic case, one cannot rely purely on quadratic phase functions such as $e^{2\pi i(\xi x^2+\eta x)/N}$ to generate all the relevant structured objects, and must also consider generalized quadratic objects such as locally quadratic phase functions, 2-step nilsequences (see below), or bracket quadratic phases such as $e^{2\pi i\lfloor\sqrt{2}n\rfloor\sqrt{3}n}$.

Let us now briefly sketch how the theory works in the $k = 4$ case. The correct notion of pseudorandomness is now given by the *Gowers U^3 uniformity norm*, defined by

$$\|f\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})} := \mathbf{E}_{n\in\mathbb{Z}/N\mathbb{Z}} \|T^n f\bar{f}\|^4_{U^2(\mathbb{Z}/N\mathbb{Z})}.$$

This norm measures the extent to which f behaves quadratically; for instance, if $f = e^{2\pi i P(x)/N}$ for some polynomial P of degree k in the finite field $\mathbb{Z}/N\mathbb{Z}$, then one can verify that $\|f\|_{U^3(\mathbb{Z}/N\mathbb{Z})} = 1$ if P has degree at most 2, but (using the Weil

estimates) we have $\|f\|_{U^3(\mathbb{Z}/N\mathbb{Z})} = O_k(N^{-1/16})$ if P has degree $k > 2$. Repeated application of Cauchy–Schwarz then yields the generalized von Neumann theorem

$$|\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}} f_0(x)T^r f_1(x)T^{2r} f_2(x)T^{3r} f_3(x)| \leq \min_{0\leq j\leq 3} \|f_j\|_{U^3(\mathbb{Z}/N\mathbb{Z})} \qquad (9)$$

whenever f_0, f_1, f_2, f_3 are bounded in magnitude by 1. The next step is to establish a dichotomy between quadratic structure and quadratic pseudorandomness in the spirit of Lemma 3.2. In the original work of Gowers [19], it was shown that a function which was not quadratically pseudorandom had local correlation with quadratic phases on medium-length arithmetic progressions. This result (when combined with the density increment argument of Roth) was already enough to prove (8) with a reasonable bound on $c(4, \delta)$ (basically of the form $1/\exp(\exp(\delta^{-C}))$); see [19], [20]. Building upon this work, a stronger dichotomy, similar in spirit to Lemma 2.5, was established in [29]. Here, a number of essentially equivalent formulations of quadratic structure were established, but the easiest to state (and the one which generalizes most easily to higher k) is that of a *(basic)* 2*-step nilsequence*, which can be viewed as a notion of "quadratic almost periodicity" for sequences. More precisely, a 2-step nilsequence a sequence of the form $n \mapsto F(T^n x\Gamma)$, where F is a Lipschitz function on a 2-step nilmanifold G/Γ, $x\Gamma$ is a point in this nilmanifold, and T is a shift operator $T: x\Gamma \mapsto \alpha x\Gamma$ for some fixed group element $\alpha \in G$. We remark that quadratic phase sequences such as $n \mapsto e^{2\pi i\alpha n^2}$ are examples of 2-step nilsequences, and generalized quadratics such as $n \mapsto e^{2\pi i\lfloor\sqrt{2}n\rfloor\sqrt{3}n}$ can also be written (outside of sets of arbitrarily small density) as 2-step nilsequences.

Lemma 3.6 (Dichotomy between randomness and structure [29]). *Suppose that* $f: \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ *is bounded in magnitude by* 1 *with* $\|f\|_{U^3(\mathbb{Z}/N\mathbb{Z})} \geq \eta$ *for some* $0 < \eta < 1$. *Then there exists a* 2*-step nilsequence* $n \mapsto F(T^n x\Gamma)$, *where* G/Γ *is a nilmanifold of dimension* $O_\eta(1)$, *and* F *is a bounded Lipschitz function* G/Γ *with Lipschitz constant* $O_\eta(1)$, *such that* $|\mathbf{E}_{1\leq x\leq N} f(x)\overline{F(T^n x\Gamma)}| \geq c(\eta)$ *for some* $c(\eta) > 1$. (*We identify the integers from* 1 *to* N *with* $\mathbb{Z}/N\mathbb{Z}$ *in the usual manner.*)

In fact the nilmanifold G/Γ constructed in [29] is of a very explicit form, being the direct sum of at most $O_\eta(1)$ circles (which are one-dimensional), skew shifts (which are two-dimensional), and Heisenberg nilmanifolds (which are three-dimensional). The dimension $O_\eta(1)$ is in fact known to be polynomial in η, but the best bounds for $c(\eta)$ are currently only exponential in nature. See [29] for further details and discussion.

The proof of Lemma 3.6 is rather lengthy but can be summarized as follows. If f has large U^3 norm, then by definition $T^n f\bar{f}$ has large U^2 norm for many n. Applying Lemma 3.2, this shows that for many n, $T^n f\bar{f}$ correlates with a linear phase function of some frequency $\xi(n)$ (which can be viewed as a kind of "derivative" of the phase of f in the "direction" n). Some manipulations involving the Cauchy–Schwarz inequality then show that $\xi(n)$ contains some additive structure (in that there are many quadruples

n_1, n_2, n_3, n_4 with $n_1 + n_2 = n_3 + n_4$ and $\xi(n_1) + \xi(n_2) = \xi(n_3) + \xi(n_4)$). Methods from additive combinatorics (notably the Balog–Szemerédi(–Gowers) theorem and Freiman's theorem, see e.g. [61]) are then used to "linearize" ξ, in the sense that $\xi(n)$ agrees with a (generalized) linear function of n on a large (generalized) arithmetic progression. One then "integrates" this fact to conclude that f itself correlates with a certain "anti-derivative" of $\xi(n)$, which is a (generalized) quadratic function on this progression. This in turn can be approximated by a 2-step nilsequence. For full details, see [29].

Thus, quadratic nilsequences are the only obstruction to a function being quadratically pseudorandom. This can be iterated to obtain structural results. The following "weak" structural theorem is already quite useful:

Theorem 3.7 (Weak structure theorem [35]). *Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ be a function bounded in magnitude by* 1*, and let $0 < \lambda < 1$. Then we can split $f = f_{U^\perp} + f_U$, where $f_{U^\perp}$ is a* 2*-step nilsequence given by a nilmanifold of dimension $O_\lambda(1)$ and by a bounded Lipschitz function F with Lipschitz constant $O_\lambda(1)$, and f_U is quadratically pseudorandom in the sense that $\|f_U\|_{U^3(\mathbb{Z}/N\mathbb{Z})} \leq \lambda$. Furthermore, $f_{U^\perp}$ is non-negative, bounded by* 1*, and has the same mean as f.*

This is an analogue of Theorem 3.4, and asserts that any bounded function has only a bounded amount of quadratic structure, with the function becoming quadratically pseudorandom once this structure is subtracted. It cannot be proven in quite the same way as in Theorem 3.4, because we have no "quadratic Fourier inversion formula" that decomposes a function neatly into quadratic components (the problem being that there are so many quadratic objects that such a formula is necessarily overdetermined). However, one can proceed by a finitary analogue of the ergodic theory approach, known as an "energy increment argument". In the ergodic setting, one uses all the quadratic objects to create a σ-algebra $\mathcal{Z}_2$, and sets $f_{U^\perp}$ to be the conditional expectation of f with respect to that σ-algebra. In the finitary setting, it turns out to be too expensive to try to use *all* the 2-step nilsequences to create a σ-algebra. However, by adopting a more adaptive approach, selecting only those 2-step nilsequences which have some significant correlation with f (or some component of f), one can obtain the above theorem; we omit the details.

It is likely that quantitative versions of this structure theorem will improve the known bounds on Szemerédi's theorem in the $k = 4$ case; see [32], [33], [34]. A closely related version of this argument was also essential in establishing Theorem 1.2, see Section 5 below.

4. Graph theory

We now turn to the third major line of attack to Szemerédi's theorem, based on graph theory (and hypergraph theory), and which is perhaps the purest embodiment of the strategy of exploiting the dichotomy between randomness and structure. For graphs,

the relevant structure theorem is the *Szemerédi regularity lemma*, which was developed in [53] in the original proof of Szemerédi's theorem, and has since proven to have many further applications in graph theory and computer science; see [41] for a survey. More recently, the analogous regularity lemma for hypergraphs have been developed in [21], [46], [47], [48], [49], [58]. Roughly speaking, these very useful lemmas assert that any graph (binary relation) or hypergraph (higher order relation), no matter how complex, can be modelled effectively as a pseudorandom sub(hyper)graph of a finite complexity (hyper)graph. Returning to the setting of the introduction, the graph regularity lemma would assert that there exists a colouring of the integers into finitely many colours such that relations such as $x - y \in A$ can be viewed approximately as pseudorandom relations, with the "probability" of the event $x - y \in A$ depending only on the colour of x and y.

The strategy of the graph theory approach is to abstract away the arithmetic structure in Szemerédi's theorem, converting the problem to one of finding solutions to an abstract set of equations, which can be modeled by graphs or hypergraphs. As before, we first illustrate this with the simple case of the $k = 3$ case of Szemerédi's theorem, which we will take in the form of Theorem 3.1. For simplicity we specialize to the case when f is the indicator function of a set A (which thus has density at least δ in $\mathbb{Z}/N\mathbb{Z}$); it is easy to see (e.g. by probabilistic arguments) that this special case in fact implies the general case. The key observation is that the problem of locating an arithmetic progression of length three can be recast as the problem of solving three constraints in three unknowns, where each constraint only involves two of the unknowns. Specifically, if $x, y, z \in \mathbb{Z}/N\mathbb{Z}$ solve the system of constraints

$$\begin{array}{cccc} & y & +2z & \in A \\ -x & & +z & \in A \\ -2x & -y & & \in A \end{array} \tag{10}$$

then $y + 2z, -x + z, -2x - y$ is an arithmetic progression of length three in A. Conversely, each such progression comes from exactly N solutions to (10). Thus, it will suffice to show that there are at least $c(3, \delta)N^3$ solutions to (10). Note that we already can construct at least δN^2 "trivial solutions" to (10), in which $y + 2z = -x + z = -2x + y$ is an element of A. Furthermore, these trivial solutions (x, y, z) are "edge-disjoint" in the sense that no two of these solutions share more than one value in common (i.e. if (x, y, z) and (x', y', z') are distinct trivial solutions then at most one of $x = x'$, $y = y'$, $z = z'$ are true). It turns out that these trivial solutions automatically generate a large number of non-trivial solutions to (10) – without using any further arithmetic structure present in these constraints. Indeed, the claim now follows from the following graph-theoretical statement.

Lemma 4.1 (Triangle removal lemma [51]). *For every $0 < \delta < 1$ there exists $0 < \sigma < 1$ with the following property. Let $G = (V, E)$ be an (undirected) graph with $|V| = N$ vertices which contains fewer than σN^3 triangles. Then it is possible to remove $O(\delta N^2)$ edges from G to create a graph G' which contains no triangles whatsoever.*

To see how the triangle removal lemma implies the claim, consider a vertex set V which consists of three copies V_1, V_2, V_3 of $\mathbb{Z}/N\mathbb{Z}$ (so $|V| = 3N$), and consider the tripartite graph $G = (V, E)$ whose edges are of the form

$$E = \{(y, z) \in V_2 \times V_3 : y + 2z \in A\} \cup \{(x, z) \in V_1 \times V_3 : -x + z \in A\} \\ \cup \{(x, y) \in V_1 \times V_2 : -2x - y \in A\}.$$

One can think of G as a variant of the Cayley graph for A. Observe that solutions to (10) are in one-to-one correspondence with triangles in G. Furthermore, the δN^2 trivial solutions to (10) correspond to δN^2 edge-disjoint triangles in G. Thus to delete all the triangles one needs to remove at least δN^2 edges. Applying Lemma 4.1 in the contrapositive (adjusting N, δ, σ by constants such as 3 if necessary), we see that G contains at least σN^3 triangles for some $\sigma = \sigma(\delta) > 0$, and the claim follows.

The only known proof of the triangle removal lemma proceeds by a structure theorem for graphs known as the *Szemerédi regularity lemma*. In order to emphasize the similarities between this approach and the previously discussed approaches, we shall not use the standard formulation of this lemma, but instead use a more recent formulation from [57], [58] (see also [1], [45]), which replaces graphs with functions, and then obtains a structure theorem decomposing such functions into a structured (finite complexity) component, a small component, and a pseudorandom (regular) component. More precisely, we work with functions $f : V \times V \to \mathbb{R}$; this can be thought of as a weighted, directed generalization of a graph on V in which every edge (x, y) is assigned a real-valued weight $f(x, y)$. The first step is to define a notion of pseudorandomness. For graphs, this concept is well understood. There are many equivalent formulations of this concept (see [6]), but we shall adopt one particularly close to the analogous concepts in previous sections, by introducing the *Gowers* $\square^2$ *cube norm* as

$$\|f\|_{\square^2}^4 := \mathbf{E}_{x,y,x',y' \in V} f(x, y) f(x, y') f(x', y) f(x', y');$$

when f is the incidence function of a graph, the right-hand side essentially counts the number of 4-cycles in that graph. Again, one can use the Cauchy–Schwarz inequality to establish that the $\square^2$ norm is indeed a norm; alternatively, one can use spectral theory and observe that the $\square^2$ norm is essentially the Schatten-von Neumann p-norm of f with $p = 4$. We refer to f as *pseudorandom* if its $\square^2$ norm is small. By two applications of Cauchy–Schwarz we have the generalized von Neumann inequality

$$|\mathbf{E}_{x,y,z \in V} f(x, y) g(y, z) h(z, x)| \leq \min(\|f\|_{\square^2}, \|g\|_{\square^2}, \|h\|_{\square^2}) \tag{11}$$

whenever f, g, h are bounded in magnitude by 1 (note that this generalizes (5)).

The next step, as before, is to establish a dichotomy between pseudorandomness and structure. The analogue of Lemma 2.2 or Lemma 3.2 is

Lemma 4.2 (Dichotomy between randomness and structure). *Suppose that* $f : V \times V \to \mathbb{R}$ *is bounded in magnitude by* 1 *with* $\|f\|_{\square^2(\mathbb{Z}/N\mathbb{Z})} \geq \eta$ *for some* $0 < \eta < 1$.

Then there exists sets $A, B \subset V$ *such that* $|\mathbf{E}_{x,y\in V} f(x,y)1_A(x)1_B(y)| \geq \eta^4/4$. *Here* $1_A(x)$ *denotes the indicator function of* A (*thus* $1_A(x) = 1$ *if* $x \in A$ *and* $1_A(x) = 0$ *otherwise*).

This lemma follows from an easy application of the pigeonhole principle and is omitted. One can iterate it (by an energy increment argument, as in Theorem 3.7) to obtain a weak version of the Szemerédi regularity lemma:

Theorem 4.3 (Weak structure theorem [10]). *Let* $f : V \times V \to \mathbb{R}$ *be a non-negative function bounded by* 1, *and let* $\varepsilon > 0$. *Then we can decompose* $f = f_{U^\perp} + f_U$, *where* $f_{U^\perp} = \mathbf{E}(f|\mathcal{Z}\otimes\mathcal{Z})$, $\mathcal{Z}$ *is a* σ*-algebra of* V *generated by at most* $2/\varepsilon$ *sets, and* $\|f_U\|_{\square^2} \leq \varepsilon$.

As with Theorem 3.4, the above theorem is too weak to be of much use, because the control one has on the pseudorandomness of f_U is fairly poor compared to the control on the complexity of $f_{U^\perp}$. The following strong version of the regularity lemma is far more useful (compare with Theorem 3.5):

Theorem 4.4 (Strong structure theorem [57]). *Let* $f : V \times V \to \mathbb{R}$ *be a non-negative function bounded by* 1, *and let* $\varepsilon > 0$. *Let* $F : \mathbb{N} \to \mathbb{N}$ *be an arbitrary increasing function* (*e.g.* $F(n) = 2^{2^n}$). *Then there exists an integer* $T = O_{F,\varepsilon}(1)$ *and a decomposition* $f = f_{U^\perp} + f_S + f_U$, *where* $f_{U^\perp} = \mathbf{E}(f|\mathcal{Z}\otimes\mathcal{Z})$, $\mathcal{Z}$ *is generated by at most* T *sets in* V, f_U *is pseudorandom in the sense that* $\|f_U\|_{\square^2} = O(1/F(T))$, *and* f_S *is small in the sense that* $\|f_S\|_{L^2(V\times V)} := (\mathbf{E}_{x,y\in V}|f_S(x,y)|^2)^{1/2} = O(\varepsilon)$. *Furthermore,* $f_{U^\perp}$, f_U *are bounded in magnitude by* 1. *Also,* $f_{U^\perp}$ *and* $f_{U^\perp} + f_S$ *are non-negative and bounded by* 1.

One can view $f_{U^\perp}$ as a "coarse" approximation to f, as it is measurable with respect to a fairly low-complexity σ-algebra, and $f_{U^\perp} + f_S = \mathbf{E}(f|\mathcal{Z}^{(n')}\otimes\mathcal{Z}^{(n')})$ as a "fine" approximation to f, which is considerably more complex but is also a far better approximation to f, in fact the accuracy of the fine approximation exceeds the complexity of the coarse approximation by any specified growth function F. Also the difference between the coarse and fine approximations is controlled by an arbitrarily small constant ε.

Theorem 4.4 already easily implies the Szemerédi regularity lemma in its traditional formulation; see [57]. It also implies Lemma 4.1, similar to how Theorem 3.5 implies the $k = 3$ version of Szemerédi's theorem; we omit the standard details.

As in the other two approaches, the above arguments extend (with some additional difficulties) to higher values of k. Again we restrict attention to the $k = 4$ case for simplicity. To locate a progression of length four in a set $A \subset \mathbb{Z}/N\mathbb{Z}$ is now equivalent to solving the system of constraints

$$\begin{array}{cccc} & y & +2z & +3w & \in A \\ -x & & +z & +2w & \in A \\ -2x & -y & & +w & \in A \\ -3x & -2y & -z & & \in A. \end{array} \tag{12}$$

This in turn follows from a hypergraph analogue of the triangle removal lemma. Define a 3-*uniform hypergraph* to be a pair $H = (V, E)$ where V is a finite set of vertices and E is a finite set of unordered triplets (x, y, z) in V, which we refer to as the *edges* of H. Define a *tetrahedron* in H to be a quadruple (x, y, z, w) of vertices such that all four triplets (x, y, z), (y, z, w), (z, w, x), (w, x, y) are edges of H.

Lemma 4.5 (Tetrahedron removal lemma [9]). *For every $0 < \delta < 1$ there exists $0 < \sigma < 1$ with the following property. Let $H = (V, E)$ be a 3-uniform hypergraph graph with $|V| = N$ vertices which contains fewer than σN^4 tetrahedra. Then it is possible to remove $O(\delta N^3)$ edges from H to create a hypergraph H' which contains no tetrahedra whatsoever.*

Letting f be the indicator function of H, we now have a situation where

$$\mathbf{E}_{x,y,z,w \in V} f(x, y, z) f(y, z, w) f(z, w, x) f(w, x, y) \leq \sigma$$

and we need to remove some small components from f so that this average now vanishes completely. Again, the key step here is to obtain a structure theorem that decomposes f into structured parts, small errors, and pseudorandom errors. The notion of pseudorandomness is now captured by the Gowers $\square^3$ cube norm, defined by

$$\|f\|_{\square^3}^8 := \mathbf{E}_{x,y,z,x',y',z' \in V} f(x, y, z) \dots f(x', y', z')$$

where the product is over the eight values of f with first co-ordinate x or x', second co-ordinate y or y', and third co-ordinate z or z'. In the case when f is the indicator function of a hypergraph H, this norm essentially counts the number of octahedra present in H. One can obtain a strong structure theorem analogous to Theorem 4.4, but with one significant difference. In Theorem 4.4, the structured component $f_{U^\perp}(x, y)$ can be broken up into a small number of components which are of the form $1_A(x)1_B(y)$. In the 3-uniform hypergraph analogue of Theorem 4.4, the structured component $f_{U^\perp}(x, y, z)$ will be broken up into a small number of components of the form $1_A(x, y)1_B(y, z)1_C(z, x)$. It turns out that in order to conclude the proof of Lemma 4.5, this structural decomposition is not sufficient by itself; one must also turn to the functions $1_A(x, y)$, $1_B(y, z)$, $1_C(z, x)$ generated by this structure theorem and decompose them further, essentially by invoking Theorem 4.4. This leads to some technical complications in the argument, although this approach to Szemerédi's theorem is still the most elementary and self-contained. See [21], [46], [47], [48], [49], [58] for details.

5. The primes

Having surveyed the three major approaches to Szemerédi's theorem, we now turn to the question of counting progressions in the primes (or in dense subsets of the primes). The major new difficulty here, of course, is that the primes have asymptotically zero

density rather than positive density, and even the most recent quantitative bounds on Szemerédi's theorem (see the discussion after Theorem 3.1) are not strong enough by themselves to overcome the "thinness" of the primes. However, it turns out that the primes (and functions supported on the primes) are still within the range of applicability of structure theorems. For instance, to oversimplify dramatically, the structure theorem in [27] essentially[5] represents the primes (or any dense subset of the primes) as a (sparse) pseudorandom subset of a set of positive density. Since sets of positive density already contain many progressions thanks to Szemerédi's theorem, it turns out that enough of these progressions survive when passing to a pseudorandom subset that one can conclude Theorem 3.1.

Interestingly, Theorem 1.2 can be tackled by (quantitative) ergodic methods, by Fourier-analytic methods, and by graph-theoretic methods, with the three approaches leading to slightly different results. For instance, the establishment of infinitely many progressions of length three in the primes by van der Corput [62] was Fourier-analytic, as was the corresponding statement for dense subsets of the primes (i.e. the $k = 3$ case of Theorem 1.2), proven 76 years later by Green [22]. The argument in [27] which proves Theorem 1.2 in full combines ideas from all three approaches, but is closest in spirit to the ergodic approach, albeit set in the finitary context of a cyclic group $\mathbb{Z}/N\mathbb{Z}$ rather than on an infinitary measure space. The argument in [59], which shows that the Gaussian primes (or any dense subset thereof) contains infinitely many constellations of any prescribed shape, and can be viewed as a two-dimensional analogue of Theorem 1.2, was proven via the (hyper)graph-theoretical approach. Finally, a more recent argument in [30], [31], in which precise asymptotics for the number of progressions of length four in the primes are obtained, as well as a "quadratic pseudorandomness" estimate on a renormalized counting function for the primes, proceeds by returning back to the original Fourier-analytic approach, but now using quadratic Fourier-analytic tools (Lemma 3.6 and Theorem 3.7) rather than linear ones.

As mentioned in the introduction, these results are discussed in other surveys [42], [25], [55], [56], [37], and we will only sketch some highlights here. In all the results, the strategy is to try to isolate the "structured" component of the primes from the "pseudorandom" component. There is some obvious structure present in the primes; for instance, they are almost all odd, they are almost all coprime to three, and so forth. This obvious structure can be normalized away fairly easily. For instance, to remove the bias the primes have towards being odd, one can replace the primes $P = \{2, 3, 5, \dots\}$ with the renormalized set $P_{2,1} := \{n : 2n+1 \text{ prime}\} = \{1, 2, 3, 5, \dots\}$. Each arithmetic progression in $P_{2,1}$ clearly induces a corresponding progression in P,

[5] This is a gross oversimplification. The precise statement is that after eliminating obvious irregularities in the primes caused by small residue classes, and excluding a small and technical exceptional set, a normalized counting function on the primes can be decomposed as a bounded function (which is thus spread out over a set of positive density), plus a pseudorandom error. Ignoring the initial elimination of obvious irregularities and the exceptional set, and pretending the bounded function was the indicator function of a positive density set A, one recovers the interpretation of the primes as a sparse pseudorandom subset of A.

but the set $P_{2,1}$ has no bias modulo 2. More generally, to reduce all the bias present in residue classes mod p for all $p < w$ (where w is a medium-sized parameter to be chosen later), one can work with a set $P_{W,b} := \{n : Wn + b \text{ prime}\}$, where W is the product of all the primes less than w and $1 \leq b < W$ is a number coprime to W. This "W-trick" allows for some technical simplifications.

Next, it is convenient not to work with the primes as a set, but rather as a renormalized counting function. One convenient choice is the von Mangoldt function $\Lambda(n)$, defined as $\log p$ if n is a power of a prime p and 0 otherwise. Actually, because of the W-trick, it is better to consider a renormalized von Mangoldt function such as $\Lambda_{W,b}(n) := \frac{W}{\phi(W)}\Lambda(Wn + b)$, where $\phi(W)$ is the Euler totient function of W. The prime number theorem in arithmetic progressions asserts that the asymptotic average value of $\Lambda_{W,b}(n)$ is equal to 1. To establish progressions of length k in the primes, it suffices to obtain a nontrivial lower bound for the asymptotic value of the average

$$\mathbf{E}_{1\leq n,r\leq N}\Lambda_{W,b}(n)\Lambda_{W,b}(n+r)\dots\Lambda_{W,b}(n+(k-1)r). \tag{13}$$

In fact this quantity is conjectured to asymptotically equal 1 as $W, N \to \infty$, with W growing much slower than N (a special case of the Hardy–Littlewood prime tuples conjecture); the intuition is that by removing all the bias present in the small residue classes, we have eliminated all the "obvious" structure in the primes, and the renormalized function $\Lambda_{W,b}$ should now fluctuate pseudorandomly around its mean value 1. However, this conjecture has only been verified in the cases $k = 3, 4$ (leading to an asymptotic count for the number of progressions of primes of length k less than a large number N); for the cases $k > 4$ we only have a lower bound of $c(k)$ for some small $c(k) > 0$.

Let us cheat slightly by pretending that $\Lambda_{W,b}$ is a function on the cyclic group $\mathbb{Z}/N\mathbb{Z}$ rather than on the integers $\mathbb{Z}$; there are some minor technical truncation issues that need to be addressed to pass from one to the other but we shall ignore them here. In order to show that (13) is close to 1, an obvious way to proceed would be to establish some kind of pseudorandomness control on the deviation $\Lambda_{W,b} - 1$ from the mean, and then some sort of generalized von Neumann theorem to show that this deviation is negligible. Based on the experience with Szemerédi's theorem, one would expect linear pseudorandomness to be the correct notion for $k = 3$, quadratic pseudorandomness for $k = 4$, and so forth. In the $k = 3$ case it is indeed a standard computation (using Vinogradov's method, or a modern variant of that method such as the one based on Vaughan's identity) to show that $\Lambda_{W,b} - 1$ is has small Fourier coefficients, which is a reasonable proxy for linear pseudorandomness; the point being that the W-trick has eliminated all the "major arcs" which would otherwise destroy the pseudorandomness. It then remains to obtain a generalized von Neumann theorem, similar to (7). In preceding sections, one was working with functions that were bounded (and hence square integrable), and one could obtain these theorems easily from Plancherel's theorem. In the current setting, the L^2 estimates on $\Lambda_{W,b}$ are unfavourable, and what one needs instead is some sort of l^p bound on the Fourier coefficients of $\Lambda_{W,b}$ for some $2 < p < 3$. This can be done by a more careful

application of Vinogradov's method, but can also be achieved using harmonic analysis methods arising from restriction theory; see [22], [28]. The key new insight here is that while the Fourier coefficients of $\Lambda_{W,b}$ are difficult to understand directly, one can *majorize* $\Lambda_{W,b}$ pointwise by (a constant multiple of) a much better behaved function ν of comparable size, whose Fourier coefficients are much easier to obtain bounds for (indeed ν is essentially linearly pseudorandom once one subtracts off its mean, which is essentially 1). This "enveloping sieve" ν is essentially the Selberg upper bound sieve, and can be viewed as a "smoothed out" version[6] of $\Lambda_{W,b}$. Restriction theory (related to the method of the large sieve) is then used to pass from Fourier control of ν to Fourier control of $\Lambda_{W,b}$.

A similar idea was used in [22], [28] to establish the $k = 3$ case of Theorem 1.2; we sketch the argument from [28] here as follows. The main objective is to establish a lower bound for expressions such as

$$\mathbf{E}_{x,r\in\mathbb{Z}/N\mathbb{Z}}\Lambda_{W,b}1_A(x)\Lambda_{W,b}1_A(x+r)\Lambda_{W,b}1_A(x+2r) \tag{14}$$

for large sets A. Restriction theory still allows us to obtain good l^p upper bound for the Fourier coefficients of $\Lambda_{W,b}1_A$. This functions as a substitute for Plancherel's theorem (which is not favourable here), and one can now obtain structure theorems such as Theorem 3.4 (and with some more effort, Theorem 3.5). This decomposes $\Lambda_{W,b}1_A$ into some structured component $f_{U^\perp}$ and a linearly pseudorandom component f_U. The generalized von Neumann theorem lets us dispose the contribution of f_U to (14), so let us focus on $f_{U^\perp}$. One can try to use the complexity bound on $f_{U^\perp}$ (controlling the number of linear phases that comprise $f_{U^\perp}$) to get some lower bound here, but this would require developing a strong structure theorem analogous to Theorem 3.5. It turns out that one can argue more cheaply, using a weaker structure theorem analogous to Theorem 3.4. The key observation is that because $\Lambda_{W,b}1_A$ is dominated (up to a constant) by the enveloping sieve ν, the structured component of $\Lambda_{W,b}1_A$ (which is essentially a convolution of $\Lambda_{W,b}1_A$ with a Fejér-like kernel) is pointwise dominated (up to a constant) by a corresponding structured component of ν. But since ν is linearly pseudorandom after subtracting off its mean, the structured component of ν turns out to essentially be just the mean of ν, which is bounded. We conclude that $f_{U^\perp}$ is bounded, at which point one can just apply Szemerédi's theorem (Theorem 3.1) directly to obtain a good lower bound on this contribution to (14), and one can now conclude the $k = 3$ case of Theorem 1.2.

The proof of Theorem 1.2 for general k in [27] follows the same general strategy, but it is convenient to abandon the Fourier framework (which becomes quite complicated for $k > 3$) and instead take an approach which borrows ingredients from all three approaches, especially the ergodic theory approach. From the Fourier approach one borrows the Gowers uniformity norms $U^{k-2}(\mathbb{Z}/N\mathbb{Z})$, which are a convenient way to define the appropriate notion of pseudorandomness for counting progressions of

[6] What is essentially happening here is that we are viewing the primes not as a zero density subset of the integers, but as a positive density subset of a set of "almost primes" which can be controlled efficiently via sieve theory.

length k. One still needs an enveloping sieve ν, but instead of using a Selberg-type sieve that enjoys good Fourier coefficient control, it turns out to be more convenient to use an enveloping sieve[7] of Goldston and Yıldırım [15], [16], [17] which has good control on k-point correlations (indeed, it behaves pseudorandomly after subtracting off its mean, which is essentially 1).

The next step is a generalized von Neumann theorem to show that the contribution of pseudorandom functions are negligible. The fact that the functions involved are no longer bounded by 1, but are instead dominated by ν, makes this theorem somewhat trickier to establish, however it can still be achieved by a number of applications of the Cauchy–Schwarz and taking advantage of the pseudorandomness properties of $\nu - 1$. This type of argument is inspired by certain "sparse counting lemmas" arising from the hypergraph approach, particuarly from [21].

The main step, as in previous sections, is a structure theorem which decomposes $\Lambda_{W,b}$ (or $\Lambda_{W,b} 1_A$) into a structured component and a pseudorandom component. In principle one could use higher order Fourier analysis (or the precise characteristic factors achieved in [39], [64] to obtain this decomposition, but this looks rather difficult technically, though progress has been made in the $k = 4$ case. Fortunately, there is a "softer" approach in which one defines structure purely by duality; to oversimplify substantially, one defines a function to be structured if it is approximately orthogonal to all pseudorandom functions. One can then obtain a soft structural theorem in which the structural component is essentially a conditional expectation of the original function to a certain σ-algebra generated by certain special structured functions which are called "dual functions" in [27]. This σ-algebra (the finitary analogue of a characteristic factor) is not too tractable to work with, but somewhat miraculously, one can utilize the pseudorandomness properties of ν and a large number of applications of the Cauchy–Schwarz inequality to show that the conditional expectation of ν with respect to this σ-algebra remains bounded (outside of a small exceptional set, which turns out to have a negligible impact). Since $\Lambda_{W,b} 1_A$ is pointwise dominated by a constant multiple of ν, the structured component of $\Lambda_{W,b} 1_A$ is similarly bounded and can thus be controlled using Szemerédi's theorem. Combining this with the generalized von Neumann theorem to handle the pseudorandom component, one obtains Theorem 1.2. The result for the Gaussian prime constellations is similar, but uses the Gowers cube norms $\square^{k-2}$ instead of the uniformity norms, and replaces Szemerédi's theorem by a hypergraph removal lemma similar to Lemma 4.1 and Lemma 4.5; see [58], [59].

The arguments used to prove Theorem 1.2 give a lower bound for the expression (13), but do not compute its asymptotic value (which should be 1). As mentioned earlier, for $k = 3$ this can be achieved by the circle method. More recently, the $k = 4$ case has been carried out in [30], [31]; the same method in fact allows one to asymptotically count the number of solutions to any two linear homogeneous equations in four prime unknowns. The key point is to show that $\Lambda_{W,b} - 1$ is quadratically pseudorandom, as the generalized von Neumann theorem will then allow one to con-

[7] A related enveloping sieve was also used in the recent establishment of narrow gaps in the primes [18].

trol (13) satisfactorily. It turns out that a variant of Lemma 3.6 applies here, and reduces matters to showing that $\Lambda_{W,b} - 1$ does not correlate significantly with any 2-step nilsequences. This task is attackable by Vinogradov's method, although it is rather lengthy and it turns out to be simpler to first replace $\Lambda_{W,b} - 1$ with the closely related Möbius function.

References

[1] Alon, N., Shapira, A., A characterization of the (natural) graph properties testable with one-sided error. In *46th Symposium on Foundations of Computer Science*, IEEE Computer Soc. Press, Los Alamitos, CA, 2005, 429–438.

[2] Behrend, F. A., On sets of integers which contain no three terms in arithmetic progression. *Proc. Nat. Acad. Sci.* **32** (1946), 331–332.

[3] Bergelson, V., Host, B., Kra, B., Multiple recurrence and nilsequences. *Invent. Math.* **160** (2) (2005), 261–303.

[4] Bourgain, J., A Szemerédi type theorem for sets of positive density in $\mathbb{R}^k$. *Israel J. Math.* **54** (3) (1986), 307–316.

[5] Bourgain, J., On triples in arithmetic progression. *Geom. Funct. Anal.* **9** (1999), 968–984.

[6] Chung, F., Graham, R., Wilson, R. M., Quasi-random graphs. *Combinatorica* **9** (1989), 345–362.

[7] Conze, J. P., Lesigne, E., Sur un théorème ergodique pour les mesures diagonales. In *Probabilités*, Publ. Inst. Rech. Math. Rennes, 1987-1, Univ. Rennes I, Rennes 1988, 1–31.

[8] Erdős, P., Turán, P., On some sequences of integers. *J. London Math. Soc.* **11** (1936), 261–264.

[9] Frankl, P., Rödl, V., Extremal problems on set systems. *Random Structures Algorithms* **20** (2) (2002), 131–164.

[10] Frieze, A., Kannan, R., Quick approximation to matrices and applications. *Combinatorica* **19** (2) (1999), 175–220.

[11] Furstenberg, H., Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.* **31** (1977), 204–256.

[12] Furstenberg, H., *Recurrence in Ergodic theory and Combinatorial Number Theory*. Princeton University Press, Princeton, NJ, 1981.

[13] Furstenberg, H., Katznelson, Y., Ornstein, D., The ergodic-theoretical proof of Szemerédi's theorem. *Bull. Amer. Math. Soc.* **7** (1982), 527–552.

[14] Furstenberg, H., Weiss, B., A mean ergodic theorem for $1/N \sum_{n=1}^{N} f(T^n x) g(T^{n^2} x)$. In *Convergence in ergodic theory and probability* (Columbus OH 1993), Ohio State Univ. Math. Res. Inst. Publ. 5, Walter de Gruyter, Berlin 1996, 193–227.

[15] Goldston, D., Yıldırım, C. Y., Higher correlations of divisor sums related to primes, I: Triple correlations. *Integers* **3** (2003), A5, 66pp. (electronic).

[16] Goldston, D., Yıldırım, C. Y., Higher correlations of divisor sums related to primes. III: k-correlations. Preprint.

[17] Goldston, D., Yıldırım, C. Y., Small gaps between primes, I. Preprint.

[18] Goldston, D., Motohashi, Y., Pintz, J., Yıldırım, C.Y., Small gaps between primes exist. *Proc. Japan Acad. Ser. A Math. Sci.* **82** (4) (2006), 61–65.

[19] Gowers, T., A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.* **8** (1998), 529–551.

[20] Gowers, T., A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* **11** (2001), 465–588.

[21] Gowers, T., Hypergraph regularity and the multidimensional Szemerédi theorem. Preprint.

[22] Green, B. J., Roth's theorem in the primes. *Ann. of Math.* **161** (3) (2005), 1609–1636.

[23] Green, B. J., A Szemerédi-type regularity lemma in abelian groups. *Geom. Funct. Anal.* **15** (2) (2005), 340–376.

[24] Green, B. J., Finite field models in additive combinatorics. In *Surveys in Combinatorics*, London Math. Soc. Lecture Note Ser. 327, Cambridge University Press, Cambridge 2005, 1–27.

[25] Green, B. J., Long arithmetic progressions of primes. Preprint.

[26] Green, B. J., Konyagin, S., On the Littlewood problem modulo a prime. *Canad. J. Math.*, to appear.

[27] Green, B. J., Tao, T., The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.*, to appear.

[28] Green, B. J., Tao, T., Restriction theory of Selberg's sieve, with applications. *J. Théor. Nombres Bordeaux* **18** (2006), 147–182.

[29] Green, B. J., Tao, T., An inverse theorem for the Gowers U^3 norm. *Proc. Edinburgh Math. Soc.*, to appear.

[30] Green, B. J., Tao, T., Quadratic uniformity of the Möbius function. Preprint.

[31] Green, B. J., Tao, T., Two linear equations in four prime unknowns. Preprint.

[32] Green, B. J., Tao, T., New bounds for Szemerédi's theorem, I: Progressions of length 4 in finite field geometries. Preprint.

[33] Green, B. J., Tao, T., New bounds for Szemerédi's theorem, II: A new bound for $r_4(N)$. In preparation.

[34] Green, B. J., Tao, T., New bounds for Szemerédi's theorem, III: A polylog bound for $r_4(N)$. In preparation.

[35] Green, B. J., Tao, T., On arithmetic regularity lemmas. In preparation.

[36] Hardy, G. H., Littlewood, J. E., Some problems of "partitio numerorum"; III: On the expression of a number as a sum of primes. *Acta Math.* **44** (1923), 1–70.

[37] Host, B., Progressions arithmetiques dans les nombres premiers (d'apres B. Green and T. Tao). *Seminaire Bourbaki*, Mars 2005, 57eme annee, 2004-2005, no. 944.

[38] Host, B., Kra, B., Convergence of Conze-Lesigne averages. *Ergodic Theory Dynam. Systems* **21** (2) (2001), 493–509.

[39] Host, B., Kra, B., Non-conventional ergodic averages and nilmanifolds. *Ann. of Math.* **161** (1) (2005) 397–488.

[40] Komlós, J., A generalization of a problem of Steinhaus. *Acta Math. Hungar.* **18** (1967), 217–229.

[41] Komlós, J., Simonovits, M., Szemerédi's regularity lemma and its applications in graph theory. In *Combinatorics*, Paul Erdös is eighty, Vol. 2 (Keszthely, 1993), Bolyai Soc. Math. Stud. 2, János Bolyai Math. Soc., Budapest 1996, 295–352.

[42] Kra, B., The Green-Tao Theorem on arithmetic progressions in the primes: an ergodic point of view. *Bull. Amer. Math. Soc.* (*N.S.*) **43** (1) (2006), 3–23.

[43] Lacey, M., Thiele, C. L^p estimates on the bilinear Hilbert transform for $2 < p < \infty$. *Ann. of Math.* **146** (1997), 693–724.

[44] Leibman, A., Polynomial sequences in groups. *J. Algebra* **201** (1998), 189–206.

[45] L. Lovász, Szegedy, B., Szemerédi's lemma for the analyst. Preprint.

[46] Nagle, B., Rödl, V., Schacht, M., The counting lemma for regular k-uniform hypergraphs. *Random Structures Algorithms* **28** (2) (2006), 113–179.

[47] Rödl, V., Schacht, M., Regular partitions of hypergraphs. *Combin. Probab. Comput.*, to appear.

[48] Rödl, V., Skokan, J., Regularity lemma for uniform hypergraphs. *Random Structures Algorithms* **25** (1) (2004), 1–42.

[49] Rödl, V., Skokan, J., Applications of the regularity lemma for uniform hypergraphs. *Random Structures Algorithms* **28** (2) (2006), 180–194.

[50] Roth, K.F., On certain sets of integers. *J. London Math. Soc.* **28** (1953), 245–252.

[51] Ruzsa, I., Szemerédi E., Triple systems with no six points carrying three triangles. *Colloq. Math. Soc. J. Bolyai* **18** (1978), 939–945.

[52] Stein, E. *Harmonic Analysis: Real Variable Methods, Orthogonality, and Oscillatory Integrals*. Princeton University Press, Princeton, NJ, 1993.

[53] Szemerédi, E., On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* **27** (1975), 299–345.

[54] Tao, T., A quantitative ergodic theory proof of Szemerédi's theorem. *Electron. J. Combin.*, to appear.

[55] Tao, T., Obstructions to uniformity, and arithmetic patterns in the primes. *Quarterly J. Pure Appl. Math.* **2** (2006), 199–217.

[56] Tao, T., Arithmetic progressions in the primes. *Collect. Math.* (2006), Vol. Extra., 37–88.

[57] Tao, T., Szemerédi's regularity lemma revisited. *Contrib. Discrete Math.* **1** (1) (2006), 8–28.

[58] Tao, T., A variant of the hypergraph removal lemma. *J. Combin. Theory Ser. A* **113** (7), 1257–1280.

[59] Tao, T., The Gaussian primes contain arbitrarily shaped constellations. *J. Anal. Math.* **99** (2006), 109–176.

[60] Tao, T., An ergodic transference theorem. Unpublished.

[61] Tao, T., Vu, V., Additive Combinatorics. Book in preparation, Cambridge University Press.

[62] van der Corput, J. G., Über Summen von Primzahlen und Primzahlquadraten. *Math. Ann.* **116** (1939), 1–50.

[63] Varnavides, P., On certain sets of positive density. *J. London Math. Soc.* **34** (1959) 358–360.

[64] Ziegler, T., Universal characteristic factors and Furstenberg averages. *J. Amer. Math. Soc.* **20** (2007), 53–97.

Department of Mathematics, UCLA, Los Angeles CA 90095, U.S.A.

E-mail: tao@math.ucla.edu

Perspectives in nonlinear diffusion: between analysis, physics and geometry

Juan Luis Vázquez

Abstract. We review some topics in the mathematical theory of nonlinear diffusion. Attention is focused on the porous medium equation and the fast diffusion equation, including logarithmic diffusion. Special features are the existence of free boundaries, the limited regularity of the solutions and the peculiar asymptotic laws for porous medium flows, while for fast diffusions we find the phenomena of finite-time extinction, delayed regularization, nonuniqueness and instantaneous extinction. Logarithmic diffusion with its strong geometrical flavor is also discussed. Connections with functional analysis, semigroup theory, physics of continuous media, probability and differential geometry are underlined.

Mathematics Subject Classification (2000). Primary 35K55; Secondary 35K65.

Keywords. Nonlinear diffusion, degenerate parabolic equations, flows in porous media.

1. Introduction

The heat equation, $\partial_t u = \Delta u$, (HE for short) is one of the three classical linear partial differential equations of second order that form the basis of any elementary introduction to the area of partial differential equations. Its success in describing the process of thermal propagation and processes of matter diffusion has witnessed a permanent acceptance since J. Fourier's essay *Théorie Analytique de la Chaleur* was published in 1822, [22], and has motivated the continuous growth of mathematics in the form of Fourier analysis, spectral theory, set theory, operator theory, and so on. Later on, it contributed to the development of measure theory and probability, among other topics.

The prestige of the heat equation has not been isolated. A number of related equations have been proposed both by applied scientists and pure mathematicians as objects of study. In a first extension of the field, the theory of linear parabolic equations was developed, with constant and then variable coefficients. The linear theory enjoyed much progress, but it was soon observed that most of the equations modelling physical phenomena without excessive simplification are nonlinear. However, the mathematical difficulties of building theories for nonlinear versions of the three classical partial differential equations (Laplace's equation, heat equation and wave equation) made it impossible to make significant progress until the 20th century was well advanced. This observation also applies to other important nonlinear PDEs

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

or systems of PDEs, like the Navier–Stokes equations and nonlinear Schrödinger equations.

The great development of functional analysis in the decades from the 1930s to the 1960s made it possible for the first time to start building theories for these nonlinear PDEs with full mathematical rigor. This happened in particular in the area of parabolic equations where the theory of linear and quasilinear parabolic equations in divergence form reached a degree of maturity reflected for instance in the classical books of O. Ladyzhenskaya et al. [33] and A. Friedman [23]. A similar evolution for elliptic and parabolic equations in non-divergence form has proceeded at a much slower pace and is now in full bloom.

We will report here on progress in the area of nonlinear diffusion. A quite general form of nonlinear diffusion equation, as it appears in the literature, is

$$\partial_t H(x,t,u) = \sum_{i=1}^{d} \partial_{x_i}(A_i(x,t,u,Du)) + F(x,t,u,Du). \tag{1}$$

Here $Du = (\partial_{x_1} u, \ldots, \partial_{x_n} u)$ stands for the spatial gradient of u. Suitable conditions should be imposed to guarantee (a minimum of) parabolicity, e.g., the matrix $(a_{ij}) = (\partial_{u_j} A_i(x,t,u,Du))$ should be positive semi-definite and $\partial_u H(x,t,u) \geq 0$. If we do not want to consider reaction or convection effects, however important they may be in the applications, the last term in the right-hand side should be dropped at the cost of skipping the rich theory for equations of the types

$$\partial_t u = \Delta u \pm u^p, \tag{2}$$

and their numerous variants. Let us also remark at this point that many applications deal with systems of such equations. A theory for equations and systems in such a generality has been in the making during the last decades, but the richness of phenomena that are included in the different examples covered in the general formulation precludes a general theory with detailed enough information. Two main areas of study have focused the attention of researchers in recent years: free boundary problems and blow-up problems. This article deals with the first topic and the associated idea of degenerate parabolic flows with finite propagation.

The study of nonlinear diffusion problems and free boundaries started at an early date. G. Lamé and E. Clapeyron addressed in 1831 the evolution of a two-phase system (water and ice) and were led to a free boundary problem that came to be known as the Stefan problem. There, the evolution of the temperature of the two media, sitting in disjoint domains, and obeying state equations of the heat equation type, has to be coupled with the evolution of the interface or free boundary separating the media. It took more than 120 years until O. Oleinik and S. Kamin gave a complete solution of the problem of existence and uniqueness in the context of weak solutions, a concept originated with J. Leray and S. Sobolev in the 1930s. Together with the obstacle problem, the Hele–Shaw problem and the porous medium equation, it formed

a solid basis for the study of free boundary problems, though of course many other examples, like the combustion problems, attracted attention. The combination of functional analysis and geometry has been a key feature of the work in this frontier area that I have followed personally in the contributions of L. Caffarelli and A. Friedman, cf. [13], [24].

I will devote a large part of this exposition to progress in the porous medium equation (shortly, PME), written as

$$\partial_t u = \Delta u^m, \quad m > 1, \tag{3}$$

when nonnegative solutions are considered, as happens in most of the applications. However, when signed solutions are allowed the form $\partial_t u = \Delta(|u|^{m-1}u)$ is used. For the limit value $m = 1$ the classical heat equation is recovered. The PME is in some sense the simplest nonlinear modification of the heat equation in the area of diffusion; this can be easily understood when we write it in the form $\partial_t u = \operatorname{div}(d(u)\nabla u)$ with $d(u) = m|u|^{m-1}$, which means a density-dependent diffusivity. Later on, we will treat the case $m < 1$ that has attracted much attention in recent times and is called the fast diffusion equation (FDE). More generally, we can consider the larger class of *generalized porous medium equations* (GPME),

$$\partial_t u = \Delta\Phi(u) + f, \tag{4}$$

also called *filtration equations*, especially in the Russian literature; here, Φ is an increasing function $\mathbb{R}_+ \mapsto \mathbb{R}_+$, and usually $f = 0$. The diffusion coefficient is now $d(u) = \Phi'(u)$, and the condition $\Phi'(u) \geq 0$ is needed to make the equation parabolic. Whenever $\Phi'(u) = 0$ for some $u \in \mathbb{R}$, we say that the equation degenerates at that u-level, since it ceases to be strictly parabolic. This is the cause for more or less serious departures from the standard quasilinear parabolic theory; such deviations will focus our attention in what follows.

Concentrating on these particular equations will allow us to see the progress of the combination of the methods of functional analysis and geometry in clarifying the novelties and characteristic features of the theory of nonlinear diffusion equations. It also makes possible to describe the peculiarities of the behaviour of the solutions in great detail. It must be said that a somewhat similar and quite impressive progress has been obtained in many connected directions. Thus, an important role in the development of the topic of the filtration equation has been played by the already mentioned *Stefan problem* that can be written as a filtration equation with

$$\Phi(u) = (u-1)_+ \quad \text{for } u \geq 0, \quad \Phi(u) = u \quad \text{for } u < 0. \tag{5}$$

More generally, we can put $\Phi(u) = c_1(u - L)_+$ for $u \geq 0$, and $\Phi(u) = c_2\, u$ for $u < 0$, where c_1, c_2 and L are positive constants. The Stefan problem and the PME have had a parallel history. When the time derivative term of the Stefan problem is simplified (limit of zero specific heat) we get the Hele–Shaw equation which models

the behaviour of viscous fluids in very narrow cells. It can be written in the form

$$\partial_t H(u) = \Delta u + f, \tag{6}$$

with H the Heaviside step function. Different models include convection and/or reaction terms or a different form of nonlinear diffusion called p-Laplacian, where Δu, resp. Δu^m, is replaced by $\nabla \cdot (|\nabla u|^{p-2}\nabla u)$. The limit case $p = 1$ has recently received much attention in connection with image processing, cf. e.g. [1].

All the results to be reported in this exposition can be found explained in more detail in the works [43], [44]. The author takes the opportunity to thank the collaborators he has been lucky to be associated with.

2. Degeneration, free boundaries and geometry

A first difficulty of the theories of nonlinear diffusion including degenerate parabolic cases has been the concept of solution. The degenerate character of the PME as compared with the HE implies that the concept of classical solution that so well suits the latter is not adequate for the former. It was soon realized that the PME has the property of finite speed of propagation of disturbances from the rest level $u = 0$. This is explained in simplest terms when we take as initial data a density distribution given by a nonnegative, bounded and compactly supported function $u_0(x)$. The physical solution of the PME for these data is a continuous function $u(x, t)$ such that for any $t > 0$ the profile $u(\cdot, t)$ is still nonnegative, bounded and compactly supported; the support expands eventually to penetrate the whole space, but it is bounded at any fixed time. The *free boundary* is defined as the boundary of the support,

$$\Gamma_u = \partial S_u, \quad S_u = \text{closure}\,\{(x, t) : u(x, t) > 0\}. \tag{7}$$

Usually, the sections at a fixed time are considered. $\Gamma_u(t)$, $S_u(t)$. From the point of view of analysis, the presence of free boundaries is associated to discontinuities of the first derivatives of the solution. This is quite easy to see in the prototype case $m = 2$ where the equation can be written as

$$\partial_t u = 2u\,\Delta u + 2|\nabla u|^2. \tag{8}$$

It is immediately clear that in the regions where $u \neq 0$ the leading term in the right-hand side is the Laplacian modified by the variable coefficient $2u$; on the contrary, for $u \to 0$, the equation simplifies into $\partial_t u \sim 2|\nabla u|^2$, i.e., the *eikonal equation* (a first-order equation of Hamilton–Jacobi type, that propagates along characteristics). In accordance with this idea, the behaviour near the free boundary is controlled by the law $\mathbf{V} = 2|\nabla u|$, where $\mathbf{V}$ is the advance speed of the front. This is equivalent to $\partial_t u = 2|\nabla u|^2$ on this level line and has been rigorously proved in standard situations. In terms of the application to flows in porous media, this also means that the front

speed equals the fluid particle speed which follows Darcy's law, the basic law of fluids in such media. See the typical front propagation in Figure 1 below. A similar calculation can be done for general $m > 1$ after introducing the so-called *pressure variable*, $v = cu^{m-1}$ for some $c \geq 0$. Putting $c = m/(m-1)$ we get

$$\partial_t v = (m-1)\, v\, \Delta v + |\nabla v|^2. \tag{9}$$

This is a fundamental transformation in the theory of the PME that allows us to get similar conclusions about the behaviour of the equation for u, $v \sim 0$ when $m > 1$, $m \neq 2$.

The use of u for functional analysis considerations and v for the dynamical and geometrical aspects is typical "dual thinking" of PME people.

3. Existence and uniqueness: generalized solutions

The non-existence of classical solutions when free boundaries appear delayed the mathematical theory of the PME. When the difficulty was addressed, it became a source of mathematical progress. Existence of solutions in the weak sense is now easy to establish for the PME or the GPME posed in the whole space with bounded initial data or in a bounded domain with zero Neumann or Dirichlet boundary conditions. Work in that direction started with O. Oleinik in 1958 [36]. The concept implies integrating once or twice by parts: in the first case we ask u to be locally integrable, $\Phi(u)$ to also have locally integrable first space derivatives, and finally the identity

$$\iint_{Q_T} \{\nabla \Phi(u) \cdot \nabla \eta - u\eta_t\}\, dxdt = \iint_{Q_T} f\eta\, dxdt \tag{10}$$

must hold for any test function $\eta \in C_c^1(Q_T)$, where $Q_T = \Omega \times (0, T)$ is the space-time domain where the solution is defined. In the case of very weak solutions we ask for a locally integrable function, $u \in L^1_{\mathrm{loc}}(Q_T)$, such that $\Phi(u) \in L^1_{\mathrm{loc}}(Q_T)$, and the identity

$$\iint_{Q_T} \{\Phi(u)\, \Delta\eta + u\eta_t + f\eta\}\, dxdt = 0 \tag{11}$$

holds for any test function $\eta \in C_c^{2,1}(Q_T)$. A very weak solution is roughly speaking a distributional solution, but all terms appearing in the formulation are required to be locally integrable functions; moreover, the initial and boundary conditions are usually inserted into the formulation (this is reflected as possible new terms in the identity along with a more precise specification of the test function space, see [44], Chapter 5).

These are concepts that have permeated nonlinear analysis in the last century. But the theory of the PME has been strongly influenced by the discovery that it generates a semigroup of contractions in the space $L^1(\Omega)$ and that a solution is most conveniently

produced by the method of implicit time discretization using the celebrated result of Crandall–Liggett of the early 1970s [6], [20] that widely extends the scope of the Hille–Yosida generation theorem from linear to nonlinear semigroups. The resulting "numerical solution" obtained in the limit of the time discretization process is called a *mild solution*, a new mathematical object that attracted enormous attention at the time. Moreover, mild solutions form a contraction semigroup in the "natural space" $L^1(\Omega)$, not a common space in analysis since it is not reflexive and has peculiar compactness properties. But note that this space is natural for probabilists.

Now that we have four concepts of solution on the table (classical, weak, very weak and mild), proper relations have to be established among them, what is easy if we can prove a sufficiently strong uniqueness theorem. This is easy for the simplest scenarios, like the PME with nonnegative boundary conditions, but not so easy for more general equations involving general diffusion nonlinearities, variable coefficients and/or lower order effects, specially nonlinear convection. A whole literature has evolved in these years to tackle the issue, for which we refer e.g. to [44], Chapter 10.

On the one hand, the investigations on the properties of mild solutions in semigroup theory led to the interest in examining so-called *strong solutions*, where all derivatives appearing in the differential equation are assumed to exist as locally integrable functions (and satisfy maybe some other convenient requirements) so that the PDE can be interpreted as an abstract evolution $t \mapsto u(t)$ where $u(t)$ lives in a functional Banach space X and satisfies

$$\frac{du(t)}{dt} = Au(t) + f, \tag{12}$$

A being a nonlinear (highly discontinuous) operator on X. Actually, the study of nonlinear diffusion has been a source of examples, counterexamples and new concepts for nonlinear semigroup theory. Concepts from mechanics like blow-up, extinction, initial discontinuity layers, have appeared naturally in these studies.

A very recent trend is the consideration of semigroups in spaces of measures, which is quite natural when we consider diffusion from the point of view of stochastic processes (nonlinear versions of Brownian motion). This has led recently to a flurry of activity concerning the property of contraction of the PME semigroup with respect to the Wasserstein distance defined in the set of nonnegative integrable functions with a fixed mass by the formula

$$d(u, v)^2 = \frac{1}{2} \inf \left\{ \iint |x - y|^2 \, d\mu(x, y) \right\}, \tag{13}$$

the infimum taken over all nonnegative Radon measures μ whose projections (marginals) are $u(x)\,dx$ and $v(y)\,dy$. The PME is then viewed as a gradient flow, cf. F. Otto [37]. The contractivity of the semigroup in this norm is proved by J. A. Carrillo, R. McCann and C. Villani [16].

A very fruitful scenario for the generalization of the PME is the combination of nonlinear diffusion with convection (i.e., with a conservation law) which leads to the

need for *entropy conditions* (mainly, of Kruzhkov type) to ensure the selection of a proper kind of solutions that guarantees both uniqueness and accordance with the underlying physics. This is work that counts the names of P. Bénilan, J. Carrillo, P. Wittbold and others, which extends the standard concept of bounded entropy solutions to merely integrable solutions by means of *renormalized entropy solutions* [7].

A still different direction is to focus on the pressure equation, that can be written in general form as

$$\partial_t u = a(u)\Delta u + |\nabla u|^2. \tag{14}$$

This is a non-divergence equation for which the methods of *viscosity solutions* (Crandall–Evans–Lions) should be better suited, [19], [11]. The proof of well-posedness for the PME (case $a(u) = cu$) was done in Caffarelli–Vázquez [14] in the class of continuous and bounded nonnegative viscosity solutions, and extended to more general GPME by Brändle–Vázquez [8]. But proving well-posedness for more general equations does not seem to be easy. In particular, the problem of characterizing bounded signed solutions of the PME is still open for viscosity solutions.

The conclusion is that the theory of nonlinear diffusion needs and benefits from a combination of functional approaches and has contributed in its turn to develop the mathematics of these abstract branches supplying them with problems, ideas and interactions. This is a consequence of the combination of relative simplicity with intrinsic difficulty, something on the other hand typical of all the classical nonlinear PDE models of science.

4. Asymptotic behaviour: nonstandard central limit theorem

This is a subject in which the mathematical investigation of nonlinear diffusion equations (NLDE) has been most active. The study of asymptotic behaviour is made attractive by the combination of analysis and geometry, which is felt in the description in terms of selfsimilar solutions and the formation of patterns.

On a general level, it has been pointed out in many papers and corroborated by numerical experiments that similarity solutions furnish the asymptotic representation for solutions of a wide range of problems in mathematical physics. The books of G. Barenblatt [4], [5] contain a detailed discussion of this subject. Self-similar solutions and scaling techniques play a prominent role in the asymptotic study of our equations.

Even when selfsimilarity does not describe the asymptotics, it usually happens that the whole pattern consists of several pieces which have a selfsimilar form in a more or less disguised way and are tied together by matching. We will not discuss here these more elaborate theories; examples in nonlinear diffusion are abundant, see the book [28] and its references.

The paradigm of long-time behaviour in parabolic equations is the theory of the linear heat equation, $m = 1$, which is the standing reference in diffusion theory.

The asymptotic behaviour of the typical initial and boundary value problems in usual classes of solutions is a well researched subject for the HE. Both the asymptotic patterns and the rates of convergence are known under various assumptions. Thus, the well-known result for the Cauchy problem says that for nonnegative and integrable initial data $u_0 \in L^1(\mathbb{R}^n)$, $u_0 \geq 0$, there is convergence of the solution of the Cauchy problem towards a constant multiple of the Gaussian kernel, $u(x,t) \sim M\,G(x,t)$, where

$$G(x,t) := \frac{1}{(4\pi t)^{N/2}} \exp\{-|x|^2/4t\}, \tag{15}$$

and $M = \int u_0(x)\,dx$ is the mass of the solution (space integration is performed by default in $\mathbb{R}^n$). When the heat equation is viewed as the PDE expression of the basic linear diffusion process in probability theory, the functions $u(\cdot,t)$ with mass 1 are viewed as the probability distributions of a stochastic process and the formula $u(x,t) \sim M\,G(x,t)$ is a way of formulating the central limit theorem.

We will explore next the analogous of this result for the PME. We start by the investigation of the long-time behaviour of solutions of the PME with data $u_0 \in L^1(\mathbb{R}^n)$ in order to prove that for large t all such solutions can be described in first approximation by the one-parameter family of ZKB solutions (from Zeldovich, Kompanyeets and Barenblatt; often the last name is used in referring to them). They are explicitly given by formulas

$$\mathcal{U}(x,t;C) = t^{-\alpha}\left(C - k\,|x|^2 t^{-2\beta}\right)_+^{\frac{1}{m-1}}, \tag{16}$$

where $(s)_+ = \max\{s,0\}$,

$$\alpha = \frac{n}{n(m-1)+2}, \quad \beta = \frac{\alpha}{n}, \quad k = \frac{\beta(m-1)}{2\,m}. \tag{17}$$

The constant $C > 0$ is free and can be used to adjust the mass of the solution: $\int_{\mathbb{R}^n} \mathcal{U}(x,t;C)\,dx = M > 0$. Let us write $\mathcal{U}_M$ for the solution with mass M and F_M for its profile. Figure 1 compares the profiles.

This is the precise statement of the asymptotic convergence result.

Theorem 4.1. *Let $u(x,t)$ be the unique weak solution of the Cauchy problem for the PME posed in $Q = \mathbb{R}^n \times (0,\infty)$ with initial data $u_0 \in L^1(\mathbb{R}^N)$, and $\int_{\mathbb{R}^n} u_0\,dx = M > 0$. Let $\mathcal{U}_M$ be the ZKB solution with the same mass as u_0. As $t \to \infty$ the solutions $u(t)$ and $\mathcal{U}_M$ are increasingly close and we have*

$$\lim_{t\to\infty} \|u(t) - \mathcal{U}_M(t)\|_1 = 0. \tag{18}$$

Convergence holds also in L^∞-norm in the proper scale:

$$\lim_{t\to\infty} t^{\alpha}\|u(t) - \mathcal{U}_M(t)\|_\infty = 0 \tag{19}$$

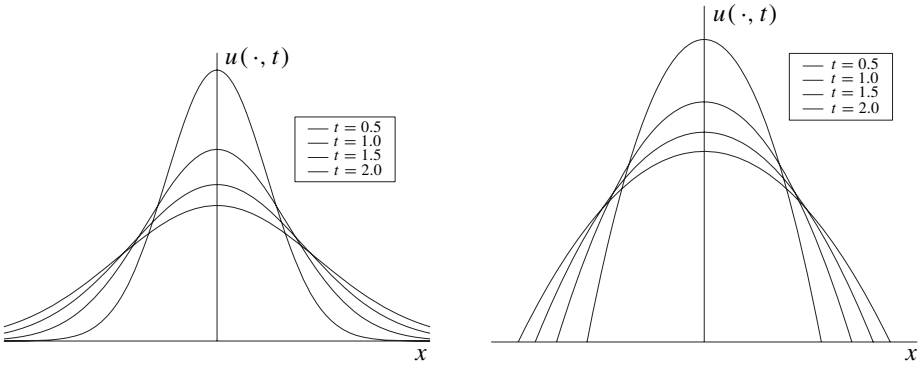


Figure 1. Comparison of the Gaussian profiles with the Barenblatt profiles.

with $\alpha = n/[n(m-1)+2]$. *Moreover, for every* $p \in (1,\infty)$ *we have*

$$\lim_{t\to\infty} t^{\alpha(p-1)/p}\|u(t) - \mathcal{U}_M(t)\|_{L^p(\mathbb{R}^n)} = 0. \tag{20}$$

Let now $\int_{\mathbb{R}^n} u_0\,dx = -M \le 0$. *The same result is true with* $\mathcal{U}_M$ *replaced by* $-\mathcal{U}_M(x.t)$ *when* $M < 0$, *and by* $\mathcal{U}_0(x,t) = 0$ *if* $M = 0$.

This result is one of the highlights of the theory of the PME. When applied to nonnegative solutions with mass 1 *it is the precise statement of the nonlinear central limit theorem for the evolution generated by the PME*. Proof of most of the result in several dimensions appeared in a celebrated paper by A. Friedman and S. Kamin [25]; however, uniform convergence was established only for nonnegative and compactly supported data. The complete proof with uniform convergence for nonnegative data in $L^1(\mathbb{R}^n)$ was done by Vázquez in [41]. In that paper seven different proofs are given. Signed solutions are admitted and even a right-hand side (forcing term) $f \in L^1(Q)$ is allowed and the limit (18) still holds.

Several remarks are in order: (1) According to this result, all the information the solution remembers from the initial configuration after a large time is reduced in first approximation only to the mass M, since the pattern and the rate are supplied by the equation. This is a very apparent manifestation of the equalizing effect of the diffusion.

(2) The PME replaces the Gaussian profile by the ZKB profile as the asymptotic pattern. This pattern has sharp fronts at a finite distance and no space tails, exponential or otherwise. This makes the PME a more realistic physical model than the HE since it avoids the problem of instantaneous propagation of signals at infinite distances.

(3) The standard deviation of the ZKB solution, and more generally of solutions that converge to it as $t \to \infty$, is $O(t^{\beta})$ and not $O(t^{1/2})$ as in the heat equation (in fact, the anomalous diffusion exponent β is less than $1/2$ for $m > 1$ and goes to zero as $m \to \infty$ or as $n \to \infty$). This makes the PME qualify as a type of *anomalous diffusion.*

(4) The convergence also takes place for the rescaled version of the equation in the Wasserstein distance d_2 [37]. But this is a different story in some sense.

(5) For a given solution u, there is only one correct choice of the constant $C = C(u_0)$ in these asymptotic estimates, since trying two ZKB solutions with different constants in the above formulas produces non-zero limits. In that sense, the estimates are sharp.

(6) The result is optimal in the sense that we cannot get better convergence rates in the general class of solutions $u_0 \in L^1(\mathbb{R}^n)$, even if we assume $u_0 \geq 0$. Explicit counterexamples settle this question.

(7) It can be further proved that whenever $m > 1$ and we take signed initial data with compact support and the total mass is positive, $M > 0$, then, the solution becomes nonnegative after a finite time. This result is not true if the restriction of compact support is eliminated.

Proof by scaling. The idea is as follows: given a solution $u = u(x,t) \geq 0$ of the PME in the class of strong solutions with finite mass, we obtain a family of solutions

$$\widetilde{u}_\lambda(x,t) = (\mathcal{T}_\lambda u)(x,t) = \lambda^\alpha u(\lambda^\beta x, \lambda\, t) \tag{21}$$

with initial data $\widetilde{u}_{0,\lambda}(x) = (\mathcal{T}_\lambda u_0)(x) = \lambda^\alpha u_0(\lambda^\beta x)$. The exponents α and β are related by

$$\alpha(m-1) + 2\beta = 1, \tag{22}$$

so that all the $\widetilde{u}_\lambda$ are again solutions of the PME. This is the scaling formula that we call the λ-scaling or *fixed scaling*. It is in fact a family of scalings with free parameter $\lambda > 0$, that performs a kind of *zoom* on the solution. In the present application we have another constraint that allows to fix both α and β to the desired values (the Barenblatt values). It is the condition of mass conservation. We only need to impose it at $t = 0$,

$$\int_{\mathbb{R}^n} (\mathcal{T}_\lambda u_0)(x)\, dx = \int_{\mathbb{R}^n} u_0(x)\, dx, \tag{23}$$

and we get $\alpha = n\,\beta$. Together with (22), this implies that α and β have the values (17) of the theorem. Note that the source-type solutions are invariant under this mass conserving λ-rescaling, i.e.

$$\mathcal{U}_M(t) = \mathcal{T}_\lambda(\mathcal{U}_M(t)).$$

The proof continues by showing that the family $\{\widetilde{u}_\lambda(t), \lambda > 0\}$, is uniformly bounded and even relatively compact in suitable functional spaces. We then pass to the limit dynamics when $\lambda \to \infty$ and identify the obtained object as the ZKB solution. We refer to [44]; Chapter 18, for complete details on the issue.

4.1. Continuous scaling: Fokker–Planck equation. A different way of implementing the scaling of the orbits of the Cauchy problem and proving the previous facts consists of using the *continuous rescaling*, which is written in the form

$$\theta(\eta,\tau) = t^\alpha u(x,t), \quad \eta = x\, t^{-\beta}, \quad \tau = \ln t, \tag{24}$$

with α and β the standard similarity exponents given by (17). Then t^α and t^β are called the *scaling factors* (or *zoom factors*), while τ is the *new time*. This version of the scaling technique has a very appealing dynamical flavor. The reader should note that *every asymptotic problem has its corresponding zoom factors that have to be determined as a part of the analysis.* In our case, the rescaled orbit $\theta(\tau)$ satisfies the equation

$$\theta_\tau = \Delta(\theta^m) + \beta\eta \cdot \nabla\theta + \alpha\theta. \tag{25}$$

This is the continuously rescaled dynamics. Since we also have the relation $\alpha = n\,\beta$, we can write the equation in divergence form as

$$\theta_\tau = \Delta(\theta^m) + \beta\,\nabla \cdot (\eta\,\theta). \tag{26}$$

This is a particular case of the so-called *Fokker–Planck equations* which have the general form

$$\partial_t u = \Delta(|u|^{m-1}u) + \nabla \cdot (\mathbf{a}(x)u), \quad \mathbf{a}(x) = \nabla V(x). \tag{27}$$

The last term is interpreted as a confining effect due to a potential V. In our case $V(x) = \beta\,|x|^2/2$, the quadratic potential. The study of Fokker–Planck equations is interesting in itself and not only in connection with the HE and the PME.

This *dynamical systems approach* allows us to see the contents of the asymptotic theorem in a better way: the orbit $\theta(\tau)$ is bounded uniformly in $L^1(\mathbb{R}^n) \cap L^\infty(\mathbb{R}^n)$; the source-type (ZKB) solutions transform into the stationary profiles F_M in this transformation, i.e., $F(\eta)$ solves the nonlinear elliptic problem

$$\Delta f^m + \beta\,\nabla \cdot (\eta\,f) = 0; \tag{28}$$

moreover, boundedness of the orbit is established; this and convenient compactness arguments allow to pass to the limit and form the ω-limit, which is the set

$$\omega(\theta) = \{f \in L^1(\Omega) : \text{there exists } \{\tau_j\} \to \infty \text{ such that } \theta(\tau_j) \to f\}. \tag{29}$$

The convergence takes place in the topology of the functional space in question, here any $L^p(\Omega)$, $1 \le p \le \infty$. The end of the proof consists in showing that the ω-limit is just the Barenblatt profile F_M. The argument can be translated in the following way. Corresponding to the sequence of scaling factors λ_n of the previous scaling, we take a sequence of delays $\{s_n\}$ and define $\theta_n(\eta, \tau) = \theta(\eta, \tau + s_n)$. The family $\{\theta_n\}$ is precompact in $L^\infty_{\mathrm{loc}}(\mathbb{R}_+ : L^1(\mathbb{R}^n))$ hence, passing to a subsequence if necessary, we have

$$\theta_n(\eta, \tau) \to \widetilde{\theta}(\eta, \tau). \tag{30}$$

Again, it is easy to see that $\widetilde{\theta}$ is a weak solution of (26) satisfying the same estimates. The end of the proof is identifying it as a stationary solution, $\widetilde{\theta}(\eta, \tau) = F_M(\eta)$, the Barenblatt profile of the same mass.

4.2. The entropy approach: convergence rates. A number of interesting results complement this basic convergence result in the recent literature. Thus, the question of obtaining an estimate of the rate at which rescaled trajectories of the PME stabilize towards the Barenblatt profile has attracted much attention. The main tool of investigation has been the consideration of the so-called *entropy functional*, defined as follows

$$H_\theta(\tau) = \int_{\mathbb{R}^n} \left\{ \frac{1}{m-1}\theta^m + \frac{\beta}{2}\eta^2\,\theta \right\} d\eta, \tag{31}$$

where $\theta = \theta(\eta, \tau)$ is the rescaled solution just defined and $\beta = 1/(n(m-1)+2)$ is the similarity exponent. H_θ represents a measure of the entropy of the mass distribution $\theta(\tau)$ at any time $\tau \geq 0$ which is well adapted to the renormalized PME evolution. Note that the entropy need not be finite for all solutions, a sufficient condition is

$$u_0 \in L^1(\mathbb{R}^n) \cap L^\infty(\mathbb{R}^n), \quad \int x^2 u_0(x)\,dx < \infty. \tag{32}$$

These properties will then hold for all times. Note that the restriction of boundedness is automatically satisfied for positive times.

Actually, we can calculate the variation of the entropy in time along an orbit of the Fokker–Planck equation, and under the above conditions on u_0, we find after an easy computation that

$$\frac{dH_\theta}{d\tau} = -I_\theta, \quad \text{where } I_\theta(\tau) = \int \theta \left| \nabla \left(\frac{m}{m-1}\theta^{m-1} + \frac{\beta}{2}\eta^2 \right) \right|^2 d\eta \geq 0. \tag{33}$$

We now pass to the limit along sequences $\theta_n(\tau) = \theta(\tau + s_n)$ to obtain limit orbits $\widetilde{\theta}(\tau)$, on which the Lyapunov function is constant, hence $dH_{\widetilde{\theta}}/d\tau = 0$. The proof of asymptotic convergence concludes in the present instance in a new way, by analyzing when $dH_\theta/d\tau$ is zero. Here is the crucial observation that ends the proof: the second member of (33) vanishes if and only if θ is a Barenblatt profile.

Let us now introduce some notations: the difference $H(\theta|\theta_\infty) = H(\theta) - H(\theta_\infty)$ is called the *relative entropy*. Function I_θ is called the *entropy production*. We can use the entropy functional to improve the convergence result by obtaining rates of convergence. This is done by computing $d^2H_\theta/d\tau^2$, the so-called Bakry–Emery analysis in the heat equation case which has been adapted to the PME by J. A. Carrillo and G. Toscani [17]. The final result of the second derivative computation is

$$\frac{dI}{d\tau} = -2\beta\, I(\tau) - R(\tau), \tag{34}$$

for a certain term $R \geq 0$. Since we know by the previous analysis that $H(\theta|\theta_\infty)$ and I_θ go to zero as $\tau \to \infty$, we conclude the following result.

Theorem 4.2. *Under the assumption that the initial entropy is finite and some regularity assumptions, we have*

$$I(\tau) \leq A\, e^{-2\beta\tau}, \quad 0 \leq H(\theta|\theta_\infty)(\tau) \leq \frac{1}{2\beta} I(\tau), \quad H(\theta|\theta_\infty) \leq B\, e^{-2\beta\tau}. \tag{35}$$

As a consequence, the convergence towards the ZKB stated in Theorem 4.1 *happens with an extra factor* t^γ *in formulas* (18)–(20)*, where*

$$\gamma = \beta \quad \text{if } 1 < m \le 2, \quad \gamma = \frac{2\beta}{m} \quad \text{if } m \ge 2, \tag{36}$$

and $\beta = 1/(n(m-1)+2)$.

In dimension $n = 1$, a convergence theorem with sharp rates can be proved by adjusting not only the mass but also the center of mass, cf. [40]. It is an open problem for $n > 1$.

4.3. Eventual concavity. There are many other directions in which the asymptotic behaviour of the PME is made more precise. This is the geometrical result obtained by Lee–Vázquez [34] (Figure 2 shows a practical instance).

Theorem 4.3. *Let* u *be a solution of the PME in* $n \ge 1$ *space dimensions with compactly supported initial data* (*and satisfying a certain non-degeneracy condition*). *Then there is* $t_c > 0$ *such that the pressure* $v(x,t)$ *is a concave function in* $\mathcal{P}(t) = \{x : v(x,t) > 0\}$ *for* $t \ge t_c$. *More precisely, for any coordinate directions* x_i, x_j,

$$\lim_{t\to\infty} t\,\frac{\partial^2 v}{\partial x_i^2} = -\beta, \quad \lim_{t\to\infty} t\,\frac{\partial^2 v}{\partial x_i \partial x_j} = 0, \tag{37}$$

uniformly in $x \in \operatorname{supp}(v)$, $i, j = 1, \dots, n$, $i \ne j$. *Here,* $\beta = 1/(n(m-1)+2)$.

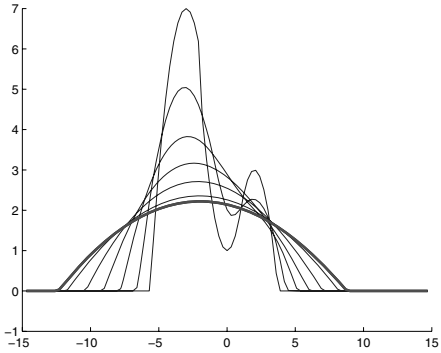


Figure 2. Evolution towards selfsimilarity and eventual concavity in the PME.

4.4. Extensions. In the case of the Cauchy–Dirichlet problem posed in a bounded domain $\Omega \subset \mathbb{R}^N$, it is well known that the asymptotic shape of any solution of the heat equation with nonnegative initial data in $L^2(\Omega)$ approaches one of the special *separated variables solutions*

$$u_1(x,t) = c\,T_1(t)\,F_1(x). \tag{38}$$

Here $T_1(t) = e^{-\lambda_1 t}$, where $\lambda_1 = \lambda_1(\Omega) > 0$ is the first eigenvalue of the Laplace operator in Ω with zero Dirichlet data on $\partial\Omega$, and the space pattern $F_1(x)$ is the corresponding positive and normalized eigenfunction. The constant $c > 0$ is determined as the coefficient of the $L^2(\Omega)$-projection of u_0 on F_1. For the PME a similar result is true with the following differences: $F_1(x)$ is the ground state of a certain nonlinear eigenvalue problem, while $T_1(t) = t^{-1/(m-1)}$, which means power decay in time. For signed solutions there exists a whole sequence of compactly supported profiles $F_k(x)$ as candidates for the separation-of-variables formula (38), but the time factor is always the same $T_1(t) = t^{-1/(m-1)}$; this is a striking difference with the linear case in which the exponentials have an increasing sequence of coefficients.

The analysis applies to the homogeneous Neumann problem and leads to a marked difference between data with positive or negative mass, where the solutions stabilize to the constant state with exponential speed (just as linear flows) and the case of zero mass, where the $t^{-1/(m-1)}$ time factor appears.

Another extension consists of considering the whole space with a number of holes; Dirichlet or Neumann boundary conditions are imposed on the boundary Γ of the holes. If for instance conditions of the form $u = 0$ are chosen on Γ, then the Barenblatt profiles still appear as the asymptotic patterns in dimension $n \geq 3$, but not in dimension $n = 1$ while dimension $n = 2$ is a borderline case [30], [9]. Actually, the influence of the holes is felt in terms of their capacity, which has an interesting physico-geometrical interpretation. Dependence on dimension is very typical of nonlinear diffusion problems, it will appear again in fast diffusion flows and is a very prominent feature in blow-up problems.

5. Some lines of research

The theory of the PME is by now well understood in the case of dimension one, but it still has gaps for $n > 1$ because n dimensional PME flows turned out to be much more complicated. Thus, the regularity of nonnegative solutions is effectively solved for $n = 1$ by stating the best Hölder regularity (the pressure is Lipschitz continuous but not C^1) and showing the worst case situation, that corresponds to the presence of moving free boundaries that always follow the same pattern, the solution locally behaves like a travelling wave. The same question in dimension $n > 1$ is still only partially understood even after intensive work of D. Aronson and coworkers [2], [3] on the so-called focusing problem. They discovered first the radial solutions with limited Hölder regularity and then the nonradial focusing modes with elongated shapes bifurcating from the radial branch as m varies (a typical break of stability in a bifurcation branch, somewhat similar to the Taylor–Couette hydrodynamical instabilities).

After the work of L. Caffarelli et al. [12], [15], the C^∞ regularity of the solutions up to the free boundary and also of the free boundary as a hypersurface was proved for large times by H. Koch [32] under convenient conditions on the data, but further progress is expected.

Even in the theory of nonnegative solutions of the Cauchy problem for the PME, there are still some basic analytical problems, like the following: the theory is very much simplified by the existence of the Aronson–Bénilan pointwise estimate $\Delta u^{m-1} \geq -C/t$. A local version of this estimate is known only in dimension $n = 1$.

On the other hand, the question of obtaining solutions for the widest possible class of initial data has been successfully solved for nonnegative solutions, but only partially understood for signed solutions. See [44], Chapters 12 and 13.

If we replace the exponent 2 by $p \in [1, \infty]$ in the Wasserstein formula (13), we get the Wasserstein non-quadratic distances. The PME semigroup is contractive in all of them in dimension $n = 1$. In particular, contraction in the d_∞ norm allows for fine estimates of the support propagation. Unfortunately, the PME semigroup is not contractive in the distance d_p for p large if $n > 1$, [42]. Actually, a similar negative result happens for the usual L^p norms in all space dimensions, see [44]. Determining the precise ranges of p for these contractivity issues is still an open problem.

6. Fast diffusion equations: physics and geometry

The fast diffusion equation is formally the same as the PME but the exponent is now $m < 1$. It appears in several areas of mathematics and science when the assumptions of linear diffusion are violated in a direction contrary to the PME. Here are some examples.

• Plasma diffusion with the Okuda–Dawson scaling implies a diffusion coefficient $D(u) \sim u^{-1/2}$ in the basic equation $u_t = \nabla \cdot (D(u)\nabla u)$, where u is the particle density. This leads to the FDE with $m = 1/2$. Other models imply exponents $m = 0$, $D(u) \sim 1/u$, or even $m = -1$, $D(u) \sim 1/u^2$.

• A very popular fast diffusion model was proposed by Carleman to study the diffusive limit of kinetic equations. He considered just two types of particles in a one dimensional setting moving with speeds c and $-c$. If the densities are u and v respectively you can write their simple dynamics as

$$\left.\begin{aligned} \partial_t u + c\,\partial_x u &= k(u, v)(v - u) \\ \partial_t v - c\,\partial_x v &= k(u, v)(u - v) \end{aligned}\right\} \tag{39}$$

for some interaction kernel $k(u, v) \geq 0$. Put in a typical case $k = (u + v)^\alpha c^2$. Write now the equations for $\rho = u + v$ and $j = c(u - v)$ and pass to the limit $c = 1/\varepsilon \to \infty$ and you will obtain to first order in powers or $\varepsilon = 1/c$:

$$\frac{\partial \rho}{\partial t} = \frac{1}{2}\frac{\partial}{\partial x}\left(\frac{1}{\rho^\alpha}\frac{\partial \rho}{\partial x}\right), \tag{40}$$

which is the FDE with $m = 1 - \alpha$, cf. [35]. The typical value $\alpha = 1$ gives $m = 0$, a surprising equation that we will find below! The rigorous investigation of the diffusion limit of more complicated particle/kinetic models is an active area of investigation.

• The fast diffusion makes a striking appearance in differential geometry, in the evolution version of the Yamabe problem. The standard Yamabe problem starts with a Riemannian manifold (M, g_0) in space dimension $n \geq 3$ and deals with the question of finding another metric g in the conformal class of g_0 having constant scalar curvature. The formulation of the problem proceeds as follows in dimension $n \geq 3$. We can write the conformal relation as

$$g = u^{4/(n-2)} g_0$$

locally on M for some positive smooth function u. The conformal factor is $u^{4/(n-2)}$. Next, we denote by $R = R_g$ and R_0 the scalar curvatures of the metrics g, g_0 resp. If we write Δ_0 for the Laplace–Beltrami operator of g_0, we have the formula $R = -u^{-N} Lu$ on M, with $N = (n+2)/(n-2)$ and

$$Lu := \kappa \Delta_0 u - R_0 u, \quad \kappa = \frac{4(n-1)}{n-2}.$$

The Yamabe problem becomes then

$$\Delta_0 u - \left(\frac{n-2}{4(n-1)}\right) R_0 u + \left(\frac{n-2}{4(n-1)}\right) R_g u^{(n+2)/(n-2)} = 0. \tag{41}$$

The equation should determine u (hence, g) when g_0, R_0 and R_g are known. In the standard case we take $M = \mathbb{R}^n$ and g_0 the standard metric, so that Δ_0 is the standard Laplacian, $R_0 = 0$, we take $R_g = 1$ and then we get the well-known semilinear elliptic equation with critical exponent.

In the evolution version, the Yamabe flow is defined as an evolution equation for a family of metrics that is used as a tool to construct metrics of constant scalar curvature within a given conformal class. More precisely, we look for a one-parameter family $g_t(x) = g(x, t)$ of metrics solution of the evolution problem

$$\partial_t g = -R\, g, \quad g(0) = g_0 \quad \text{on } M. \tag{42}$$

It is easy to show that this is equivalent to the equation

$$\partial_t (u^N) = Lu, \quad u(0) = 1 \quad \text{on } M.$$

after rescaling the time variable. Let now (M, g_0) be $\mathbb{R}^n$ with the standard flat metric, so that $R_0 = 0$. Put $u^N = v$, $m = 1/N = (n-2)/(n+2) \in (0, 1)$. Then

$$\partial_t v = L v^m, \tag{43}$$

which is a fast diffusion equation with exponent $m_y \in (0, 1)$ given by

$$m_y = \frac{n-2}{n+2}, \quad 1 - m_y = \frac{4}{n+2}.$$

If we now try separate variables solutions of the form $v(x,t) = (T-t)^{\alpha} f(x)$, then necessarily $\alpha = 1/(1-m_y) = (n+2)/4$, and $F = f^m$ satisfies the semilinear elliptic equation with critical exponent that models the stationary version:

$$\Delta F + \frac{n+2}{4} F^{\frac{n+2}{n-2}} = 0. \tag{44}$$

We will stop at this point the motivation of nonlinear diffusion coming from geometry, to return later with the logarithmic diffusion. The influence of PDE techniques is strongly felt in present-day differential geometry, cf. A. Chang's exposition at the 2002 ICM [18].

6.1. Behaviour of fast diffusion flows: the good range. For values $m \sim 1$ the difference with the PME is noticed in the infinite speed of propagation: solutions with nonnegative data become immediately positive everywhere in the space domain (be it finite or infinite). This looks like the heat equation and in some sense it is. When we look at the source solutions we find explicit Barenblatt functions

$$U_m(x,t;M)^{1-m} = \frac{t}{C\,t^{2\alpha/n} + k_1\,x^2}, \tag{45}$$

with $C = a(m,n)M^{2(m-1)\alpha/n}$ and k_1 is an explicit function of m and n. Figure 3 shows the form.

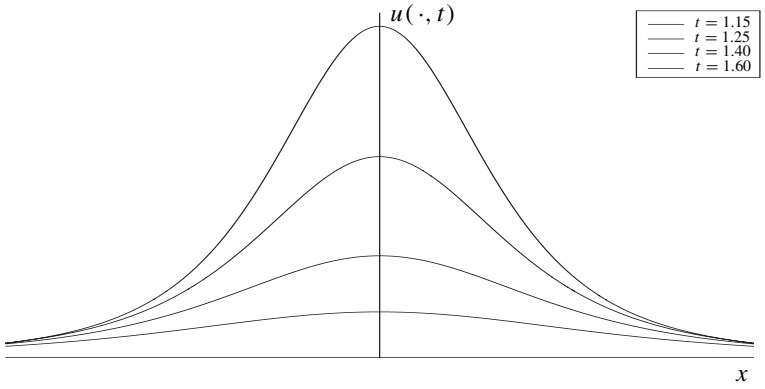


Figure 3. The fast diffusion solution with fat tails.

The main difference in the ZKB profiles is the power-like tail at infinity, which very much differs from the Gaussian (exponential) behaviour. These tails, called fat tails, are currently the object of study in several areas of economy, finance and statistical physics and their properties and role are still not well understood.

The new Barenblatt solutions play the same role they played for $m > 1$ even if they have a different shape. Indeed, the asymptotic behaviour of general solution is

still described by Theorem 4.1 if $m_c < m < 1$, where $m_c = (n-2)_+/n$ is called the first critical exponent. Actually, the convergence is better: we have proved in [41] that the relative error $e(x,t) = u(x,t)/U_m(x,t) - 1$ converges to zero uniformly in x as $t \to \infty$, a property that is obviously false for $m > 1$ because of the (slightly) different supports.

6.2. Behaviour of fast diffusion flows: the subcritical range. Significant novelties in the mathematical theory of the FDE appear once we cross the line $m = m_c$ downwards. Then, the picture changes and we enter a realm of strange diffusions. Note that m_c is larger than the Yamabe exponent m_y. Thus, concerning the basic problem of optimal space for existence, H. Brezis and A. Friedman proved in [10] that there can be no solution of the equation if $m \le m_c$ when the initial data is a Dirac mass, so that we lose the source solution, our main example of the range $m > m_c$. M. Pierre [39] extended the non-existence result to measures supported in sets of small capacity if $m < m_c$. But at least solutions exist for all initial data $u_0 \in L^1_{\rm loc}(\mathbb{R}^n)$ when $0 < m < m_c$, and moreover they are global in time, $u \in C([0,\infty) : L^1_{\rm loc}(\mathbb{R}^n))$. Such an existence result is not guaranteed when we go further down in exponent, $m \le 0$; then, solutions with initial data in $L^1(\mathbb{R}^n)$ just do not exist.

However, and contrary to the 'upper' fast diffusion range $m_c < m < 1$, it is not true that locally integrable data produce locally bounded solutions at positive times, as in the various examples constructed in [43]. Attention must be paid therefore to the existence and properties of large classes of weak solutions that are not smooth, not even locally bounded. This leads to a main fact to be pointed out about smoothing estimates: there can be no L^1-L^∞ effects.

Extinction and Marcinkiewicz spaces. For $m < m_c$ (even for $m \le 0$) there is an explicit example of solution which completely vanishes in finite time, and has the form

$$U(x,t;T) = c\left(\frac{T-t}{|x|^2}\right)^{1/(1-m)} \tag{46}$$

with $T > 0$ arbitrary, and $c = c(m,n) > 0$ a given constant. Formula (46) produces a weak solution of the FDE that is positive and smooth for $0 < t < T$ and $x \neq 0$; note further that it belongs to the Marcinkiewicz space $M^{p_*}(\mathbb{R}^n)$ with $p_* = n(1-m)/2$, a quantity that is larger than 1 if $m < m_c$.

The positive result that we can derive from comparison with this solution is the following.

Theorem 6.1. *Let $n \ge 3$ and $m < m_c$. For every $u_0 \in M^{p_*}(\mathbb{R}^n)$, there exists a time $T > 0$ such that $u(x,t)$ vanishes for $t \ge T$. It can be estimated as*

$$0 < T \le d\,\|u_0\|_{M^{p_*}}^{1-m} := T_1(u_0) \tag{47}$$

with $d = d(m,n) > 0$. Moreover, for all $0 < t < T$ we have $u(t) \in M^{p_*}(\mathbb{R}^n)$ and $u^*(t) \prec U(t;T)$ where T is chosen so that $U(x,0;T)$ has the same M^{p_*}-norm as u_0, i.e., $M = c_m T^{1-m}$.

The relevant functional spaces $M^p(\mathbb{R}^n)$ are the so-called Marcinkiewicz spaces or weak L^p spaces, defined for $1 < p < \infty$ as the set of locally integrable functions such that

$$\int_K |f(x)|dx \le C|K|^{(p-1)/p},$$

for all subsets K of finite measure. It is further proved that solutions with data in the space $M^p(\mathbb{R}^n)$ with $p > p_*$ become bounded for all positive times and do not necessarily extinguish in finite time, while solutions with data in the space $M^p(\mathbb{R}^n)$ with $1 < p < p_*$ become L^1 functions for all positive times and do not necessarily extinguish in finite time, see [43], Chapter 5. While becoming bounded is a typical feature of the parabolic theory (called the L^∞ smoothing effect), becoming L^1 is a kind of extravaganza that happens for these fast diffusion flows (it was introduced and called *backward effect* in [43]).

Delayed regularity. A further curious effect is proved in Chapter 6 of the same reference: functions in the larger space $M^{p_*}(\mathbb{R}^n) + L^\infty(\mathbb{R}^n)$ typically preserve their unboundedness for a time $T > 0$ and then become bounded. This is also called *blow-down* in finite time.

Large-time behaviours: selfsimilarity with anomalous exponents. The actual asymptotic behaviour of the solutions of the FDE in the exponent range $0 < m < m_c$ depends on the class of initial data. We are interested in "small solutions" that extinguish in finite time, We will concentrate on solutions that start with initial data in $L^1(\mathbb{R}^n)$, or solutions that fall into this class for positive times previous to extinction by the backward effect. In the range $m > m_c$ the ZKB solutions provide the clue to the asymptotics for all nonnegative solutions with L^1-data. We know that these solutions do not exist in the range $m < m_c$. So we need to look for an alternative. This alternative has to take into account the fact that solutions with M^{p_*}-data disappear (vanish identically) in finite time.

The class of self-similarity solutions of the form

$$U(x,t) = (T-t)^\alpha f(x\,(T-t)^\beta), \tag{48}$$

called selfsimilar of Type II, will provide the clue to the asymptotic behaviour near extinction. We have to find the precise exponents and profile that correspond to a solution of the form (48) and represent the large time behaviour of many other solutions. We know from the start that $\alpha(1-m) = 2\beta + 1$. But there is no conservation law that dictates to us the remaining relation needed to uniquely identify the exponents. This may seem hopeless but the representative solutions exist and have precise exponents and profile. This is a situation that appears with a certain frequency in mechanics and was called by Y. Zel'dovich *self-similarity of the second kind*, the exponents being known as *anomalous exponents.* Anomalous means here that the exponents cannot be obtained from dimensional considerations or conservation laws, as is done in the ZKB case by means of the scaling group. Such kind of solutions is of great interest because of their analytical difficulty.

The selection rule for the anomalous exponents is usually topological, tied to the existence and behaviour of the solutions of a certain nonlinear eigenvalue problem. In the present case, the selection is done through the existence of a special class of self-similar solutions with fast decay at infinity. The construction was performed by J. King, M. Peletier and H. Zhang [31], [38] and is extended and described in detail in [43], Chapter 7. We call them KPZ solutions.

We can then pass to the question of convergence of general classes of solutions towards the KPZ solutions. This is in analogy to the results for the ZKB profiles for $m > m_c$. The results are more complete when $m = m_y$, where the problem has a nice geometrical interpretation. The proof of convergence results towards the KPZ solution is only known in the case of radial solutions when $m \neq m_y$, cf. [26].

FDE with exponent $m = (n-2)/(n+2)$: Yamabe problem. The exponent is special in the sense that when we separate variables and pass to the Emden–Fowler equation for $G = F^m$

$$-\Delta G = G^p, \tag{49}$$

then $p = 1/m$ equals the Sobolev exponent $p_s = (n+2)/(n-2)$, that is known to have a great importance in the theory of semilinear elliptic equations. We may thus call m_y the Sobolev exponent of the FDE. We recall that the FDE is related for this precise exponent to the famous Yamabe flow of Riemannian geometry. As we have said, this flow is used by geometers as a tool to deform Riemannian metrics into metrics of constant scalar curvature within a given conformal class. Returning to the consideration of the family of KPZ solutions with anomalous exponents, this is the "easy case" where $\beta = 0$ (that corresponds to separate variables) so that $\alpha = (n+2)/4$. The corresponding family of self-similar solutions is explicitly known and given by the Loewner–Nirenberg formula

$$F(x,\lambda) = k_n \left(\frac{\lambda}{\lambda^2 + |x|^2} \right)^{(n+2)/2} \tag{50}$$

with $k_n = (4n)^{(n+2)/4}$ and $\lambda > 0$ arbitrary. These patterns represent conformal metrics with constant curvature in the geometrical interpretation. Here is the result of [21] as improved in [43], Chapter 7.

Theorem 6.2. *Let $n \geq 3$ and $m = (n-2)/(n+2)$ and let $u(x,t) \geq 0$ be a solution of the FDE existing for a time $0 < t < T$. Under the assumption that $u_0 \in L^{2n/(n+2)}(\mathbb{R}^n)$ the solution of the FDE is bounded for all $t > 0$. Moreover, there exist λ and $x_0 \in \mathbb{R}^n$ such that*

$$(T-t)^{-(n+2)/4} u(x,t) = F(x - x_0, \lambda) + \theta(x,t) \tag{51}$$

and $\|\theta(t)\|_{L^{p*}} \to 0$ as $t \to T$. The exponent in the space assumption is optimal.

We just recall that $p_* = 2n/(n+2)$ in the present case.

Exponential decay at the critical end-point. Inspection of the ZKB solutions as m goes down to m_c shows that asymptotic decay happens as $t \to \infty$ with increasing powers of time, i.e., $u \sim t^{-\alpha}$ and $\alpha \to \infty$. Exponential decay holds for the FDE with critical exponent m_c for a large number of initial, but not for all L^1 data. We have

Theorem 6.3. *Let $m = m_c$ and $n \geq 3$. Solutions in $L^1(\mathbb{R}^n) \cap L^\infty(\mathbb{R}^n)$ decay in time according to the rate*

$$\log(1/\|u(t)\|_\infty) \sim C(n) M^{-2/(n-2)} t^{n/(n-2)} \tag{52}$$

as $t \to \infty$, $M = \|u_0\|_1$. This rate is sharp.

This behaviour is not selfsimilar and has been calculated by V. Galaktionov, L. Peletier and J. L. Vázquez in [27], based on previous formal analysis of J. King [31]. The proof uses a delicate technique of matched asymptotics with an outer region which after a nonlinear transformation undergoes convergence to a selfsimilar profile of convective type. This is said here to show that unexpected patterns can appear as the result of these manipulations. Slower pace of decay happens for non-integrable solutions, as the following selfsimilar example shows

$$u(x,t) = \frac{1}{(bx^2 + ke^{2nbt})^{n/2}}, \quad b, k > 0. \tag{53}$$

7. Logarithmic diffusion

The fast diffusion equation in the limit case $m = 0$ in two space dimensions is a favorite case in the recent literature on fast diffusion equations. The equation can be written as

$$\partial_t u = \operatorname{div}(u^{-1} \nabla u) = \Delta \log(u), \tag{54}$$

hence the popular name of *logarithmic diffusion.* The problem has a particular appeal because of its application to differential geometry, since it describes the evolution of surfaces by Ricci flow. More precisely, it represents the evolution of a conformally flat metric g by its Ricci curvature,

$$\frac{\partial}{\partial t} g_{ij} = -2 \operatorname{Ric}_{ij} = -R\, g_{ij}, \tag{55}$$

where Ric is the Ricci tensor and R the scalar curvature. If g is given by the length expression $ds^2 = u\,(dx^2 + dy^2)$, we arrive at equation (54). This flow, proposed by R. Hamilton in [29], is the equivalent of the Yamabe flow in two dimensions. We remark that what we usually call the mass of the solution (thinking in diffusion terms) becomes here the *total area* of the surface, $A = \iint u\, dx_1 dx_2$.

Several peculiar aspects of the theory are of interest: non-uniqueness, loss of mass, regularity and asymptotics. Maybe the most striking is the discovery that conservation of mass is broken in a very precise way.

• Let us consider integrable data. This is the basic result of the theory.

Theorem 7.1. *For every $u_0 \in L^1(\mathbb{R}^2)$, with $u_0 \geq 0$ there exists a unique function $u \in C([0,T) : L^1(\mathbb{R}^2))$, which is a classical ($C^\infty$ and positive) solution of* (54) *in Q_T and satisfies the area constraint*

$$\int u(x,t)dx = \int u_0(x)dx - 4\pi\, t. \tag{56}$$

Such solution is maximal among the solutions of the Cauchy problem for (54) *with these initial data, and exists for the time $0 < t < T = \int_{\mathbb{R}^2} u_0(x)\,dx/4\pi$. Moreover, the solution is obtained as the limit of positive solutions with initial data $u_{0\varepsilon}(x) = u_0(x) + \varepsilon$ as $\varepsilon \to 0$.*

The mysterious loss of 4π units of area (mass) has attracted the attention of researchers. In the geometrical application it is quite easy to see it as a form of the Gauss–Bonnet theorem. It is shown that the Gaussian curvature K is given by $K = \Delta u/2u$, and then

$$\int_{\mathbb{R}^2} u_t\,dx = -2\int_M K\,d\,\mathrm{Vol}_g = -4\pi.$$

There are also analytical proofs of this fact, that look a bit mysterious, see [43], Chapter 8.

• One of the peculiar properties of this equation is the existence of multiple solutions with finite area with the same initial data that are characterized by the behaviour at infinity. The situation is completely understood in the radial case and the following general result is proved.

Theorem 7.2. *For every nonnegative radial function $u_0 \in L^1(\mathbb{R}^2)$ and for every bounded function $f(t) \geq 2$, there exists a unique function $u \in C([0,T) : L^1(\mathbb{R}^2))$, which is a radially symmetric and classical solution of (P_0) in Q_T and satisfies the mass constraint*

$$\int u(x,t)dx = \int u_0(x)dx - 2\pi\int_0^t f(\tau)\,d\tau. \tag{57}$$

It exists as long as the integral in the LHS is positive. The case $f = 0$ corresponds to the maximal solution of the Cauchy problem. In any case, the solution is bounded for all $t > 0$.

Thus, not only there are infinitely many solutions for every fixed nontrivial initial function u_0, but also the extinction time can be controlled by means of the flux data f. Moreover, these solutions satisfy the asymptotic spatial behaviour

$$\lim_{r\to\infty} r\,\partial_r(\log u(r,t)) = -f(t) \tag{58}$$

for a.e. $t \in (0,T)$. Non-uniqueness extends to non-integrable solutions. Thus, the stationary profile

$$u(x_1,x_2,t) = Ae^{Bx_1}, \quad A, B > 0,$$

is not the unique solution with such data, it is not even the maximal solution.

• Actually, the geometrical interpretation in the case of data with finite area favors the flow with conditions at infinity $f = 4$, hence the mass loss per unit time equals 8π, which are interpreted as regular closed compact surfaces. Here is the most typical example

$$u(x,t) = \frac{8(T-t)}{(1+x^2)^2}, \tag{59}$$

which represents the evolution of a ball with total area $\int u(x,t)\,dx = 8\pi(T-t)$.

• Coming to the regularity question, solutions with data in $L^1(\mathbb{R}^2)$ are bounded. But the limit when the data tend to a measure, more precisely to a Dirac mass, is not included. Indeed, when we approximate a Dirac delta $M\delta(x)$ by smooth integrable functions $\varphi_n(x)$, solve the problem in the sense of maximal solutions $u_n(x,t)$ and pass to the limit in the approximation, the following result is obtained

$$\lim_{n\to\infty} u_n(x,t) = (M - 4\pi t)_+\delta(x). \tag{60}$$

In physical terms, it means that logarithmic diffusion is unable to spread a Dirac mass, but somehow it is able to dissipate it in finite time. A delicate thin layer process occurs by which the mass located at $x = 0$ is transferred to $x = \infty$ without us noticing. We explain this phenomenon in the recent paper [45] where the following result is proved: we assume that the initial mass distribution can be written as

$$d\mu_0(x) = f(x)dx + \sum_{i=1}^{k} M_i\,\delta(x - x_i). \tag{61}$$

where $f \geq 0$ is an integrable function in $\mathbb{R}^2$, the $x_i, i = 1, \ldots, k$, are a finite collection of (different) points on the plane, and we are given masses $0 < M_k \leq \cdots \leq M_2 \leq M_1$. The total mass of this distribution is

$$M = M_0 + \sum_{i=1}^{k} M_i, \quad \text{with } M_0 = \int f\,dx. \tag{62}$$

We construct a solution for this problem as the limit of natural approximate problems with smooth data:

Theorem 7.3. *Under the stated conditions, there exists a limit solution of the log-diffusion Cauchy problem posed in the whole plane with initial data μ_0. It exists in the time interval $0 < t < T$ with $T = M/2\pi$. It satisfies the conditions of maximality at infinity.*

More precisely, the solution is continuous into the space of Radon measures, $u \in C([0,T] : \mathcal{M}(\mathbb{R}^2))$, and it has two components, singular and regular. The

singular part amounts to a collection of (*shrinking in time*) *point masses concentrated on the points* $x = x_i$ *of the precise form*

$$u_{sing} = \sum_i (M_i - 4\pi t)_+ \delta(x - x_i). \tag{63}$$

The regular part can be described as follows:

(i) *When restricted to the perforated domain* $Q_* = \left(\mathbb{R}^2 - \bigcup_i \{x_i\}\right) \times (0, T)$, *u is a smooth solution of the equation, it takes the initial data* $f(x)$ *for a.e.* $x \neq x_i$, *and vanishes at* $t = T$.

(ii) *At every time* $t \in (0, T)$ *the total mass of the regular part is the result of adding to* M_0 *the inflow coming from the point masses and subtracting the outflow at infinity.*

(iii) *Before each point mass disappears, we get a singular behaviour near the mass location as in the radial case, while later on the solution is regular around that point.*

For complete details on this issue we refer to [45].

The theory of measure-valued solutions of diffusion equations is still in its beginning. A large number of open problems are posed for subcritical fast diffusion.

References

[1] Andreu-Vaillo, F., Caselles, V., Mazón, J. M., *Parabolic quasilinear equations minimizing linear growth functionals*. Progr. Math. 223, Birkhäuser, Basel 2004.

[2] Angenent, S. B., Aronson, D. G., Betelu, S. I., Lowengrub, J. S., Focusing of an elongated hole in porous medium flow. *Phys. D* **151** (2–4) (2001), 228–252.

[3] Aronson, D. G., Graveleau, J. A., Self-similar solution to the focusing problem for the porous medium equation. *European J. Appl. Math.* **4** (1) (1993), 65–81.

[4] Barenblatt, G. I., *Scaling, Self-Similarity, and Intermediate Asymptotics*. Cambridge University Press, Cambridge 1996; updated version of *Similarity, Self-Similarity, and Intermediate Asymptotics*, Consultants Bureau, New York 1979.

[5] Barenblatt, G. I., *Scaling*. Cambridge Texts in Appl. Math., Cambridge University Press, Cambridge, 2003.

[6] Bénilan, P., Equations d'évolution dans un espace de Banach quelconque et applications. Ph. D. Thesis, Université Orsay, 1972.

[7] Bénilan, P., Carrillo, J., Wittbold, P., Renormalized entropy solutions of scalar conservation laws. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **29** (2) (2000), 313–327.

[8] Brändle, C., Vázquez, J. L., Viscosity solutions for quasilinear degenerate parabolic equations of porous medium type. *Indiana Univ. Math. J.* **54** (3) (2005), 817–860.

[9] Brändle, C., Quirós, F., Vázquez, J. L., Asymptotic behaviour of the porous media equation in domains with holes. *Interfaces Free Bound.*, to appear.

[10] Brezis, H., Friedman, A., Nonlinear parabolic equations involving measures as initial conditions. *J. Math. Pures Appl.* **62** (1983), 73–97.

[11] Caffarelli, L. A., Cabré, X., *Fully nonlinear elliptic equations*. Amer. Math. Soc. Colloq. Publ. 43, Amer. Math. Soc., Providence, RI, 1995.

[12] Caffarelli, L. A., Friedman, A., Regularity of the free boundary of a gas flow in an n-dimensional porous medium. *Indiana Univ. Math. J.* **29** (1980), 361–391.

[13] Caffarelli, L. A., Salsa, S., *A geometric approach to free boundary problems*. Grad. Stud. Math. 68, Amer. Math. Soc., Providence, R.I., 2005.

[14] Caffarelli, L. A., Vázquez, J. L., Viscosity solutions for the porous medium equation. In *Differential equations: La Pietra 1996* (ed. by M. Giaquinta, J. Shatah and S. R. S. Varadhan), Proc. Sympos. Pure Math. 65, Amer. Math. Soc., Providence, RI, 1999, 13–26.

[15] Caffarelli, L. A., Vázquez, J. L., Wolanski, N. I., Lipschitz continuity of solutions and interfaces of the N-dimensional porous medium equation. *Indiana Univ. Math. J.* **36** (1987), 373–401.

[16] Carrillo, J. A., McCann, R., Villani, C., Contractions in the 2-Wasserstein length space and thermalization of granular media. *Arch. Rational Mech. Anal.* **179** (2006), 217–264.

[17] Carrillo, J. A., Toscani, G., Asymptotic L^1-decay of solutions of the porous medium equation to self-similarity. *Indiana Univ. Math. J.* **49** (2000), 113–141.

[18] Chang, S. Y. A., Yang, P. C., Nonlinear Partial Differential Equations in Conformal Geometry. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. I, Higher Ed. Press, Beijing 2002, 189–207.

[19] Crandall, M. G., Evans, L. C., Lions, P. L., Some properties of viscosity solutions of Hamilton-Jacobi equations. *Trans. Amer. Math. Soc.* **282** (1984), 487–502.

[20] Crandall, M. G., Liggett, T. M., Generation of semi-groups of nonlinear transformations on general Banach spaces. *Amer. J. Math.* **93** (1971) 265–298.

[21] del Pino, M., M. Sáez, M., On the Extinction Profile for Solutions of $u_t = \Delta u^{(N-2)/(N+2)}$. *Indiana Univ. Math. J.* **50** (2) (2001), 612–628.

[22] Fourier, J., *Théorie analytique de la Chaleur*. Reprint of the 1822 original, Éditions Jacques Gabay, Paris 1988; English version: *The Analytical Theory of Heat*. Dover, New York 1955.

[23] Friedman, A., *Partial Differential Equations of Parabolic Type*. Prentice-Hall, Englewood Cliffs, NJ, 1964.

[24] Friedman, A., *Variational Principles and Free Boundaries*. Wiley and Sons, New York 1982.

[25] Friedman, A., Kamin, S., The asymptotic behavior of gas in an n-dimensional porous medium. *Trans. Amer. Math. Soc.* **262** (1980), 551–563.

[26] Galaktionov, V. A., Peletier, L. A., Asymptotic behaviour near finite time extinction for the fast diffusion equation. *Arch. Rational Mech. Anal.* **139** (1) (1997), 83–98.

[27] Galaktionov, V. A., Peletier, L. A., Vázquez, J. L., Asymptotics of the fast-diffusion equation with critical exponent. *SIAM J. Math. Anal.* **31** (5) (2000), 1157–1174.

[28] Galaktionov, V. A., Vázquez, J. L., *A Stability Technique for Evolution Partial Differential Equations. A Dynamical Systems Approach*. Progr. Nonlinear Differential Equations Appl. 56, Birkhäuser, Boston, MA, 2004.

[29] Hamilton, R. S., The Ricci flow on surfaces. *Contemp. Math.* **71** (1988), 237–262.

[30] Gilding, B. H., Goncerzewicz, J., Large-time bahaviour of solutions of the exterior-domain Cauchy-Dirichlet problem for the porous media equation with homogeneous boundary data. *Monatsh. Math.* **150** (2007), 11–39.

[31] King, J. R., Self-similar behaviour for the equation of fast nonlinear diffusion. *Phil. Trans. Roy. Soc. London Ser. A* **343** (1993), 337–375.

[32] Koch, H., Non-Euclidean singular integrals and the porous medium equation. University of Heidelberg, Habilitation Thesis, 1999; http://www.iwr.uniheidelberg.de/groups/amj/koch.html.

[33] Ladyzhenskaya, O. A., Solonnikov, V. A., Ural'tseva, N. N., *Linear and Quasilinear Equations of Parabolic Type*. Transl. Math. Monographs 23, Amer. Math. Soc, Providence, RI, 1968.

[34] Lee, K.-A., Vázquez, J. L., Geometrical properties of solutions of the Porous Medium Equation for large times. *Indiana Univ. Math. J.* **52** (4) (2003), 991–1016.

[35] Lions, P. L., Toscani, G., Diffusive limits for finite velocities Boltzmann kinetic models. *Rev. Mat. Iberoamericana* **13** (1997), 473–513.

[36] Oleinik, O. A., Kalashnikov, A. S., Chzou, Y.-I., The Cauchy problem and boundary problems for equations of the type of unsteady filtration. *Izv. Akad. Nauk SSR Ser. Math.* **22** (1958), 667–704.

[37] Otto, F., The geometry of dissipative evolution equations: the porous medium equation. *Comm. Partial Differential Equations* **26** (1–2) (2001), 101–174.

[38] Peletier, M. A., Zhang, H., Self-similar solutions of a fast diffusion equation that do not conserve mass. *Differential Integral Equations* **8** (1995) 2045–2064.

[39] Pierre, M., Nonlinear fast diffusion with measures as data. In *Nonlinear parabolic equations: qualitative properties of solutions* (Rome, 1985), Pitman Res. Notes Math. Ser. 149, Longman Sci. Tech., Harlow 1987, 179–188.

[40] Vázquez, J. L., Asymptotic behaviour and propagation properties of the one-dimensional flow of gas in a porous medium. *Trans. Amer. Math. Soc.* **277** (2) (1983), 507–527.

[41] Vázquez, J. L., Asymptotic behaviour for the Porous Medium Equation posed in the whole space. *J. Evol. Equ.* **3** (2003), 67–118.

[42] Vázquez, J. L., The Porous Medium Equation. New contractivity results. In *Elliptic and parabolic problems*, Progr. Nonlinear Differential Equations Appl. 63, Birkhäuser, Basel 2005, 433–451.

[43] Vázquez, J. L., *Smoothing and Decay Estimates for Nonlinear Diffusion Equations*. Oxford Lecture Ser. Math. Appl. 33, Oxford University Press, Oxford 2006.

[44] Vázquez, J. L., *The Porous Medium Equation. Mathematical theory*. Oxford Math. Monogr., Oxford University Press, Oxford 2007.

[45] Vázquez, J. L., Evolution of point masses by planar logarithmic diffusion. Finite-time blow-down. *Discrete Contin. Dyn. Syst.*, to appear.

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain
E-mail: juanluis.vazquez@uam.es

Applications of equivariant cohomology

Michèle Vergne

Abstract. We will discuss the equivariant cohomology of a manifold endowed with the action of a Lie group. Localization formulae for equivariant integrals are explained by a vanishing theorem for equivariant cohomology with generalized coefficients. We then give applications to integration of characteristic classes on symplectic quotients and to indices of transversally elliptic operators. In particular, we state a conjecture for the index of a transversally elliptic operator linked to a Hamiltonian action. In the last part, we describe algorithms for numerical computations of values of multivariate spline functions and of vector-partition functions of classical root systems.

Mathematics Subject Classification (2000). Primary 19; Secondary 52.

Keywords. Equivariant cohomology, Hamiltonian action, symplectic reduction, localization formula, polytope, index, transversally elliptic operator, spline, Euler–Maclaurin formula.

1. Introduction

The aim of this article is to show how theorems of localization in equivariant cohomology not only provide beautiful mathematical formulae, but also stimulated progress in algorithmic computations. I will focus on my favorite themes: quantization of symplectic manifolds and algorithms for polytopes, and neglect many other applications. Many mathematicians have shared their ideas with me, notably Welleda Baldoni, Nicole Berline, Michel Brion, Michel Duflo, Shrawan Kumar, Paul-Emile Paradan and Andras Szenes. I will therefore often employ a collective "we", instead of anxiously weighing my own contribution.

I will describe here the theory of equivariant cohomology with generalized coefficients of a manifold M on which a Lie group K acts. The integral of such a cohomology class is a generalized function $I(\phi)$ on $\mathfrak{k}$, with ϕ in $\mathfrak{k}$, the Lie algebra of K. We wish to solve two problems. The first is to give a "localization formula" for $I(\phi)$ as a "short" expression. The second is: given such a short formula for $I(\phi)$, compute the value $\hat{I}(\xi)$ of the Fourier transform of I at a point $\xi \in \mathfrak{k}^*$ in terms of the initial geometric data. Let me give the motivation for such questions.

By integrating de Rham cohomology classes on a manifold, one obtains certain numerical quantities. For example, the symplectic volume vol_M of a compact symplectic manifold M is the integral of the Liouville form, and the Atiyah–Singer cohomological formula for the index of an elliptic operator D on M is an integral of a cohomology

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

class with compact support on T^*M. In the interplay between toric varieties and polytopes, these numerical quantities correspond respectively to the volume of a polytope and to the number of integral points inside a rational polytope. Moreover, the volume is the classical limit of the discrete version, the number of integral points in dilated polytopes.

When the manifold is provided with the action of a compact Lie group K, similar objects are described by integrals of equivariant cohomology classes. The equivariant volume $\mathrm{vol}_M(\phi)$ of a compact Hamiltonian manifold M is a C^∞ function of $\phi \in \mathfrak{k}$, obtained by integrating a particular equivariant cohomology class on M. More generally, if M is a non-compact Hamiltonian manifold with proper moment map, and additional convergence conditions, its equivariant volume $\mathrm{vol}_M(\phi)$ is a generalized function on $\mathfrak{k}$. As shown by Duistermaat–Heckman, the value at $\xi \in \mathfrak{k}^*$ of the inverse Fourier transform of $\mathrm{vol}_M(\phi)$ is the symplectic volume of the Marsden–Weinstein reduction of M at ξ. If a K-invariant operator D is elliptic in the directions transverse to the orbits of K, its index $\mathrm{Index}(D)$ is a generalized function on K, that is, a series of characters of K. It can be described in terms of integrals of equivariant cohomology classes on T^*M. The discrete inversion problem is to determine each Fourier coefficient of $\mathrm{Index}(D)$. When D is an operator linked to the symplectic structure, we think of $\mathrm{Index}(D)$ as the quantum version of the equivariant volume. The Guillemin–Sternberg conjecture, now established by Meinrenken–Sjamaar for any compact Hamiltonian manifold, is an example where such an inversion problem has a beautiful answer in geometric terms.

In the case of a manifold with a circular symmetry, we proved a localization formula for integrals of equivariant cohomology classes as a sum of local contributions from the fixed points. This formula is similar to the Atiyah–Bott Lefschetz fixed point formula for the equivariant index of an elliptic operator on M. A drawback of such formulae is that each individual term has poles, and the Fourier transform of an individual term is meaningless. We will describe here a more general principle of localization for integrals of equivariant cohomology classes. Let κ be a K-invariant vector field tangent to the orbits of K. Witten showed that equivariant integrals on M can be computed in terms of local data near the set C of zeroes of κ. Furthermore, for each connected component C_F of C, the local contribution of C_F is a generalized function on $\mathfrak{k}$. Witten's localization theorem can be best understood through Paradan's identity: $1 = 0$ on $M - C$, in equivariant cohomology with generalized coefficients. Basic definitions and Paradan's identity are explained in Section 3.

The identity $1 = 0$ on $M - C$ has many independent applications that we describe in Section 4. When M is a Hamiltonian manifold with moment map μ, the set of zeroes of the Kirwan vector field is the set of critical points of the function $\|\mu\|^2$. According to Witten's theorem, integrals on reduced spaces of M can be related to equivariant integrals on M. Using a similar localization argument for transversally elliptic operators, Paradan was able to extend the proof of the Guillemin–Sternberg conjecture to some non-compact Hamiltonian spaces linked to representation theory of real semi-simple Lie groups via Kirillov's orbit method. We will state a generalization

of the Guillemin–Sternberg conjecture for a transversally elliptic operator canonically attached to a Hamiltonian action in Section 4.

From the localization formulae, one is led to study generalized functions which are regular outside a union of hyperplanes. This will be the topic of Section 5. In particular, we will relate the cohomology ring of toric manifolds to cycles in the complement of an arrangement of hyperplanes.

As there are some relations between Hamiltonian geometry and convex polytopes, these localization theorems have an analogue for polytopes. Such an analogue is the local Euler–Maclaurin formula for polytopes, which was conjectured by Barvinok–Pommersheim. We will indicate in Section 6 how some theoretical results on intersection rings can be turned into effective tools for numerical computations. We implemented algorithms for various problems such as computing the value of the convolution of a large number of Heaviside distributions, the number of integral points in network polytopes and Kostant partitions functions, with applications to the tensor multiplicities formulae. This last section can be read independently. Indeed, these applications to polytopes have elementary proofs, but it was through interaction with Hamiltonian geometry that some of these tools were discovered.

For lack of space, I was only able to include central references to the topics discussed in this text. For more bibliographical comments, references and motivations, one might consult [13], [25], [27], [49] and my home page (notably, the text called "Exégèse") at math.polytechnique.fr/cmat/vergne/. The texts [50] and [48] are introductory and hopefully reader-friendly.

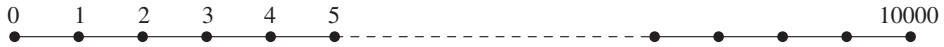
2. Simple examples

In this section, I will give simple examples of sums which can be represented by short formulae, and a simple example of the inverse problem we have in mind. I will also give a sketch of the proof of the stationary phase formula as similar stationary phase arguments will be our fundamental tools.

2.1. Geometric series. Some formulae in mathematics condense a large amount of information in short expressions. The most striking formula perhaps is the one that sums a very long geometric series:

$$\sum_{i=0}^{10000} q^i = \frac{1}{1-q} + \frac{q^{10000}}{1-q^{-1}}.$$

For a straightforward calculation of the left hand side for a given value q, one needs to know the value of the function q^i at all the 10001 integral points of the interval $[0, 10000]$, while for the right hand side one needs only the value of this function at the end points $0, 10000$. Note that each term of the right hand side has a pole at $q = 1$.



The short formula (here A, B, i are integers)

$$\sum_{i=A}^{B} q^i = \frac{q^A}{1-q} + \frac{q^B}{1-q^{-1}} = -\frac{q^{A-1}}{1-q^{-1}} - \frac{q^{B+1}}{1-q} \tag{1}$$

is related to the following equalities of characteristic functions:

$$\begin{aligned}\chi([A,B]) &= \chi([A,\infty[) + \chi(]-\infty,B]) - \chi(\mathbb{R}) \\ &= \chi(\mathbb{R}) - \chi(]-\infty,A[) - \chi(]B,\infty[).\end{aligned}$$

We draw the picture of the last equality.

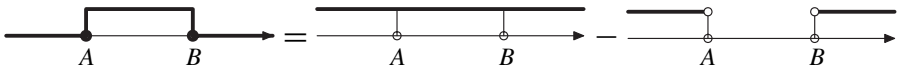


Figure 1. Decomposition of an interval.

Then to sum q^i from A to B, we first sum q^i from $-\infty$ to ∞ and subtract the two sums over the integers strictly less than A and over the integers strictly greater than B. Thus, if

$$S_0 := \sum_{i=-\infty}^{\infty} q^i, \quad S_A := \sum_{-\infty}^{A-1} q^i, \quad S_B := \sum_{B+1}^{\infty} q^i,$$

we obtain formally, or, setting $q = e^{i\phi}$, in the sense of generalized functions on the unit circle,

$$S = S_0 - S_A - S_B. \tag{2}$$

For a value $q \neq 1$, the first sum S_0 is 0 as follows from $(1-q)S_0 = 0$, while S_A, S_B are just geometric progressions and we come back to the short formula (1).

The reader may recognize in Formula (1) a very simple instance of the Atiyah–Bott Lefschetz fixed point formula on the Riemann sphere. Formula (2) illustrates Paradan's localization of elliptic operators, which we describe in Section 4.2. Indeed, Formula (2) is an example of the decomposition of the equivariant index of an elliptic operator on the Riemann sphere in a sum of indices of three transversally elliptic operators (see Example 13).

2.2. Inverse problem. The inverse problem may be described as follows: given a short expression for a sum, compute an individual term of the sum.

Here is an example. Consider the following product of geometric series $G := \left(\sum_{i=0}^{\infty} q_1^i\right)^3 \left(\sum_{j=0}^{\infty} q_2^j\right)^3 \left(\sum_{k=0}^{\infty} q_1^k q_2^k\right)^3$ given by the short expression:

$$S(q_1,q_2) := \frac{1}{(1-q_1)^3}\frac{1}{(1-q_2)^3}\frac{1}{(1-q_1q_2)^3}.$$

Let us compute the coefficient $c(a,b)$ of $q_1^a q_2^b$ in G. If $a \geq b$, an iterated application of the residue theorem in one variable leads to

$$c(a,b) = \mathrm{res}_{x_2=0}\left(\mathrm{res}_{x_1=0}\,\frac{e^{ax_1}e^{bx_2}\,dx_1\,dx_2}{(1-e^{-x_1})^3(1-e^{-x_2})^3(1-e^{-(x_1+x_2)})^3}\right).$$

If we set

$$g(a,b) = \frac{(b+1)(b+2)(b+3)(b+4)(b+5)(7a^2-7ab+2b^2+21a-9b+14)}{14\cdot 5!},$$

we obtain the following equalities.

$$\text{If } a \geq b, \text{ then } c(a,b) = g(a,b). \tag{3}$$

$$\text{If } a \leq b, \text{ then } c(a,b) = g(b,a). \tag{4}$$

We will discuss in Section 5.1 a residue theorem (Theorem 18) in several variables, which gives an algorithmic solution to this type of inversion problem.

The Guillemin–Sternberg conjecture (see Section 4.3) gives a geometric interpretation of the Fourier coefficients of series for similar inversion problems.

2.3. Stationary phase. Let M be a compact manifold of dimension n, f a smooth function on M and dm a smooth density. Consider the function

$$F(t) := \int_M e^{itf(m)}dm.$$

The dominant contribution to the value of this integral as t tends to infinity arises from the neighborhood of the set C of critical points of f. We indicate a proof of this fact, as similar arguments will be employed later on. Consider the image of M by the map $x = f(m)$ and the push-forward of the density dm. Then $F(t) = \int_{\mathbb{R}} e^{itx} f_*(dm)$. Choose a smooth function χ on M, equal to 1 in a neighborhood of the set C and supported near C. Then $F(t) = F_C(t) + R(t)$, where

$$F_C(t) := \int_{\mathbb{R}} e^{itx} f_*(\chi\, dm), \quad R(t) = \int_{\mathbb{R}} e^{itx} f_*((1-\chi)dm).$$

$R(t)$ is the Fourier transform of a smooth compactly supported function, and thus decreases rapidly at infinity. It is not hard to show that, if f has a finite number of non-degenerate critical points, then

$$F(t) \sim F_C(t) \sim \sum_{p\in C} e^{itf(p)} \sum_{k\geq 0}^{\infty} a_{p,k} t^{-\frac{n}{2}+k},$$

where the constants $a_{p,k}$ can be computed in terms of f and dm near $p \in C$. We can say that asymptotically, the integral "localizes" at a finite number of points p.

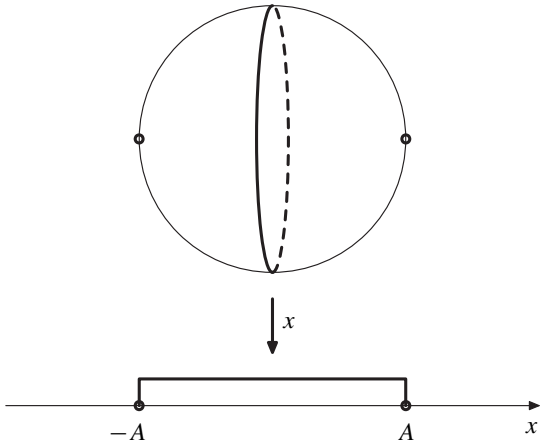


Figure 2. Projecting the sphere $x^2 + y^2 + z^2 = A^2$.

Example 1. Let M be the sphere $\{x^2 + y^2 + z^2 = A^2\}$ of radius A endowed with the Liouville volume form $dm := \frac{dy \wedge dz}{2\pi x}$. Let our function f be the projection onto the x-axis: $f = x$. We immediately see that $f_*(dm)$ is the characteristic function of the interval $[-A, A]$. Thus we obtain the formula

$$F(t) = \int_{-A}^{A} e^{itx} dx = \frac{e^{-iAt}}{-it} + \frac{e^{iAt}}{it}.$$

Observe that here $F(t)$ is not just asymptotically, but exactly equal to the local expression. The reason is that in this example the function f is the Hamiltonian of an action of the circle group $S^1 := \{e^{i\phi}\}$ on a compact symplectic manifold, and dm is the Liouville measure. In such a case, the Duistermaat–Heckman exact stationary phase formula [26] implies that $f_*(dm)$ is locally polynomial on $f(M)$ and that

$$F(t) = \sum_{p \in C} e^{itf(p)} a_{p,0} t^{-\frac{n}{2}}. \tag{5}$$

We will interpret the Duistermaat–Heckman formula as an example of the abelian localization formula (Theorem 7) of integrals of equivariant forms in Section 3.5.

3. Equivariant differential forms

Our motivation to study equivariant differential forms came from representation theory.

Let M be a manifold with an action of the circle group S^1. The Atiyah–Bott fixed point formula [3] describes the equivariant index of an elliptic operator on M in terms

of local data near the fixed points of the action. One of the applications of the formula was a geometric interpretation of the Weyl formula for the characters of irreducible representations of compact Lie groups.

The character formula has continuous analogues: the formulae for the Fourier transforms of coadjoint orbits, which are linked to representation theory via Kirillov's orbit method. For compact groups, this is the Harish-Chandra formula; for non-compact semi-simple groups, Rossmann gave a fixed point formula in the case of discrete series characters.

In joint work with Nicole Berline, I found a geometric interpretation of Rossmann's formula using equivariant forms [14]. The cohomological tool behind our computation was a deformation of the de Rham complex with the use of vector fields. A similar formalism was described by Witten [51] with different motivation. There were earlier results which condensed certain integrals on M in short formulae localized near "fixed points", such as Bott's residue formulae [19], its generalization by Baum–Cheeger [11] and the Duistermaat–Heckman exact stationary phase formula [26]. As explained by Atiyah and Bott [4], our result was related to localization in topological equivariant cohomology. However, this revival of "de Rham" theory of equivariant cohomology in terms of differential forms turned out to be very fruitful, especially in applications to non-compact spaces and stationary phase type arguments.

3.1. Equivariant de Rham complex. Notation. I keep the notation N for not necessarily compact manifolds, and M for compact manifolds. Similarly a compact group will be denoted by the letter K, while G will be an arbitrary real Lie group. The letters T, H will be reserved for tori, which are compact connected abelian Lie groups, and therefore are just products of circle groups $\{e^{i\theta_a}\}$. In this case, I take as basis of the Lie algebra $\mathfrak{t}$, elements J_a such that $\exp(\theta_a J_a) := e^{i\theta_a}$ ($\theta_a \in \mathbb{R}$). The gothic german letters $\mathfrak{g}$, $\mathfrak{k}$, $\mathfrak{t}$, $\mathfrak{h}$ denote the corresponding Lie algebras, $\mathfrak{g}^*$, $\mathfrak{k}^*$, $\mathfrak{t}^*$, $\mathfrak{h}^*$ the dual vector spaces, J^a the dual basis to a basis J_a. If $s \in G$, I denote by N_s the set of fixed points of the action of s on the G-manifold N. The letter ϕ denotes an element of $\mathfrak{g}$. If $\mathfrak{g} = \mathbb{R}J$ is the Lie algebra of S^1, I identify $\mathfrak{g}$ and $\mathbb{R}$. I denote by $S(\mathfrak{g}^*)$ the algebra of polynomial functions on $\mathfrak{g}$, by $C^\infty(\mathfrak{g})$ the space of C^∞ functions on $\mathfrak{g}$ and by $C^{-\infty}(\mathfrak{g})$ the space of generalized functions on $\mathfrak{g}$. An element $v \in C^{-\infty}(\mathfrak{g})$ is denoted by $v(\phi)$ although the value at $\phi \in \mathfrak{g}$ of v may not be defined. By definition, it is always defined in the distributional sense: if $F(\phi)$ is a C^∞ function on $\mathfrak{g}$ with compact support (a test function), then $\langle v, Fd\phi\rangle$, denoted by $\int_{\mathfrak{g}} v(\phi)F(\phi)d\phi$, is well defined.

Let us first define the equivariant cohomology algebra with C^∞ coefficients of a G-manifold N.

Let G be a Lie group acting on a manifold N. For $\phi \in \mathfrak{g}$, we denote by $V\phi$ the vector field on N generated by the infinitesimal action of $-\phi$: for $x \in N$, $V_x\phi := \frac{d}{d\varepsilon}\exp(-\varepsilon\phi)\cdot x|_{\varepsilon=0}$. If N is provided with an action of S^1, we simply denote by J the vector field VJ. Let $\mathcal{A}(N)$ be the algebra of differential forms on N with complex coefficients, and denote by d the exterior derivative. If V is a vector field, let $\iota(V)$

be the contraction by V. If $\nu := \sum_{i=0}^{\dim N} \nu_{[i]}$ is a differential form on an oriented manifold N, then the integral of ν over N is by definition the integral of the top degree term of ν: $\int_N \nu := \int_N \nu_{[\dim N]}$, provided that this last integral is convergent.

A smooth map $\alpha : \mathfrak{g} \to \mathcal{A}(N)$ is called an *equivariant form*, if α commutes with the action of G on both sides. The equivariant de Rham operator D ([14], [51]) may be viewed as a deformation of the de Rham operator d with the help of the vector field $V\phi$. It is defined on equivariant forms by the formula

$$(D(\alpha))(\phi) := d(\alpha(\phi)) - \iota(V\phi)\alpha(\phi).$$

Then $D^2 = 0$. An equivariant form α is equivariantly closed if $D\alpha = 0$. The *cohomology space*, denoted by $\mathcal{H}^\infty(\mathfrak{g}, N)$, is, as usual, the kernel of D modulo its image. This is an algebra, $\mathbb{Z}/2\mathbb{Z}$-graded in even and odd classes. If $G := \{1\}$, this is the usual cohomology algebra $\mathcal{H}(N)$.

The integral of an equivariant differential form may be defined as a generalized function. Indeed, let $F(\phi)$ be a test function on $\mathfrak{g}$; then $\int_{\mathfrak{g}} \alpha(\phi)F(\phi)d\phi$ is a differential form on N. If this differential form is integrable on N for all test functions F, then $\int_N \alpha$ is defined by

$$\left\langle \int_N \alpha,\, F d\phi \right\rangle := \int_N \int_{\mathfrak{g}} \alpha(\phi)F(\phi)d\phi.$$

Of course if N is compact oriented, $\int_N \alpha(\phi)$ is a C^∞ function.

3.2. Hamiltonian spaces. Examples of equivariantly closed forms arise in Hamiltonian geometry.

Let N be a symplectic manifold with symplectic form Ω. We say that the action of G on N is Hamiltonian with moment map $\mu : N \to \mathfrak{g}^*$ if, for every $\phi \in \mathfrak{g}$, $d(\langle\phi, \mu\rangle) = \iota(V\phi) \cdot \Omega$. Thus the zeroes of the vector field $V\phi$ (that is, the *fixed points* of the one parameter group $\exp(t\phi)$) are the critical points of $\langle\phi, \mu\rangle$.

The equivariant symplectic form $\Omega(\phi) := \langle\phi, \mu\rangle + \Omega$ is a closed equivariant form. Indeed,

$$(d - \iota(V\phi))(\langle\phi, \mu\rangle + \Omega) = d(\langle\phi, \mu\rangle) - \iota(V\phi) \cdot \Omega + d(\Omega)$$

and this is equal to 0 as both equations

$$d\Omega = 0, \quad d(\langle\phi, \mu\rangle) = \iota(V\phi) \cdot \Omega$$

hold.

The two basic examples of Hamiltonian spaces with an Hamiltonian action of S^1 are:

(1) $\mathbb{R}^2$ if the action of S^1 has a fixed point.

(2) The cotangent bundle T^*S^1 if the action of S^1 is free.

(1) Let $N := \mathbb{R}^2$ with coordinates $[x, y]$. The circle group S^1 acts by rotations with isolated fixed point $[0, 0]$. The symplectic form is $\Omega := dx \wedge dy$. The function $\frac{x^2+y^2}{2}$ is the Hamiltonian function for the vector field $J := y\partial_x - x\partial_y$. Thus the equivariant symplectic form is

$$\Omega(\phi) = \phi\left(\frac{x^2+y^2}{2}\right) + dx \wedge dy.$$

(2) Let $N := T^*S^1 = S^1 \times \mathbb{R}$. The circle group S^1 acts freely by rotations on S^1. If $[e^{i\theta}, t]$ is a point of T^*S^1 with $t \in \mathbb{R}$, the symplectic form is $\Omega := dt \wedge d\theta$. The function t is the Hamiltonian function for the vector field $J := -\partial_\theta$. Thus the equivariant symplectic form is

$$\Omega(\phi) = \phi\, t + dt \wedge d\theta.$$

A particularly important closed equivariant form is $e^{i\Omega(\phi)}$. If $\dim N := 2\ell$, then

$$e^{i\Omega(\phi)} = e^{i\langle\phi,\mu\rangle}\left(1 + i\Omega + \frac{(i\Omega)^2}{2!} + \cdots + \frac{(i\Omega)^\ell}{\ell!}\right).$$

3.3. Equivariant volumes. Let M be a compact K-Hamiltonian manifold of dimension 2ℓ. By definition, the equivariant symplectic volume of M is the function of $\phi \in \mathfrak{k}$ given by

$$\mathrm{vol}_M(\phi) := \frac{1}{(2i\pi)^\ell}\int_M e^{i\Omega(\phi)} = \int_M e^{i\langle\phi,\mu(m)\rangle}\frac{\Omega^\ell}{\ell!(2\pi)^\ell}.$$

Note that $\mathrm{vol}_M(0)$ is the symplectic volume of M. The last integral, according to the Duistermaat–Heckman-formula [26], localizes as a sum of integrals on the connected components of the set of zeroes of $V\phi$. If this set of zeroes is finite,

$$\mathrm{vol}_M(\phi) = \sum_{p\in \text{ zeroes of } V\phi} \frac{e^{i\langle\phi,\mu(p)\rangle}}{i^\ell\sqrt{\det_{T_pM} L_p(\phi)}}, \tag{6}$$

where $L_p(\phi)$ is the endomorphism of T_pM determined by the infinitesimal action of ϕ at p. As K is compact, there is a well-defined polynomial square root of the function $\phi \mapsto \det_{T_pM} L_p(\phi)$, the sign being determined by the orientation.

Example 2. Consider, as in Example 1, Section 2.3, the sphere M with S^1-action given by rotation around the x-axis and $\Omega := \frac{dy\wedge dz}{x}$. Then $f := x$ is the Hamiltonian function of the vector field $J := (y\partial_z - z\partial_y)$. The equivariant volume is the C^∞ function

$$\mathrm{vol}_M(\phi) = \int_M e^{i\phi x}dm = \frac{e^{-iA\phi}}{-i\phi} + \frac{e^{iA\phi}}{i\phi}.$$

Let us point out some examples of non-compact manifolds N where the equivariant symplectic volume exists in the sense of generalized functions. We will use the following generalized functions:

$$Y^+(\phi) := \int_0^\infty e^{i\phi t}dt, \quad Y^-(\phi) := \int_{-\infty}^0 e^{i\phi t}dt, \quad \delta_0(\phi) := \int_{-\infty}^\infty e^{i\phi t}dt.$$

Note that the generalized function $Y^+(\phi)$ is the boundary value of the holomorphic function $\frac{1}{-i\phi}$ defined on the upper-half plane, so that it satisfies the relation $(-i\phi)Y^+(\phi) = 1$. The generalized function $\delta_0(\phi)$ satisfies the relation $\phi\,\delta_0(\phi) = 0$.

Return to our two basic examples $\mathbb{R}^2$ and T^*S^1 with action of S^1.

(1) $N := \mathbb{R}^2$. We have

$$\mathrm{vol}_N(\phi) = \frac{1}{2\pi}\int_{\mathbb{R}^2} e^{i\phi\frac{(x^2+y^2)}{2}}dxdy = \int_0^\infty e^{i\phi r}dr = Y^+(\phi). \tag{7}$$

When $\phi \neq 0$, we have $\mathrm{vol}_N(\phi) = \frac{1}{-i\phi}$. This coincides with what would be the Duistermaat–Heckman formula in the non-compact case: there is just one fixed point $[0, 0]$ for the action.

(2) $N := T^*S^1$. We have

$$\mathrm{vol}_N(\phi) = \frac{1}{2\pi}\int_{\mathbb{R}\times S^1} e^{i\phi t}dtd\theta = \int_{\mathbb{R}} e^{i\phi t}dt = \delta_0(\phi).$$

Thus $\mathrm{vol}_N(\phi)$ is always 0 when $\phi \neq 0$. This is consistent with the fixed point philosophy: the action of S^1 on T^*S^1 is free, thus the set of zeroes of $V\phi$ is empty when $\phi \neq 0$.

The next example illustrates our original motivation to introduce the equivariant differential complex.

Coadjoint orbits. Let G be a real Lie group. Recall [30] that when $N := G\lambda$ is the orbit of an element $\lambda \in \mathfrak{g}^*$ by the coadjoint representation, then N has a G-Hamiltonian structure, such that the moment map is the inclusion $N \to \mathfrak{g}^*$. The equivariant volume $\mathrm{vol}_N(\phi)$ is defined as a generalized function on $\mathfrak{g}$, if the orbit $G\lambda$ is tempered. This is just the Fourier transform of the G-invariant measure supported on $G\lambda \subset \mathfrak{g}^*$.

When N is a coadjoint orbit of a compact Lie group K, Harish-Chandra gave a fixed point formula for $\mathrm{vol}_N(\phi)$. Now this is seen as a special case of the Duistermaat–Heckman formula (6). Rossmann [41] and Libine [32] extended the Harish-Chandra formula to the case of closed coadjoint orbits of reductive non-compact Lie groups, involving delicate constants at fixed points at "infinity" defined combinatorially by Harish-Chandra and Hirai and topologically by Kashiwara.

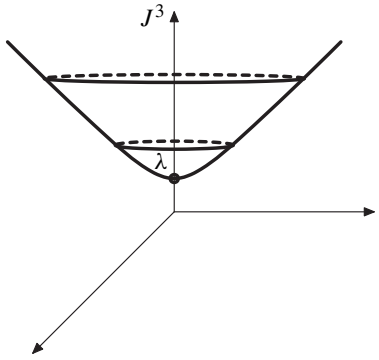
Here is an example. Consider the group $\mathrm{SL}(2, \mathbb{R})$ with Lie algebra $\mathfrak{g}$ with basis

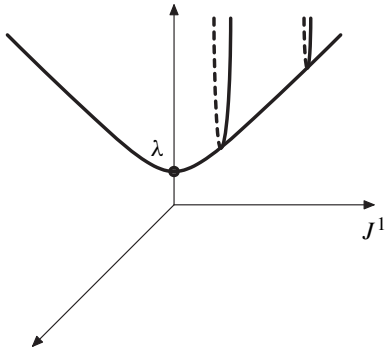
$$J_1 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad J_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad J_3 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The one-parameter group generated by J_3 is compact, while those generated by J_1 and J_2 are non-compact. Let $\lambda > 0$. The manifold

$$N := \{\xi_1 J^1 + \xi_2 J^2 + \xi_3 J^3; \xi_3^2 - \xi_1^2 - \xi_2^2 = \lambda^2, \xi_3 > 0\}$$

is a coadjoint orbit. Then the generalized function $\mathrm{vol}_N(\phi_1 J_1 + \phi_2 J_2 + \phi_3 J_3)$ is given by an invariant locally L_1-function, analytic outside $\phi_1^2 + \phi_2^2 - \phi_3^3 = 0$.





$$\mathrm{vol}_N(\phi_3 J_3) = -\frac{e^{i\lambda\phi_3}}{2i\phi_3}, \qquad \mathrm{vol}_N(\phi_1 J_1) = \frac{e^{-|\lambda\phi_1|}}{2|\phi_1|}.$$

The formula for the generator J_3 of a compact group action is in agreement with the "fixed point formula philosophy". The formula for J_1 is difficult to explain within a general framework. Indeed, the non-compact group $\exp(\phi_1 J_1)$ acts freely on N; however, the value of the function $\mathrm{vol}_N(\phi_1 J_1)$ is non-zero even though there are no fixed points on N. In [32], N is embedded in the cotangent bundle of the Riemann sphere $M := P_1(\mathbb{C})$, and a subtle argument of deformation to fixed points of J_1 in M "explains" the formula for $\mathrm{vol}_N(\phi_1 J_1)$.

3.4. Equivariant cohomology groups. After having defined $\mathcal{H}^\infty(\mathfrak{g}, N)$, I will move on to the definition of two other equivariant cohomology groups.

Cartan's complex. Here we consider, for a K-manifold N, the space $\mathcal{A}^{\mathrm{pol}}(\mathfrak{k}, N) := (S(\mathfrak{k}^*) \otimes \mathcal{A}(N))^K$ of equivariant forms $\alpha(\phi)$ depending polynomially on ϕ. The corresponding cohomology space $\mathcal{H}^{\mathrm{pol}}(\mathfrak{k}, N)$ is a $\mathbb{Z}$-graded algebra, where elements of $\mathfrak{k}^*$ have degree two, and differential forms their exterior degree. If N is a vector space with linear action of K, then $\mathcal{H}^{\mathrm{pol}}(\mathfrak{k}, N) = S(\mathfrak{k}^*)^K$. A basic theorem of H. Cartan says: if K acts on a compact manifold M with finite stabilizers, then $\mathcal{H}^{\mathrm{pol}}(\mathfrak{k}, M) = \mathcal{H}^*(M/K)$.

If N is non-compact, we can also consider the space $\mathcal{A}^{\mathrm{pol,cpt}}(\mathfrak{k}, N) := (S(\mathfrak{k}^*) \otimes \mathcal{A}^{\mathrm{cpt}}(N))^K$ of equivariant forms $\alpha(\phi)$ which are compactly supported on N. We

denote by $\mathcal{H}^{\mathrm{pol,cpt}}(\mathfrak{k}, N)$ the corresponding cohomology space. Integration is well defined on it if N is oriented and the result of integration $\int_N \alpha(\phi)$ is a polynomial function on $\mathfrak{k}$, invariant under the adjoint action of K on $\mathfrak{k}$.

If N is a vector space, there exists a unique element $\mathrm{Thom}(\phi) \in \mathcal{H}^{\mathrm{pol,cpt}}(\mathfrak{k}, N)$ with integral equals to 1.

Let us give the formula for $N := \mathbb{R}^2$ with action of S^1.

• $N := \mathbb{R}^2$. Let χ be any smooth compactly supported function on $\mathbb{R}$ such that $\chi(0) = 1$. Then

$$\mathrm{Thom}_\chi(\phi) := \frac{-1}{2\pi}(\phi\, \chi(x^2 + y^2) + 2\chi'(x^2 + y^2)dx \wedge dy) \tag{8}$$

is a representative of $\mathrm{Thom}(\phi)$.

If N is a vector space, a representative of $\mathrm{Thom}(\phi)$ with "Gaussian look" is given by Mathai–Quillen in [33].

Details on Cartan's theory and further developments can be found in the stern monograph (which contains treasures) [25], or in the attractive book [27]. This de Rham point of view for topological equivariant cohomology seems to be adapted only to smooth spaces. However, the use of equivariant Poincaré dual allows us to work on algebraic varieties, where the Joseph polynomials and the Rossmann localization formula (see [42]) are important tools. For lack of space, I will not pursue this topic. Let me also mention the theory of equivariant Chow groups for algebraic actions on algebraic varieties defined over any field, initiated by Totaro and developed by Edidin–Graham and Brion.

Generalized coefficients ([25]). An equivariant form $\alpha(\phi)$ with $C^{-\infty}$ coefficients is a generalized function on $\mathfrak{g}$ with values in $\mathcal{A}(N)$. Thus for any smooth function F on $\mathfrak{g}$ with compact support, the integral $\int_{\mathfrak{g}} \alpha(\phi)F(\phi)d\phi$ is a differential form on N. We denote by $\mathcal{A}^{-\infty}(\mathfrak{g}, N)$ the space of such forms. If $N := \bullet$ is a point, an equivariant form with $C^{-\infty}$ coefficients is just an element of $(C^{-\infty}(\mathfrak{g}))^G$, that is, an invariant generalized function on $\mathfrak{g}$. The operator D is well defined on $\mathcal{A}^{-\infty}(\mathfrak{g}, N)$, and we denote the corresponding cohomology space by $\mathcal{H}^{-\infty}(\mathfrak{g}, N)$. It is a module over $\mathcal{H}^{\infty}(\mathfrak{g}, N)$. If K acts freely on N, the natural image of $\mathcal{H}^{\infty}(\mathfrak{k}, N)$ in $\mathcal{H}^{-\infty}(\mathfrak{k}, N)$ is equal to 0.

Example 3. Let $M := S^1 = \{e^{i\theta}\}$. The group $S^1 := \{e^{i\phi}\}$ acts freely on M by rotations. Let $\mathfrak{g} := \mathbb{R}J$ be the Lie algebra of S^1. Then $\mathcal{H}^{-\infty}(\mathfrak{g}, M) = \mathbb{C}v$, where $\phi v = 0$. A representative of v, still denoted by v, is the closed equivariant form

$$v(\phi) := \delta_0(\phi)d\theta.$$

Note that $\int_M v(\phi) = (2\pi)\delta_0(\phi)$.

On the other hand, we have $1 = -i\, D(Y^+(\phi)d\theta)$ so that

$$1 = 0 \quad \text{in } \mathcal{H}^{-\infty}(\mathfrak{g}, M).$$

Thus the image of $\mathcal{H}^{\infty}(\mathfrak{g}, M) = \mathbb{C} \cdot 1$ in $\mathcal{H}^{-\infty}(\mathfrak{g}, M)$ vanishes.

3.5. Localization or 1 = 0. Let N be a K-manifold and let κ be a K-invariant vector field, tangent to K-orbits. If $\nu\colon N \to \mathfrak{k}$ is a K-invariant map, then κ, defined by

$$\kappa_m := \frac{d}{d\varepsilon} \exp(\varepsilon \nu(m)).m|_{\varepsilon=0} \tag{9}$$

is such a vector field.

Let C be the set of zeroes of κ. Via a K-invariant Riemannian structure $(\bullet, \bullet)$ on N, identify κ with the K-invariant 1-form on N: $\langle \kappa, \bullet \rangle := (\kappa, \bullet)$. Witten considers the exact equivariant form $D\kappa(\phi) = -\langle \kappa, V\phi \rangle + d\kappa$. From our tangential hypothesis, $\phi \mapsto \langle \kappa_m, V\phi \rangle$ is a non-zero element of $\mathfrak{k}^*$ when m is not in C.

Let $\alpha(\phi) \in \mathcal{H}^\infty(\mathfrak{k}, N)$, compactly supported on N. For any test function $F(\phi)$ on $\mathfrak{k}$ and any a in $\mathbb{R}$, we have the equality

$$\iint_{N\times\mathfrak{k}} \alpha(\phi)F(\phi)d\phi = \int_N \int_{\mathfrak{k}} e^{-iaD\kappa(\phi)}\alpha(\phi)F(\phi)d\phi. \tag{10}$$

When a tends to infinity, standard estimates on Fourier transforms shows that the differential form $\int_{\mathfrak{k}} e^{-iaD\kappa(\phi)}\alpha(\phi)F(\phi)d\phi$ becomes very small outside C.

Inspired by Witten's deformation argument, Paradan proves that outside C, the constant 1 is equal to 0 in $\mathcal{H}^{-\infty}(\mathfrak{k}, N - C)$.

Theorem 4 (Paradan, [37]). *On $N - C$, the integral*

$$B(\phi) := i \int_0^\infty e^{-iaD\kappa(\phi)}\kappa da$$

is a well defined element of $\mathcal{A}^{-\infty}(\mathfrak{k}, N - C)$ and we have $1 = D(B(\phi))$. Thus

$$1 = 0 \quad \text{in } \mathcal{H}^{-\infty}(\mathfrak{k}, N - C).$$

Indeed, intuitively $B(\phi) = \frac{\kappa}{D\kappa(\phi)}$, so that $DB(\phi) = \frac{D\kappa(\phi)}{D\kappa(\phi)} = 1$.

Multiplying an element $\alpha(\phi)$ of $\mathcal{H}^\infty(\mathfrak{k}, N)$ by 1, we see that $\alpha(\phi)$ vanishes on $N - C$. In the next proposition, we give an explicit representative of α with support near C.

Proposition 5 ([37]). *Let χ be a K-invariant function on N supported on a small neighborhood of C and such that $\chi = 1$ on a smaller neighborhood of C. Let*

$$P(\phi) := \chi + d\chi \wedge B(\phi).$$

Then $P(\phi)$ is a closed equivariant form in $\mathcal{A}^{-\infty}(\mathfrak{k}, N)$ supported near C. Furthermore, we have the equation in $\mathcal{A}^{-\infty}(\mathfrak{k}, N)$:

$$P = 1 + D((\chi - 1)B).$$

Thus, if $\alpha(\phi) \in \mathcal{H}^\infty(\mathfrak{k}, N)$, then $P(\phi)\alpha(\phi)$ is supported near C and equal to $\alpha(\phi)$ in $\mathcal{H}^{-\infty}(\mathfrak{k}, N)$.

In the basic examples $\mathbb{R}^2$ or T^*S^1 with action of S^1, and κ appropriately chosen, the forms $B(\phi)$ and $P(\phi)$ are easy to calculate.

• Consider $N := \mathbb{R}^2$ with $\kappa := y\partial_x - x\partial_y$. On $\mathbb{R}^2 - \{[0,0]\}$, in polar coordinates r, θ, we compute that $B(\phi) = -iY^+(\phi)d\theta$. Thus, if χ is a smooth function with compact support on $\mathbb{R}$ and equal to 1 in a neighborhood of 0, then

$$P(\phi) = (2i\pi)Y^+(\phi)\mathrm{Thom}_\chi(\phi),$$

where $\mathrm{Thom}_\chi(\phi)$ is defined by Formula (8). Note that the integral of $P(\phi)$ on N is $(2i\pi)Y^+(\phi)$.

• Consider $N := T^*S^1$ with $\kappa := -t\partial_\theta$. Then in coordinates t, θ,

$$B(\phi) = -iY^+(\phi)d\theta \quad \text{if } t > 0,$$
$$B(\phi) = iY^-(\phi)d\theta \quad \text{if } t < 0.$$

If χ is a smooth function with compact support on $\mathbb{R}$ and equal to 1 in a neighborhood of 0, then

$$P(\phi) = \chi(t) + \chi'(t)dt \wedge B(\phi).$$

Note that the integral of $P(\phi)$ on N is $(2i\pi)(Y^+(\phi) + Y^-(\phi)) = (2i\pi)\delta_0(\phi)$.

For the sake of simplicity, assume that N is compact. Consider the form $P \in \mathcal{H}^{-\infty}(\mathfrak{k}, N)$ constructed in Proposition 5 and supported near the set C of zeroes of κ. We write $C = \cup C_F$ where C_F are the connected components of the set C. Write $P = \sum_F P_F$ where P_F is compactly supported on a small neighborhood U_F of C_F. Proposition 6 reduces the calculation of the integral of $\alpha(\phi)$ on N to calculations near C. We obtain the following localization theorem.

Theorem 6 ([37]). *Consider an equivariant class $\alpha(\phi) \in \mathcal{H}^\infty(\mathfrak{k}, N)$. For any component C_F of the set C, let $\alpha_F(\phi) \in \mathcal{H}^\infty(\mathfrak{k}, U_F)$ an equivariant class equal to $\alpha(\phi)$ on U_F. Then*

$$\int_N \alpha(\phi) = \sum_{C_F} \int_{U_F} P_F(\phi)\alpha_F(\phi).$$

In this localization theorem, each local contribution $\int_{U_F} P_F(\phi)\alpha_F(\phi)$ is a generalized function on $\mathfrak{k}^*$. Thus the Fourier transform of each local contribution has a meaning, under a moderate growth condition for α.

As an application, we recover the exact stationary phase, and more generally the "abelian" localization formula, with the following tool. For a S^1-action with generator J, we choose $\kappa := J$, so that C is the set of fixed points of the one parameter group $\exp(\phi J)$. We obtain the following result that we state in the case of isolated fixed points.

Theorem 7 ([14], [51], [4]). *Let S^1 acting on a compact manifold M with isolated fixed points. Let $\alpha(\phi)$ be a closed equivariant form with C^∞ coefficients. Then*

$$(2\pi)^{-\frac{\dim M}{2}} \int_M \alpha(\phi) = \sum_{p \in \{\text{fixed points}\}} \frac{i_p^*\alpha(\phi)}{\sqrt{\det_{T_pM} L_p(\phi)}}.$$

4. Applications and conjectures

4.1. Integrals on reduced spaces

4.1.1. Reduced spaces. Let N be a Hamiltonian K-manifold. Assume that $\xi \in \mathfrak{k}^*$ is a regular value of the moment map μ and let K_ξ be the stabilizer of ξ. Then K_ξ acts with finite stabilizers in $\mu^{-1}(\xi)$ so that $\mu^{-1}(\xi)/K_\xi$ is a symplectic orbifold, called the reduced space at ξ and denoted by N_ξ. We denote by s_ξ the number of elements of the stabilizer of a generic point in $\mu^{-1}(\xi)$. If $\xi = 0$, we also denote $N_0 = \mu^{-1}(0)/K$ by $N//K$. When N is a projective manifold, then $N//K$ is the quotient in the sense of Mumford's geometric invariant theory (see chapter 8.2 [36]). By considering the symplectic manifold $N \times (K \cdot (-\xi))$ (the shifting trick), we may always consider reduction at 0.

If 0 is a regular value, Kirwan associates to an equivariant closed form $\alpha(\phi)$ on N a cohomology class α_{red} on $N//K$: $\alpha(\phi)|_{\mu^{-1}(0)}$ is equivalent to the pull-back of α_{red}. The Kirwan map $\chi : \mathcal{H}_K^*(N) \to \mathcal{H}^*(N//K)$ is surjective, at least when N is compact.

The following result relates the equivariant volume of M to volumes of reduced spaces.

Proposition 8 ([26]). *If M is a K-Hamiltonian manifold, then*

$$\mathrm{vol}_M(\phi) = \int_{\mathfrak{k}^*} e^{i\langle \xi, \phi\rangle} \,\mathrm{vol}(M_\xi) d\xi.$$

This theorem holds also if N is a K-Hamiltonian manifold with proper moment map, under some convergence conditions. As shown by Formula (7) (Section 3.3), if a torus T acts on a vector space N with weights $\beta_a \in \mathfrak{t}^*$, all contained in a half-space, then the equivariant volume $\mathrm{vol}_N(\phi)$ is the boundary value of $\frac{1}{\prod_a (-i\beta_a(\phi))}$. Its Fourier transform is the convolution H of the Heaviside distributions supported on the half-lines $\mathbb{R}^+\beta_a$. Computing volumes of the reduced manifolds N_ξ is the same as computing the value of H at a point $\xi \in \mathfrak{t}^*$. In Section 5.1, we will explain how to do it using iterated residues.

In the next section, we explain Witten's generalization of Proposition 8.

4.1.2. Witten's localization theorem. Assume that M is a compact K-Hamil-tonian manifold with moment map $\mu\colon M \to \mathfrak{k}^*$. We choose a K-invariant identification $\mathfrak{k}^* \to \mathfrak{k}$ given by a K-invariant inner product. The vector field κ defined by $\kappa_m := \frac{d}{d\varepsilon} \exp(-\varepsilon\mu(m)) \cdot m|_{\varepsilon=0}$ is K-invariant. We refer to this particularly important vector field as the Kirwan vector field. In this case, the set C of zeroes of κ is the set of critical points of the invariant function $\|\mu\|^2$ on M. One connected component of C is the set $\mu^{-1}(0)$ of zeroes of the moment map (if not empty). The following theorem follows from Witten's deformation argument: Formula (10) in Section 3.5.

Theorem 9 (Witten [52]). *Let M be a compact Hamiltonian K-manifold and $p(\phi)$ an equivariantly closed form with polynomial coefficients. Assume that* 0 *is a regular value of the moment map. Then*

$$\int_{\mathfrak{k}} \left(\int_M e^{i\Omega(\phi)} p(\phi) \right) d\phi = s_0 (2i\pi)^{\dim \mathfrak{k}} \operatorname{vol}(K) \int_{M//K} e^{i\Omega_{\mathrm{red}}} p_{\mathrm{red}}.$$

Let me explain the meaning of the integral on the left. Let $I_M(\phi) := \int_M e^{i\Omega(\phi)} p(\phi)$. This is an analytic function on $\mathfrak{k}$ with at most polynomial growth. We compute $\int_{\mathfrak{k}} e^{i\langle \xi, \phi \rangle} I_M(\phi) d\phi$ in the sense of Fourier transform. This Fourier transform is a polynomial near $\xi = 0$ (this is part of the theorem). The left-hand side $\int_{\mathfrak{k}} I_M(\phi) d\phi$ is by definition the value of this polynomial at $\xi = 0$.

The theorem above is used to compute integrals on reduced spaces. Indeed, the right hand side of the equality is the integral of a cohomology class over the reduced space $M//K$ of M, which is difficult to compute. Instead, we first compute an equivariant integral on the original space M (easy to do thanks to the usual reduction to the maximal torus T and the abelian localization formula). Then we have to compute the value of the Fourier transform of $I_M(\phi)$ at the point 0. This in turn demands the computation of the value of the convolution of Heaviside distributions at some explicit points of $\mathfrak{t}^*$: the images by μ of the fixed points of the action of T on M.

Using different methods, other proofs and refinements to Witten's theorem have been given ([28], [47], [37], [43]). Let us recall Paradan's method. We apply Theorem 6 to the form $\alpha(\phi) = e^{i\Omega(\phi)} p(\phi)$. Here C_F varies over the connected components of the set of critical points of $\|\mu\|^2$. The image of a connected component C_F by the moment map μ is a K-orbit $K\beta$. The set $C_0 := \mu^{-1}(0)$ projecting on 0 is one connected component of C (if non-empty). The Fourier transform of $\int_M e^{i\Omega(\phi)} p(\phi) P_F(\phi)$ when C_F projects on $K\beta$ with $\beta \neq 0$ is supported on $\|\xi\| \geq \|\beta\|$. Thus the value of the Fourier transform of $\int_M e^{i\Omega(\phi)} p(\phi)$ at 0 comes only from $\int_M e^{i\Omega(\phi)} p(\phi) P_0(\phi)$ and requires only local knowledge of our data near $\mu^{-1}(0)$. To summarize, in Witten's localization formula, the Fourier transform of the local terms arising from components different from C_0 are moved away from our focus of attention: the point 0 in $\mathfrak{k}^*$.

These facts are illustrated in the example below. This also shows that local calculations near critical points essentially reduce to $\mathbb{R}^2$ or T^*S^1.

Example 10. Return to Example 2 of the sphere $M := \{x^2 + y^2 + z^2 = A^2\}$, with moment map $\mu(x, y, z) = x$. The critical values of x^2 are $0, A, -A$. The set of critical points has three connected components: the circle C_0 drawn in black in Figure 3, $\{p^+\}$ and $\{p^-\}$. The normal bundle to C_0 is identified with T^*S^1 and the normal bundles to p^+, p^- with $\mathbb{R}^2$. Let

$$\operatorname{vol}_M(\phi) = \frac{1}{2i\pi} \int_M e^{i\Omega(\phi)}.$$

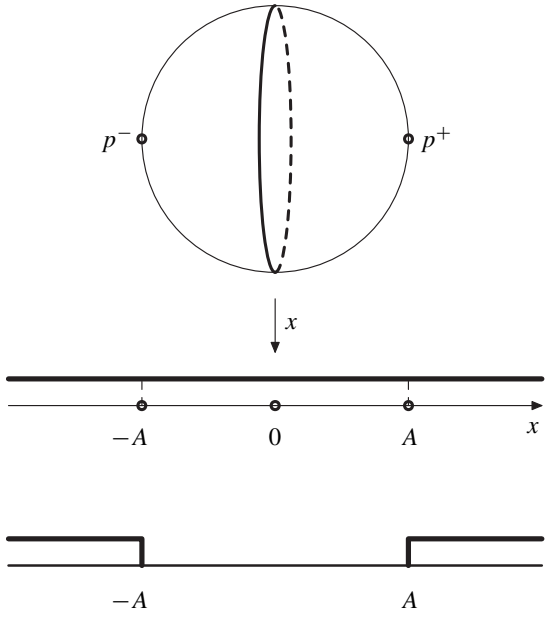


Figure 3. Decomposition of equivariant volumes.

Using the Kirwan vector field, we obtain a decomposition $\mathrm{vol}_M(\phi) = v_0(\phi) + v_{p^-}(\phi) + v_{p^+}(\phi)$ with

$$v_0(\phi) := \frac{1}{2i\pi}\int_M e^{i\Omega(\phi)} P_0(\phi) = \delta_0(\phi),$$
$$v_{p^-}(\phi) := \frac{1}{2i\pi}\int_M e^{i\Omega(\phi)} P_{p^-}(\phi) = -e^{-i\phi A} Y^-(\phi),$$
$$v_{p^+}(\phi) := \frac{1}{2i\pi}\int_M e^{i\Omega(\phi)} P_{p^+}(\phi) = -e^{i\phi A} Y^+(\phi).$$

This decomposition corresponds to the cone decomposition of the interval $[-A, A]$ described in Figure 1 in Section 2.1.

4.2. Index of transversally elliptic operators. Consider a compact even-dimensional oriented manifold M. For the sake of simplicity, we assume M provided with an almost complex structure. We choose an Hermitian metric $\|\xi\|^2$ on T^*M. For $[x, \xi] \in T^*M$, the symbol of the Dolbeault–Dirac operator $\overline{\partial} + \overline{\partial}^*$ is the Clifford multiplication $c(\xi)$ on the complex vector bundle $\Lambda T_x^* M$. It is invertible for $\xi \neq 0$, since $c(\xi)^2 = -\|\xi\|^2$. Let $\mathcal{E}$ be an auxiliary vector bundle over M, then $c_{\mathcal{E}}([x, \xi]) := c(\xi) \otimes \mathrm{Id}_{\mathcal{E}_x}$ defines an element of $\boldsymbol{K}(T^*M)$, the $\boldsymbol{K}$-theory group of T^*M. Assume that a compact group K acts on M and $\mathcal{E}$. Now the topological index $\mathrm{Index}(c_{\mathcal{E}})$

of $c_{\mathcal{E}} \in \boldsymbol{K}_K(T^*M)$ is an invariant function on K (which computes the equivariant index of the K-invariant operator $\overline{\partial}_{\mathcal{E}} + \overline{\partial}^*_{\mathcal{E}}$). The index theorem of Atiyah–Segal–Singer expresses $\mathrm{Index}(c_{\mathcal{E}})(k)$ ($k \in K$) in terms of the fixed points of k on M. We constructed (see [13]) the equivariant Chern character $\mathrm{ch}(\phi, \mathcal{E})$ of the vector bundle $\mathcal{E}$ and the equivariant Todd class $\mathrm{Todd}(\phi, M)$ such that (for ϕ small)

$$\mathrm{Index}(c_{\mathcal{E}})(\exp\phi) = (2i\pi)^{-(\dim M)/2} \int_M \mathrm{ch}(\phi, \mathcal{E})\mathrm{Todd}(\phi, M). \tag{11}$$

For $\phi = 0$, this is the Atiyah–Singer formula. Formula (11) is a "delocalization" of the Atiyah–Segal–Singer formula. The delocalized index formula (11) can be adapted to new cases such as:

- Index of transversally elliptic operators.
- L^2-index of some elliptic operators on some non-compact manifolds (as in Narasimhan–Okamoto, Parthasarathy, Atiyah–Schmid, Connes–Moscovici).

Indeed, in these two contexts, the index exists in the sense of generalized functions but cannot be always computed in terms of fixed point formulae.

Recall Atiyah–Singer's definition of transversally elliptic operators (see [2]). Let N be a K-manifold and $T^*_K N$ be the conormal bundle to K-orbits. A transversally elliptic pseudo-differential operator S is elliptic in the directions normal to the K-orbits. Thus S together with the action of the Casimir of $\mathfrak{k}$ defines an elliptic system, and the space of solutions of S decomposes as a Hilbert direct sum of finite-dimensional spaces of K-finite solutions. The symbol of S defines an element $\sigma(S)$ of $\boldsymbol{K}_K(T^*_K N)$. The index of the operator S is the character of K in the virtual vector space obtained as difference of K-finite solutions of S and its adjoint. This is an invariant generalized function on K. In [16], we gave a cohomological formula for the index of S in terms of $\sigma(S) \in \boldsymbol{K}_K(T^*_K N)$, as an equivariant integral on T^*N in the spirit of the delocalized formula (11). This result was inspired by Bismut's ideas on delocalizations [18] and Quillen's superconnection formalism.

The following example shows that, contrary to the melancholy remark of Atiyah about his work on transversally elliptic operators (page 6, vol. 4, [1]), there are many transversally elliptic bundle maps of great interest.

Consider a K-manifold N with a K-invariant vector field κ tangent to orbits. As before, we assume that N is provided with a K-invariant almost complex structure and Hermitian metric. We still denote by $c(\xi)$ the Clifford action of $\xi \in T^*_x N$ on the complex space $\Lambda T^*_x N$. The analogue in K-theory of Witten's deformation is the bundle map

$$c_{\kappa,\mathcal{E}}([x, \xi]) := c(\xi - \kappa_x) \otimes \mathrm{Id}_{\mathcal{E}_x}, \tag{12}$$

defined by Paradan [38]. Note that $c_{\kappa,\mathcal{E}}([x, \xi])$ is invertible except if $\xi = \kappa_x$. If furthermore $[x, \xi] \in T^*_K N$, then $\xi = 0$ and $\kappa_x = 0$. Indeed, by our hypothesis, under identification of T^*N with TN, κ_x is tangent to Kx while ξ is normal to Kx.

When N is compact, $c_{\kappa,\mathcal{E}}$ is transversally elliptic and equal in $\boldsymbol{K}$-theory to the elliptic symbol $c_{\mathcal{E}}$, via the deformation $c(\xi - a\kappa_x) \otimes 1_{\mathcal{E}}$, for $a \in [0, 1]$. Under the conditions stated below, Paradan's construction defines a transversally elliptic element even if N is a non-compact manifold. See also the construction by M. Braverman [21] of a related operator.

Proposition 11 ([38]). *Assume that the set C of zeroes of κ is compact. Then $c_{\kappa,\mathcal{E}}$ is transversally elliptic on T^*N with support the zero section $[C, 0]$.*

Recall the closed equivariant form P on N supported on a neighborhood of C constructed with the help of κ in Proposition 5. Then

Theorem 12 ([40]). *Near the identity element 1 of K, the index of $c_{\kappa,\mathcal{E}}$ is given by the formula*

$$\mathrm{Index}(c_{\kappa,\mathcal{E}})(\exp\phi) = (2i\pi)^{-(\dim N)/2} \int_N \mathrm{ch}(\phi, \mathcal{E})\mathrm{Todd}(\phi, N)P(\phi) \tag{13}$$

and by similar integral formulae over N_s near any point $s \in K$.

When M is compact, Formula (13) reduces to Formula (11) since $P(\phi)$ is equal to 1 in cohomology. But even in this case, Formula (13) has important implications, as the symbol $c_{\mathcal{E}}$ is broken into several parts according to the connected components of C: $c_{\mathcal{E}} = \sum_F c_{\mathcal{E},F}$ where $c_{\mathcal{E},F}$ is supported on $[C_F, 0]$. Thus

$$\mathrm{Index}(c_{\mathcal{E}}) = \sum_F \mathrm{Index}(c_{\mathcal{E},F}).$$

Each local contribution $\mathrm{Index}(c_{\mathcal{E},F})$ is well defined as a character of an infinite-dimensional representation of K. This was one of the motivations of Atiyah and Singer for introducing transversally elliptic operators.

As in the Witten localization formula, this allows in important cases to compute the invariant part $\mathrm{Index}(c_{\mathcal{E}})^K$ through considering only the contribution of C_0. The Fourier series attached to the other components do not interfere with our focus of attention: the multiplicity of the trivial representation. This fact is illustrated in the example below.

Example 13. Return to Example 10. Let A be a positive integer. We identify $P_1(\mathbb{C})$ with $M_A := \{x^2 + y^2 + z^2 = A^2\}$ through the map

$$[z_1, z_2] \mapsto \left(A\frac{|z_1|^2 - |z_2|^2}{|z_1|^2 + |z_2|^2}, 2A\frac{\Re(z_1\overline{z_2})}{|z_1|^2 + |z_2|^2}, 2A\frac{\Im(z_1\overline{z_2})}{|z_1|^2 + |z_2|^2} \right),$$

the action $(e^{i\phi}z_1, z_2)$ becoming the rotation around the x-axis. We consider the Dolbeault–Dirac operator D_{2A} on $P_1(\mathbb{C})$ with solution space $\oplus_{j+k=2A}\mathbb{C}z_1^j z_2^k$. Twisting the action by $e^{i\phi A}$, its equivariant index is $\sum_{k=-A}^{A} q^k$ with $q := e^{i\phi}$. Using the

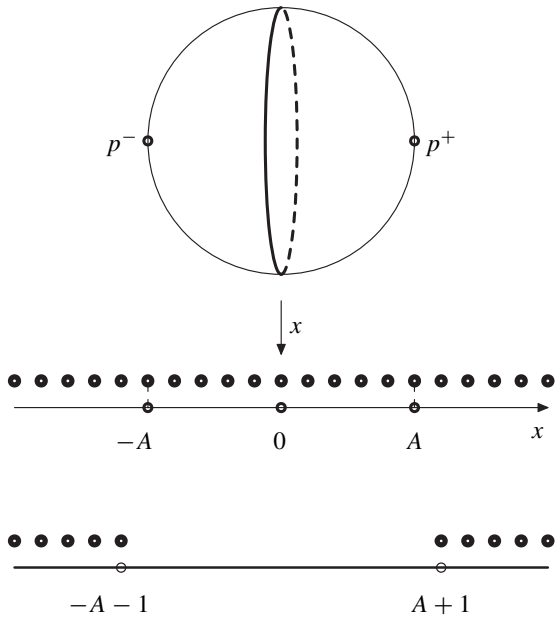


Figure 4. Decomposition of equivariant indices.

Kirwan vector field, we decompose $D_{2A} = D_0 + D_{p^+} + D_{p^-}$ into the sum of three transversally elliptic operators with support $[C_0, 0]$, $[p^+, 0]$, $[p^-, 0]$, respectively. To compute the index of D_0, we are led to compute the set of solutions of the Dolbeault operator on the complex manifold $\mathbb{C}/\mathbb{Z} = S^1 \times \mathbb{R}$, the action of $S^1 = \mathbb{R}/2\pi\mathbb{Z}$ being by translations, and we obtain all functions e^{ikz} for any $k \in \mathbb{Z}$. Thus

$$\mathrm{Index}(D_0) = \sum_{k=-\infty}^{\infty} q^k.$$

Near the fixed points p^+, p^-, we obtain the index of the lift of the operators $\overline{\partial}^{\pm}$ (see [2]) on $\mathbb{C}$ (shifted):

$$\mathrm{Index}(D_{p^+}) = -\sum_{k=A+1}^{\infty} q^k, \quad \mathrm{Index}(D_{p^-}) = -\sum_{k=-\infty}^{-A-1} q^k.$$

The equality

$$\mathrm{Index}(D_{2A}) = \mathrm{Index}(D_0) + \mathrm{Index}(D_{p^+}) + \mathrm{Index}(D_{p^-})$$

is Formula (2) in Section 2.1.

It might happen that the integral $\int_N \mathrm{ch}(\phi, \mathcal{E})\mathrm{Todd}(\phi, N)$ over our non-compact manifold N is already convergent in the distributional sense, and as $P = 1$ in cohomology, it might happen, modulo the convergence of the boundary term, that the following equality holds

$$\mathrm{Index}(c_{\kappa,\mathcal{E}})(\exp\phi) = (2i\pi)^{-(\dim N)/2} \int_N \mathrm{ch}(\phi, \mathcal{E})\mathrm{Todd}(\phi, N).$$

This is indeed the case for discrete series. To state the result, we rephrase the preceding constructions in the spin context. If N is an even-dimensional oriented spin manifold, and $\mathcal{E}$ a twisting vector bundle, we denote by $\sigma(\xi)$ the Clifford action of $\xi \in T_x^*N$ on spinors, and by $\sigma_{\mathcal{E}}$ the symbol of the twisted Dirac operator $D_{\mathcal{E}}$. If M is a compact K-manifold, the equivariant index of $D_{\mathcal{E}}$ is given by a formula similar to (11):

$$\mathrm{Index}(\sigma_{\mathcal{E}})(\exp\phi) = (2i\pi)^{-(\dim M)/2} \int_M \mathrm{ch}(\phi, \mathcal{E})\hat{A}(\phi, M), \tag{14}$$

where the equivariant class $\hat{A}$ replaces the equivariant Todd class.

Under the same hypothesis as in Proposition 11, the bundle map

$$\sigma_{\kappa,\mathcal{E}}([x, \xi]) = \sigma(\xi - \kappa_x) \otimes \mathrm{I}_{\mathcal{E}_x}$$

is transversally elliptic and its equivariant index is a generalized function on K.

Let G be a real reductive Lie group with maximal compact subgroup K. We assume that the maximal torus T of K is a maximal torus in G. Let $N := G\lambda$ be the orbit of a regular admissible element $\lambda \in \mathfrak{t}^*$. Harish-Chandra associates to λ a representation of G, realized as the L^2-index of the twisted Dirac operator D_λ. The moment map μ for the K-action on N is the projection $G\lambda \to \mathfrak{t}^*$ and the set C of zeroes of the Kirwan vector field κ is easy to compute in this case: it consists of the compact orbit $K \cdot \lambda$.

Theorem 14 (Paradan [39]). *The character of the discrete series $\Theta^G(\lambda)$ restricted to K is the index of the transversally elliptic element $\sigma_{\kappa,\mathcal{L}_\lambda}$ on N.*

Here $\mathcal{L}_\lambda$ is the Kostant line bundle $G \times_{G(\lambda)} \mathbb{C}_\lambda$ on $N = G/G(\lambda)$. A calculation of the index of $\sigma_{\kappa,\mathcal{L}_\lambda}$ (which is supported on $K \cdot \lambda$) leads immediately to Blattner's formula for $\Theta^G(\lambda)|_K$.

4.3. Quantization and symplectic quotients. Let N be a G-manifold (N, G non-necessarily compact), and $\mathcal{E}$ a G-equivariant vector bundle on N with G-invariant connection ∇. We can then construct the closed equivariant form $\mathrm{ch}(\phi, \mathcal{E})$ ([15], [20]). For the sake of simplicity, I assume the existence of a G-invariant complex structure. Then I conjectured (under additional conditions that I do not know how to formulate exactly, see attempts in [46])

Conjecture. There exists a representation $Q(N, \mathcal{E})$ of G such that the character $\mathrm{Tr}_{Q(N,\mathcal{E})}(g)$ is given by the formula

$$\mathrm{Tr}_{Q(N,\mathcal{E})}(\exp\phi) = (2i\pi)^{-(\dim N)/2} \int_N \mathrm{ch}(\phi, \mathcal{E})\mathrm{Todd}(\phi, N) \tag{15}$$

near $1 \in G$ and by a similar integral formula over N_s near any elliptic point s of G.

Thus, via integration of equivariant cohomology classes, it should be possible to define a push-forward map from a generalized $\boldsymbol{K}$-theory of vector bundles with connections on G-manifolds to invariant generalized functions on G, under some convergence conditions, and assuming the existence of a suitable equivariant Todd class.

Remark 15. When N is a coadjoint admissible regular orbit of any real algebraic Lie group G and $\mathcal{E}$ the Kostant half-line bundle, Formula (15), with the $\hat{A}$ class instead of the Todd class, becomes Kirillov's universal formula [29] for characters (proved by Kirillov for compact and nilpotent groups, by Duflo, Rossmann, Bouaziz, Khalgui, Vergne,... for any real algebraic group). If N, G are compact, Formula (15), with $\hat{A}$ instead of Todd, is the equivariant index formula for the Dirac operator twisted by $\mathcal{E}$. Thus Formula (15), modified as in [46], is a fusion of the Kirillov universal character formula and of the formulae of Atiyah–Segal–Singer for indices of twisted Dirac operators.

Now let (M, Ω) be a compact symplectic manifold with Hamiltonian action of a compact group K. We assume the existence of a K-equivariant line bundle $\mathcal{L}$ on M with connection ∇ of curvature equal to $i\Omega$. In other words, M is prequantizable in the sense of [30] and we call $\mathcal{L}$ the Kostant line bundle. We take an almost complex structure compatible with Ω (see [35]). Then we denote $Q(M, \mathcal{L})$ simply by $Q(M)$. This is a canonical finite-dimensional virtual representation $Q(M)$ of K, the quantization of the symplectic manifold M. The spectrum of the action of $\phi \in \mathfrak{k}$ in $Q(M)$ should be the "quantum" version of the levels of energy of the Hamiltonian function $\langle \mu, \phi \rangle$ on M (see [49] for survey). Guillemin and Sternberg conjectured in 1982 that the multiplicity of the irreducible representation V_ξ of K (of highest weight $\xi \in \mathfrak{t}_+^* \subset \mathfrak{k}^*$) in the representation $Q(M)$ is equal to $Q(M_\xi)$ and proved it for the case of Kähler manifolds. This is summarized by the slogan: "Quantization commutes with Reduction". In other words, when $\xi = 0$, we should have the equality

$$\int_K \mathrm{Tr}_{Q(M)}(k)dk = \int_{M//K} \mathrm{ch}(\mathcal{L}//K)\mathrm{Todd}(M//K).$$

Although a fixed point formula exists for $\mathrm{Tr}_{Q(M)}(k)$, it is difficult to extract the Guillemin–Sternberg conjecture directly from the Atiyah–Bott Lefschetz formula. Thus this conjecture (fundamental for the credo of quantum mechanics) remained unproved for years. Witten's inversion formula [52]

$$\int_{\mathfrak{k}} \left(\int_M e^{i\Omega(\phi)} p(\phi) \right) d\phi = s_0 (2i\pi)^{\dim \mathfrak{k}} \mathrm{vol}(K) \int_{M//K} e^{i\Omega_{\mathrm{red}}} p_{\mathrm{red}}$$

is in strong analogy with this conjecture. In particular, apart from factors of $2i\pi$, the form $e^{i\Omega_{\text{red}}}$ is equal to $\text{ch}(\mathcal{L}//K)$. Meinrenken [34] used the Atiyah–Bott Lefschetz formula and symplectic cutting in a subtle way to give a proof of Guillemin–Sternberg conjecture for any compact K-Hamiltonian manifold. This result was extended further to singular symplectic quotients in Meinrenken–Sjamaar [35].

Definition 16. Let N be a prequantizable Hamiltonian K-manifold with Kostant line bundle $\mathcal{L}$ such that the moment map is proper and the set of zeroes of the Kirwan vector field κ is compact. Define

$$Q(N) := \text{Index}(c_{\kappa,\mathcal{L}}).$$

Thus $Q(N)$ is a Fourier series of characters $\text{Tr}(V_\xi)$.

Conjecture. The multiplicity m_ξ of the irreducible representation V_ξ in $Q(N)$ is equal to $Q(N_\xi)$.

When N is compact, this is the Guillemin–Sternberg conjecture.

Paradan [39] proved this conjecture (in the spin context) when $N := G\lambda$ is an admissible regular elliptic coadjoint orbit of a reductive real Lie group G and K the maximal compact subgroup of G. Together with Theorem 14, this implies that irreducible representations $\Theta^K(\xi)$ (of highest weight $\xi - \rho_{\mathfrak{k}}$) of K occurring in Harish-Chandra's discrete series $\Theta^G(\lambda)|_K$ are such that ξ lies in the interior of the Kirwan polytope $\mu(N) \cap \mathfrak{t}^*_+$. This is a strong constraint on representations appearing in $\Theta^G(\lambda)|_K$.

Example 17. Figure 5 is the drawing for the restriction of the representation $\Theta^G(\lambda)$ of SO(4, 1) to SO(4). The black dots are the ξ such that $\Theta^K(\xi)$ occurs in $\Theta^G(\lambda)$ (they all occur with multiplicity 1). The horizontal strip is the Kirwan polytope $\mu(G\lambda) \cap \mathfrak{t}^*_+$.

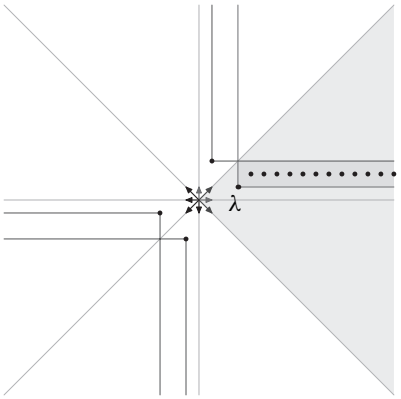


Figure 5. Restriction of discrete series and the Kirwan polytope.

5. Arrangement of hyperplanes

5.1. Convolution of Heaviside distributions and cycles in the complement of a set of hyperplanes. Let us consider a set $\mathcal{B} := \{\beta_1, \dots, \beta_n\}$ of linear forms β_a on a vector space V of dimension r, all in an open half-space of V^*. We assume that the set $\mathcal{B}$ spans V^*. By definition, an element $\xi \in V^*$ is regular if it does not lie in a cone spanned by $(r-1)$ elements of $\mathcal{B}$. A connected component of the set of regular elements is called a chamber.

The convolution H of the Heaviside distributions of the half-lines $\mathbb{R}^+\beta_a$ is a multivariate spline function on V^*, that is, a locally polynomial function continuous on the cone $\mathrm{Cone}(\mathcal{B})$ spanned by $\mathcal{B}$. Our problem is to compute $H(\xi)$ at a particular point $\xi \in V^*$. In principle, $H(\xi)$ is given by the following limit of integrals (on the non-compact "cycle" V of dimension r, and in the sense of Fourier transforms):

$$H(\xi) = \lim_{\varepsilon \to 0} (2i\pi)^{-r} \int_V e^{-i\langle \xi, v\rangle} \frac{1}{\prod_{a=1}^n \langle \beta_a, v + i\varepsilon\rangle} dv$$

where ε is in the dual cone to $\mathrm{Cone}(\mathcal{B})$.

Consider the complement of the hyperplanes defined by $\mathcal{B}$ in the complexified space $V_{\mathbb{C}}$:

$$V(\mathcal{B}) := \{v \in V_{\mathbb{C}};\ \langle v, \beta\rangle \neq 0 \text{ for all } \beta \in \mathcal{B}\}.$$

Jeffrey and Kirwan [28] introduced a residue calculus on the space of functions defined on $V(\mathcal{B})$. A rational function on $V(\mathcal{B})$ is of the form $R(v) = \frac{L(v)}{\prod_{a=1}^n \langle \beta_a, v\rangle^{n_a}}$ where $L(v)$ is a polynomial. The following theorem results from Jeffrey–Kirwan ideas, further refined in [22] and [45]. We still denote by dv the holomorphic r-form $dv_1 \wedge \cdots \wedge dv_r$ on $V_{\mathbb{C}}$.

Theorem 18. *Let $\mathfrak{c} \subset \mathrm{Cone}(\mathcal{B})$ be a chamber. There exists a compact oriented cycle $Z(\mathfrak{c})$ of dimension r contained in $V(\mathcal{B})$ such that for any rational function R on $V(\mathcal{B})$ and any $\xi \in \mathfrak{c}$*

$$\lim_{\varepsilon \to 0} \int_V e^{-i\langle \xi, v\rangle} R(v + i\varepsilon) dv = \int_{Z(\mathfrak{c})} e^{-i\langle \xi, v\rangle} R(v) dv.$$

We gave in [45] a representative for the r-dimensional cycle $Z(\mathfrak{c})$ in $\mathbb{C}^r$ as the set of solutions of r real analytic equations related to quantum cohomology. Furthermore, we gave a simple algorithm, further simplified by De Concini–Procesi [24], to compute the homology class of $Z(\mathfrak{c})$ as a disjoint union of tori, so that integration on $Z(\mathfrak{c})$ is simply the algebraic operation of taking ordinary iterated residues. Indeed, if $T(\boldsymbol{\varepsilon}) \subset V(\mathcal{B})$ is a compact torus of the form in some coordinates $(v_1, v_2, \dots, v_r) \in \mathbb{C}^r := V_{\mathbb{C}}$

$$T(\boldsymbol{\varepsilon}) := \{v \in V(\mathcal{B});\ |v_k| = \varepsilon_k, \text{ for } k = 1, \dots, r\},$$

with $\boldsymbol{\varepsilon} := [\varepsilon_1 \ll \varepsilon_2 \ll \cdots \ll \varepsilon_r]$ a sequence of increasing real numbers (here $\varepsilon_1 \ll \varepsilon_2$ meaning that ε_2 is significantly greater than ε_1, see [45] for precise definitions), then

the integration on $T(\varepsilon)$ of a function $F(v_1, v_2, \ldots, v_r)$ with poles on the hyperplanes defined by $\mathcal{B}$ is

$$\frac{1}{(2i\pi)^r}\int_{T(\varepsilon)} F(v_1, v_2, \ldots, v_r)dv = \operatorname{res}_{v_r=0}\operatorname{res}_{v_{r-1}=0}\cdots\operatorname{res}_{v_1=0} F(v_1, v_2, \ldots, v_r),$$

where each residue is taken assuming that the variables with higher indices have a fixed, non-zero value.

Let me explain why this algorithm is efficient for computing the convolution $H(\xi)$ of a large number of Heaviside distributions in a vector space of small dimension. The usual way to compute $H(\xi)$ is by induction on the cardinal of $\mathcal{B}$. Here we fix ξ in a chamber $\mathfrak{c}$ and we compute the cycle $Z(\mathfrak{c})$ (depending on $\mathfrak{c}$) by induction on the dimension of V. It can be done quite quickly using the maximal nested sets of De Concini–Procesi, at least for classical root systems [5].

5.2. Intersection numbers on toric manifolds. Let T be a torus of dimension r acting diagonally on $N := \mathbb{C}^n$ with weights $\mathcal{B} := [\beta_1, \beta_2, \ldots, \beta_n]$. We assume that the cone $\mathrm{Cone}(\mathcal{B})$ spanned by the vectors β_a is an acute cone in $\mathfrak{t}^*$ with non-empty interior. The moment map $\mu\colon \mathbb{C}^n \to \mathfrak{t}^*$ for the action of T is $\mu(z_1, \ldots, z_n) = \sum_{a=1}^n |z_a|^2\beta_a$. The reduced space $N_\xi = \mu^{-1}(\xi)/T$ at a point $\xi \in \mathrm{Cone}(\mathcal{B})$ is *a toric variety*. It is an orbifold if ξ is regular. The space N_ξ is still provided with a Hamiltonian action of the full diagonal group $H := (S^1)^n$ with Lie algebra $\mathfrak{h} := \{\sum_{a=1}^n v_a J_a\}$. The image of N_ξ under the moment map for H is the convex polytope

$$P(\xi) := \left\{ \sum_{a=1}^n x_a J^a \in \mathfrak{h}^*;\ x_a \geq 0;\ \sum_{a=1}^n x_a\beta_a = \xi \right\}.$$

Computing the volume of the polytope $P(\xi)$ is the same as computing the symplectic volume of N_ξ. All manifolds N_ξ when ξ varies in a chamber $\mathfrak{c}$ are the same toric manifold $N_\mathfrak{c}$, the additional data $\xi \in \mathfrak{c}$ being in one-to-one correspondence with the Hamiltonian structure on $N_\mathfrak{c}$ coming from its identification with the reduced space N_ξ.

The T-equivariant cohomology of N is $S(\mathfrak{t}^*)$. For each chamber $\mathfrak{c}$, the Kirwan map gives a surjective map $\chi(p) := p_{\mathrm{red}}$ from $S(\mathfrak{t}^*)$ to $\mathcal{H}^*(N_\mathfrak{c})$. The following theorem allows us to compute integrals on toric manifolds.

Theorem 19 ([45]). *Let $p \in S(\mathfrak{t}^*)$, then*

$$\int_{N_\mathfrak{c}} \chi(p) = (2i\pi)^{-r}\int_{Z(\mathfrak{c})} \frac{p(\phi)}{\prod_{a=1}^n \langle\beta_a, \phi\rangle}d\phi.$$

Let $\xi \in \mathfrak{c}$ and let $p(\phi) := \langle\phi, \xi\rangle$. Then the cohomology class p_{red} is the symplectic form of $N_\mathfrak{c}$ determined by ξ. This way we obtain the formula:

Corollary 20. *Let $\xi \in \mathfrak{c}$, then*

$$\mathrm{vol}(N_\xi) = \frac{1}{(2\pi)^r}\int_{Z(\mathfrak{c})} \frac{e^{-i\langle\xi,\phi\rangle}}{\prod_{a=1}^n \langle\beta_a, \phi\rangle}d\phi.$$

We recall that the homology class of the cycle $Z(\mathfrak{c})$ is computed recursively so that the preceding integral is easily calculated using iterated residues.

6. Polytopes and computations

It is well known that many theorems on toric varieties have analogues in the world of polytopes. With Brion, Szenes, Baldoni, Berline, we carefully gave elementary proofs of the corresponding theorems on polytopes, even if our inspiration came from equivariant cohomology on Hamiltonian manifolds.

Let $\mathcal{B} := [\beta_1, \dots, \beta_n]$ be a sequence of linear forms on a vector space V of dimension r strictly contained in a half-space of V^*. If $\xi \in V^*$, the partition polytope is

$$P_{\mathcal{B}}(\xi) := \left\{ \boldsymbol{x} = [x_1, x_2, \dots, x_n] \in \mathbb{R}^n;\ x_a \geq 0;\ \textstyle\sum_{a=1}^n x_a \beta_a = \xi \right\}.$$

Any polytope can be realized as a partition polytope.

Example 21 (Transportation polytopes). Consider two sequences $[r_1, r_2, \dots, r_k]$, $[c_1, c_2, \dots, c_\ell]$ of positive numbers with $\sum_i r_i = \sum_j c_j$. Then Transport(k, ℓ, r, c) is the polytope consisting of all real matrices with k rows and n columns, with non-negative entries, and with sums of entries in row i equal to r_i and in column j equal to c_j. This is a special case of a network polytope (see [6], [7]).

The volume of $P_{\mathcal{B}}(\xi)$ is equal to the value at ξ of the convolution of the Heaviside distributions supported on the half-lines $\mathbb{R}^+\beta_a$. This becomes computationally hard if there is a large number of convolutions. The volume of Transport(k, ℓ, r, c) necessitates the convolution of $k\ell$ Heaviside distributions in a space of dimension $k+\ell-1$. For example, Beck–Pixton [12] could compute, on parallel computers, the volume of Transport(k, ℓ, r, c) for $k = 10$, $\ell = 10$, for special values $r_i = c_j = 1$ in 17 years of computation time (scaled on 1 Ghz processor).

Theorem 22. *Let* $\mathfrak{c}$ *be a chamber of* Cone$(\mathcal{B})$ *and let* $\xi \in \overline{\mathfrak{c}}$. *Then*

$$\mathrm{vol}(P_{\mathcal{B}}(\xi)) = (2i\pi)^{-r} \frac{1}{(n-r)!} \int_{Z(\mathfrak{c})} \frac{\langle \xi, v \rangle^{n-r}}{\prod_{a=1}^n \langle \beta_a, v \rangle} dv.$$

Using De Concini–Procesi recursive determination of $Z(\mathfrak{c})$, this formula is expressed as a specific sum of iterated residues.

Assume the β_a span a lattice Λ in V^*, and that ξ is in Λ. The discrete analogue of the volume of $P_{\mathcal{B}}(\xi)$ is the number $N_{\mathcal{B}}(\xi)$ of integral points in the rational polytope $P_{\mathcal{B}}(\xi)$. A fundamental result of Barvinok [8] asserts that $N_{\mathcal{B}}(\xi)$ can be computed in polynomial time, when n is fixed.

The function $N_{\mathcal{B}}(\xi)$ associates to the vector ξ the number of ways to represent the vector ξ as a sum of a certain number of vectors β_a. This is called the vector-partition function of $\mathcal{B}$. There is also a formula [44] for $N_{\mathcal{B}}(\xi)$ as an integral on

the cycle $Z(\mathfrak{c})$. This integral formula has interesting theoretical applications, such as information on the jumps of the partition function from chamber to chamber. For example, the appearance of the five linear factors in $g(a, b)$ (Formula (3) of Section 2.2) follows from [44]. However, except for relatively good systems $\mathcal{B}$, this formula does not allow polynomial time computations. A program for the counting of number of points in any rational polytope following Barvinok's algorithm is done in Latte [31]. For systems not too far from unimodularity, our programs based on integration on $Z(\mathfrak{c})$, that is, on iterated residues, are more efficient. It leads to the fastest computation of number of integral points in network polytopes [6], Kostant partition functions, weight multiplicities c_μ^λ and tensor product multiplicities $c_{\lambda,\mu}^\nu$ of classical Lie algebras (the bit size of the weights λ, μ, ν can be very large [5], [23]).

Finally, let me describe the local Euler–Maclaurin formula which was conjectured by Barvinok–Pommersheim [10]. It was after observing the analogy of this conjecture with the localization theorem (Theorem 6) that I fully realized the beauty of this conjecture. Nicole Berline and I proved it by using elementary means, based on the study of some valuations on rational cones in an Euclidean space,

Let P be a convex polytope in $\mathbb{R}^d$. For the sake of simplicity we assume that P has *integral vertices*. Let $\mathcal{F}$ be the set of faces of P. For each face F of P, the transverse cone of P along F is a cone of dimension equal to the codimension of F.

Theorem 23 (Local Euler–Maclaurin formula). *For each face F, there exists a constant coefficients differential operator D_F (of infinite order), depending only on the transverse cone of P along F, such that, for any polynomial function Φ on $\mathbb{R}^d$,*

$$\sum_{\xi \in P \cap \mathbb{Z}^d} \Phi(\xi) = \sum_{F \in \mathcal{F}} \int_F D_F(\Phi).$$

The detailed statement for any rational convex polytope and what we really mean by "depending only on" is in [17].

The operators D_F have rational coefficients and can be computed in polynomial time when d and the order of the expansion are fixed, with the help of the Barvinok signed decomposition of cones and the LLL short vector algorithm. The local property of D_F means that if two polytopes P and P' are the same in a neighborhood of a generic point of F, then the operators D_F for P and P' coincide.

The local Euler–Maclaurin formula gives in particular a local formula for the number of integral points in P or in the dilated polytopes tP. The Ehrhart polynomial $E(P)(t)$ is defined as the number of integral points in tP, for t a non-negative integer. Then $E(P)(t) = \sum_{i=0}^n e_i t^{n-i}$, with $e_0 = \mathrm{vol}(P)$. Barvinok [9] recently showed that the (periodic) coefficients e_i with $i \leq k$ can be computed in polynomial time, when P is a rational simplex. We hope to implement soon another polynomial time algorithm for the same problem based on our local formula.

Even though time often prevails, in numerical computations as in life, it was rewarding for us to see that our theoretical results could help in effective computations.

References

[1] Atiyah, M. F., *Collected works.* Clarendon Press, Oxford 1988.

[2] Atiyah, M. F., *Elliptic operators and compact groups.* Lecture Notes in Math. 401, Springer-Verlag, Berlin 1974.

[3] Atiyah, M. F., Bott, R., A Lefschetz fixed-point formula for elliptic complexes. I. *Ann. of Math.* **86** (1967), 374–407; II. *Ann. of Math.* **88** (1968), 451–491.

[4] Atiyah, M. F., Bott, R., The moment map and equivariant cohomology. *Topology* **23** (1984), 1–28.

[5] Baldoni, W., Beck, M., Cochet, C., Vergne, M., Volume computation for polytopes and partition functions for classical root systems. *Discrete Comput. Geom.* **35** (2006), 551–595; programs available on www.math.polytechnique.fr/cmat/vergne/

[6] Baldoni, W., de Loera, J., Vergne, M., Counting Integer Flows in Networks. *Found. Comput. Math.* **4** (2004), 277–314; programs available on www.math.ucdavis.edu/~totalresidue/

[7] Baldoni, W., Vergne, M., Residues formulae for volumes and Ehrhart polynomials of convex polytopes. Preprint, 2001; arXiv:math.CO/0103097.

[8] Barvinok, A. I., A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. Oper. Res.* **19** (1994), 769–779.

[9] Barvinok, A. I., Computing the Ehrhart quasi-polynomial of a rational simplex. *Math. Comp.* **75** (2006), 1449–1466.

[10] Barvinok, A. I., Pommersheim, J. E., An algorithmic theory of lattice points in polyhedra. In *New perspectives in algebraic combinatorics* (Billera, Louis J. et al., eds.), Math. Sci. Res. Inst. Publ. 38, Cambridge University Press, Cambridge 1999, 91–147.

[11] Baum, P., Cheeger, J., Infinitesimal isometries and Pontryagin numbers. *Topology* **8** (1969), 173–193.

[12] Beck, M., Pixton, D., The volume of the 10-th Birkhoff polytope. 2003; arXiv:math.CO/0305332.

[13] Berline, N., Getzler, E., M. Vergne, M., *Heat kernels and Dirac operators.* Grundlehren Math. Wiss. 298, Springer-Verlag, Berlin 1992.

[14] Berline, N., Vergne, M., Fourier transforms of orbits of the coadjoint representation. In *Representation theory of reductive groups* (Park City, Utah, 1982), Progr. Math. 40, Birkhäuser, Boston, MA, 1983, 53–67.

[15] Berline, N., Vergne, M., Classes caractéristiques équivariantes. Formule de localisation en cohomologie équivariante. *C. R. Acad. Sci. Paris Sér. I Math.* **295** (1982), 539–541.

[16] Berline, N., Vergne, M., L'indice équivariant des opérateurs transversalement elliptiques. *Invent. Math.* **124** (1996), 51–101.

[17] Berline, N., Vergne, M., Local Euler–Maclaurin formula for polytopes. Preprint, 2006; arXiv:math.CO/0507256.

[18] Bismut, J.-M., Localization formulas, superconnections, and the index theorem for families. *Comm. Math. Phys.* **103** (1986), 127–166.

[19] Bott, R., Vector fields and characteristic numbers. *Mich. Math. J.* **14** (1967), 231–244.

[20] Bott, R., Tu, L., Equivariant characteristic classes in the Cartan model. In *Geometry, analysis and applications* (Varanasi 2000), World Scientific Publishing, River Edge, NJ, 2001, 3–20.

[21] Braverman, M., Index theorem for equivariant Dirac operators on non-compact manifolds. *K-Theory* **27** (2002), 61–101.

[22] Brion, M., Vergne, M., Arrangement of hyperplanes I: Rational functions and Jeffrey-Kirwan residue. *Ann. Sci. École Norm. Sup.* **32** (1999), 715–741.

[23] Cochet, C., Vector partition function and representation theory. Preprint, 2005; arXiv:math.RT/0506159; programs available on www.math.polytechnique.fr/cmat/vergne/

[24] De Concini, C., Procesi, C., Nested sets and Jeffrey-Kirwan residues. In *Geometric methods in algebra and number theory*, Progr. Math. 235, Birkhäuser, Boston, MA, 2005, 139–149.

[25] Duflo, M., Kumar, Shrawan, Vergne, M., Sur la cohomologie équivariante des variétés différentiables. *Astérisque* **215** (1993).

[26] Duistermaat, J. J., Heckman, G., On the variation in the cohomology of the symplectic form of the reduced phase space. *Invent. Math.* **69** (1982), 259–268; Addendum: *Invent. Math.* **72** (1983), 153–158.

[27] Guillemin, V., Sternberg, S., *Supersymmetry and equivariant de Rham theory*. Math. Past Present, Springer-Verlag, Berlin 1999.

[28] Jeffrey, L. C., Kirwan, F. C., Localization for non-abelian group actions. *Topology* **34** (1995), 291–327.

[29] Kirillov, A. A., Characters of unitary representations of Lie groups. *Funkcional. Anal. i Priložen* **2** (1968), 40–55; English transl. *Funct. Anal. Appl.* **2** (1968), 133–146.

[30] Kostant, B., Quantization and unitary representations. I. Prequantization. In *Lectures in modern analysis and applications*, III, Lecture Notes in Math. 170, Springer-Verlag, Berlin 1970, 87–208.

[31] de Loera, J., Haws, D., Hemmecke, R., Huggins, P., Tauzer, J., Yoshida, R., *A User's guide for Latte*. www.math.ucdavis.edu/~latte.

[32] Libine, M., A localization argument for characters of reductive Lie groups: an introduction and examples. In *Noncommutative harmonic analysis*, Progr. Math. 220, Birkhäuser, Boston, MA, 2004, 375–393.

[33] Mathai, V., Quillen, D., Superconnections, Thom classes, and equivariant differential forms. *Topology* **25** (1986), 85–110.

[34] Meinrenken, E., Symplectic surgery and the Spin-c Dirac operator. *Adv. Math.* **134** (1998), 240–277.

[35] Meinrenken, E., Sjamaar, R., Singular reduction and quantization. *Topology* **38** (1999), 699–762.

[36] Mumford, D., Fogarty, J., Kirwan, F., *Geometric invariant theory.* Third edition. Ergeb. Math. Grenzgeb. 34, Springer-Verlag, Berlin 1994.

[37] Paradan, P. E., The moment map and equivariant cohomology with generalized coefficients. *Topology* **39** (2000), 401–444.

[38] Paradan, P. E., Localization of the Riemann-Roch character. *J. Funct. Anal.* **187** (2001), 442–509.

[39] Paradan, P. E., Spin^c quantization and the K-multiplicities of the discrete series. *Ann. Sci. École Norm. Sup.* **36** (2003), 805–845.

[40] Paradan, P. E., Vergne, M., Equivariant Chern character with compact support. In preparation.

[41] Rossmann, W., Kirillov's character formula for reductive groups. *Invent. Math.* **48** (1978), 207–220.

[42] Rossmann, W., Equivariant multiplicities on complex varieties. Orbites unipotentes et représentations III. *Astérisque* **173–174** (1989), 313–330.

[43] Sawin, S. F., Witten's Nonabelian Localization for Noncompact Hamiltonian Spaces. Preprint, 2005; arXiv:math.SG/0503385.

[44] Szenes, A., Vergne, M., Residue formulae for vector partitions and Euler-Maclaurin sums. *Adv. in Appl. Math.* **30** (2003), 295–342.

[45] Szenes, A., Vergne, M., Toric reduction and a conjecture of Batyrev and Materov. *Invent. Math.* **158** (2004), 453–495.

[46] Vergne, M., Geometric quantization and equivariant cohomology. In *First European Congress of Mathematics* (Paris 1992), vol. 1, Progr. Math. 119, Birkhäuser, Basel 1994, 249–295.

[47] Vergne, M., A note on the Jeffrey-Kirwan-Witten localization formula. *Topology* **35** (1996), 243–266.

[48] Vergne, M., Cohomologie équivariante et théorème de Stokes. Notes de Sylvie Paycha. In *Analyse sur les groupes de Lie et théorie des représentations* (Kénitra, 1999), Sémin. Congr. 7, Soc. Math. France, Paris 2003, 1–43.

[49] Vergne, M., Quantification géométrique et réduction symplectique. Séminaire Bourbaki, vol. 2000/2001; *Astérisque* **282** (2002), 249–278.

[50] Vergne, M., Residue formulae for Verlinde sums, and for number of integral points in convex rational polytopes. Notes by Sylvie Paycha. In *Proceedings of the Tenth General Meeting of the European Women in Mathematics* (Malta 2001), World Scientific Publishing, New Jersey, London, Singapore, Hong-Kong 2003, 223–285.

[51] Witten, E., Supersymmetry and Morse theory. *J. Differential Geom.* **17** (1982), 661–692.

[52] Witten, E., Two dimensional gauge theories revisited. *J. Geom. Phys.* **9** (1992), 303–368.

Centre de Mathématiques Laurent Schwartz, 91128 Palaiseau, France
E-mail: vergne@math.polytechnique.fr

$\mathcal{P}$, $\mathcal{NP}$ and mathematics – a computational complexity perspective

Avi Wigderson

"$\mathcal{P}$ versus $\mathcal{NP}$ – a gift to mathematics from computer science"
Steve Smale

Abstract. The $\mathcal{P}$ versus $\mathcal{NP}$ question distinguished itself as the central question of theoretical computer science nearly four decades ago. The quest to resolve it, and more generally, to understand the power and limits of *efficient* computation, has led to the development of computational complexity theory. While this mathematical discipline in general, and the $\mathcal{P}$ vs. $\mathcal{NP}$ problem in particular, have gained prominence within the mathematics community in the past decade, it is still largely viewed as a problem of computer science.

In this paper I shall try to explain why this problem, and others in computational complexity, are not only mathematical problems but also problems *about mathematics*, faced by the working mathematician. I shall describe the underlying concepts and problems, the attempts to understand and solve them, and some of the research directions this led us to. I shall explain some of the important results, as well as the major goals and conjectures which still elude us. All this will hopefully give a taste of the motivations, richness and interconnectedness of our field. I shall conclude with a few *non computational* problems, which capture $\mathcal{P}$ vs. $\mathcal{NP}$ and related computational complexity problems, hopefully inviting more mathematicians to attack them as well.

I believe it important to give many examples, and to underlie the intuition (and sometimes, philosophy) behind definitions and results. This may slow the pace of this article for some, in the hope to make it clearer to others.

Mathematics Subject Classification (2000). Primary 68Q15; Secondary 68Q17.

Keywords. $\mathcal{P}$, $\mathcal{NP}$, computational complexity.

1. Prelude: computation, undecidability and the limits of mathematical knowledge

Which mathematical structures can we hope to understand? Let us focus on the most basic mathematical task of classification[1]. We are interested in a particular class of objects, and a particular property. We seek to *understand* which of the objects have the property and which do not. Examples include

[1] This context will be general enough to be interesting and possible ramifications to other mathematical tasks are typically clear.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

(1) Which Diophantine equations have solutions?

(2) Which knots are unknotted?

(3) Which dynamical systems are chaotic?

(4) Which theorems are provable in Peano arithmetic?

(5) Which pairs of manifolds are diffeomorphic?

(6) Which elementary statements about the Reals are true?

(7) Which elliptic curves are modular?

A central question is what do we mean by *understanding*. When are we satisfied that our classification problem was reasonably solved? Are there problems like this which we can never solve? A central observation (popularized mainly by Hilbert) is that "satisfactory" solutions usually provide (explicitly or implicitly) procedures, which when applied to an object, determine (in finite time) if it has the property or not. Hilbert's problems (1) and (4) above were stated, it seems, with expectation that the answer would be positive, namely that mathematicians would be able to understand them in this sense.

The breakthrough developments in the 1930s, by Gödel, Turing, Church and others led to the formal definition of an *algorithm*. This development, aside from enabling the computer revolution, made mathematically precise what Hilbert meant by a "mechanical procedure". With it, precise theorems could be proved on the limits of our knowledge; it led to proofs that some basic mathematical problems, like (1) and (4) above will never be understood in this sense. There cannot be any *decision procedure* (an algorithm which always halts) to discern provable from unprovable statements in number theory (this was shown independently by Turing and Church), or to discern solvable from unsolvable Diophantine equations (by Davis, Putnam, Robinson and Mattiasevich). These classification problems are *undecidable*.

The crucial ingredient in those (and all other undecidability) results, is showing that each of these mathematical structures can *encode computation*. This is known today to hold for many different structures in algebra, topology, geometry, analysis, logic, and more, even though apriori the structures studied seem to be completely unrelated to computation. This ubiquity makes every mathematician a potential computer scientist in disguise. We shall return to refined versions of this idea later.

Naturally, such negative results did not stop mathematical work on these structures and properties – it merely focused the necessity to understanding interesting subclasses of the given objects. Specific classes of Diophantine equations were understood much better, e.g. Fermat's Last Theorem and the resolution of problem (7). The same holds for restricted logics for number theory, e.g. Presburger arithmetic.

The notion of a decision procedure as a minimal requirement for understanding of a mathematical problem has also led to direct positive results. It suggests that we look

for a decision procedure as *a means*, or as *first step* for understanding a problem. Thus Haken [50] showed how knots can be so understood, with his decision procedure for problem (2), and Tarski [108] showed that real-closed fields can be understood with decision procedure for problem (6). Naturally, significant *mathematical, structural* understanding was needed to develop these algorithms. Haken developed the theory of *normal surfaces*, and Tarski invented *quantifier elimination*, for their algorithms, both cornerstones of the respective fields. This only reveals the obvious: mathematical and algorithmic understanding are related and often go hand in hand. And what was true in previous centuries is truer in this one – the language of algorithms is slowly becoming competitive with the language of equations and formulas (which are special cases of algorithms) for explaining complex mathematical structures[2].

Now that we have seen algorithmic mathematical understanding *in principle*, it is natural to go beyond and try to quantify that level of understanding. Again, we would use a computational yardstick for it. We argue that better mathematical understanding goes hand in hand with better algorithms for "obtaining" that understanding from the given structures. To formalize it, we shall start introducing the computational terms that are central to the theory of computational complexity.

2. The computational complexity of classification (and other) problems

In this section we shall develop the basic notions of data representation, efficient computations, efficient reductions between problems, efficient verification of proofs, the classes, $\mathcal{P}$, $\mathcal{NP}$, co$\mathcal{NP}$ and $\mathcal{NP}$-complete problems. We shall focus on time (= number of elementary operations[3] performed) as the primary resource of algorithms, when studying their efficiency. Other resources, such as memory, parallelism and more are studied in computational complexity, but we will not treat them here.

2.1. A motivating example. Let us consider the following two classification problems.

(1′) Which Diophantine equations of the form $Ax^2 + By + C = 0$ are solvable by *positive* integers?

(2′) Which knots on 3-dimensional manifolds bound a surface of genus $\leq g$?

Problem (1′) is a restriction of problem (1) above. Problem (1) was undecidable, and it is natural to try to understand more restricted classes of Diophantine equations. Problem (2′) is a generalization of problem (2) above in two ways (the case of genus $g = 0$ corresponds to the knot being unknotted, and we are not restricted to knots in $\mathbb{R}^3$). Problem (2) was decidable, and we may want to understand (2′) even better.

[2] An early familiar example is Galois' proof that roots of real polynomials of degree at least 5 have no *formula* with radicals, contrasted with Newton's *algorithm* for approximating such roots.

[3] Each acting on fixed amount of data (e.g. 10 digits).

At any rate, most mathematicians would tend to agree that problems $(1')$ and $(2')$ have absolutely nothing to do with each other. They are from very different fields, with completely different notions, goals and tools. However, the theorem below suggests that this view may be wrong.

Theorem 2.1. *Problems* $(1')$ *and* $(2')$ *are* equivalent.

Moreover, the equivalence notion is natural and completely formal. Intuitively, any understanding we have of one problem, can be *simply* translated into a similar understanding of the other. The formal meaning will unfold in Subsection 2.10. To get there we need to develop the language and machinery which yield such surprising results. We start with formally defining the (finite!) representation of objects in both problems, and in general.

Consider the set of all equations of the form $Ax^2 + By + C = 0$ with integer coefficients A, B, C. A finite representation of such equation is obvious – the triple of coefficients (A, B, C). Given such a triple – does the corresponding polynomial has a positive integer root (x, y)? Let $2DIO$ denote the subset of triples for which the answer is YES.

Finite representation of inputs to problem $(2')$ is a bit more tricky, but still natural. The inputs consist of a 3-dimensional manifold M, a knot K embedded on it, and an integer G. A finite representation can describe M by a triangulation (finite collection of tetrahedra and their adjacencies). The knot K will be described as a link (closed path) along edges of the given tetrahedra. Given a triple (M, K, G), does the surface that K bounds have genus at most G? Let $KNOT$ denote the subset for which the answer is YES.

Any finite object (integers, tuples of integers, finite graphs, finite complexes, etc.)[4] can be represented naturally by binary sequences (say over the alphabet $\{0, 1\}$). Indeed, this encoding can be done such that going back and forth between the object and its representation is simple and efficient (a notion to be formally defined below). Consequently, we let I denote the set of all finite binary sequences, and regard it as the set of inputs to all our classification problems. In this language, given a binary sequence $x \in \mathrm{I}$ we may interpret it as a triple of integers (A, B, C) and ask if the related equation is in $2DIO$. This is problem $(1')$. We can also interpret x as a triple (M, K, G) of manifold, knot and integer, and ask if it is in the set $KNOT$. This is problem $(2')$.

Theorem 2.1 states that there are *simple* translations (in both directions) between solving problem $(1')$ and problem $(2')$. More precisely, it provides functions $f, h : \mathrm{I} \to \mathrm{I}$ performing these translations:

$(A, B, C) \in 2DIO$ iff $f(A, B, C) \in KNOT$,

and

$(M, K, G) \in KNOT$ iff $h(M, K, G) \in 2DIO$.

[4] A theory of algorithms which directly operate on real or complex numbers is developed in [16], which has natural parallels to some of the notions and results we shall meet.

So, if we have gained enough understanding of topology to solve e.g. the knot genus problem, it means that we automatically have gained enough number theoretic understanding for solving these quadratic Diophantine problems (and vice versa).

The translating functions f and h are called *reductions*. We capture the *simplicity* of a reduction in *computational* terms. We demand that it will be *efficiently* computable. This is what we define next.

2.2. Efficient computation and the class $\mathcal{P}$. In all that follows, we focus on asymptotic complexity. Thus e.g. we care neither about the time it takes to factor the number $2^{67} - 1$ (as much as Mersenne cared about it), nor about the time it takes to factor all 67-bit numbers, but rather about the asymptotic behavior of factoring n-bit numbers, as a function of the input length n. The asymptotic viewpoint is inherent to computational complexity theory, and we shall see in this article that it reveals structure which would be obscured by finite, precise analysis.

Efficient computation (for a given problem) will be taken to be one whose runtime on any input of length n is bounded by a *polynomial* function in n. Let I_n denote all binary sequences in I of length n.

Definition 2.2 (The class $\mathcal{P}$). A function $f : \mathrm{I} \to \mathrm{I}$ is in the class $\mathcal{P}$ if there is an algorithm computing f and positive constants A, c, such that for every n and every $x \in \mathrm{I}_n$ the algorithm computes $f(x)$ in at most An^c steps.

Note that the definition applies in particular to Boolean functions (whose output is $\{0, 1\}$) which capture classification problems. We will abuse notation and sometimes think of $\mathcal{P}$ as the class containing *only* these classification problems. Observe that a function with a long output can be viewed as a sequence of Boolean functions, one for each output bit.

This definition was suggested by Cobham [23], Edmonds [32] and Rabin [86], all attempting to formally delineate *efficient* from just finite (in their cases, exponential time) algorithms. Of course, nontrivial polynomial time algorithms were discovered earlier, long before the computer age. Many were discovered by mathematicians, who needed efficient methods to calculate (by hand). The most ancient and famous example is of course Euclid's GCD algorithm, which bypasses the factorization of the inputs when computing their common factor.

Why polynomial? The choice of polynomial time to represent efficient computation seems arbitrary, and indeed different possible choices can be made[5]. However, this particular choice has justified itself over time from many points of view. We list some important ones.

Polynomials typify "slowly growing" functions. The closure of polynomials under addition, multiplication and composition preserves the notion of efficiency under natural programming practices, such as using two programs in sequence, or using one as a subroutine of another. This choice removes the necessity to describe the

[5] and indeed were made and studied in computational complexity.

computational model precisely (e.g. it does not matter if we allow arithmetic operations only on single digits or on arbitrary integers, since long addition, subtraction, multiplication and division have simple polynomial time algorithms taught in grade school). Similarly, we need not worry about data representation: one can efficiently translate between essentially any two natural representations of a set of finite objects.

From a practical viewpoint, while a running time of, say, n^2 is far more desirable than n^{100}, very few known efficient algorithms for natural problems have exponents above 3 or 4. On the other hand, many important natural problems which so far resist efficient algorithms, cannot at present be solved faster than in *exponential* time. Thus reducing their complexity to (any) polynomial will be a huge conceptual improvement.

The importance of understanding the class $\mathcal{P}$ is obvious. There are numerous computational problems that arise (in theory and practice) which demand efficient solutions. Many algorithmic techniques were developed in the past 4 decades and enable solving many of these problems (see e.g. the textbook [27]). These drive the ultra-fast home computer applications we now take for granted like web searching, spell checking, data processing, computer game graphics and fast arithmetic, as well as heavier duty programs used across industry, business, math and science. But many more problems yet (some of which we shall meet soon), perhaps of higher practical and theoretical value, remain elusive. The challenge of *characterizing* this fundamental mathematical object – the class $\mathcal{P}$ of efficiently solvable problems – is far beyond us at this point.

We end this section with a few examples of nontrivial problems in $\mathcal{P}$ of mathematical significance. In each the interplay of mathematical and computational understanding needed for the development of these algorithms is evident.

- **Primality testing.** Given an integer, determine if it is prime. Gauss literally challenged the mathematical community to find an efficient algorithm, but it took two centuries to resolve. The story of this recent achievement of [3] and its history are beautifully recounted in [46].

- **Linear programming.** Given a set of linear inequalities in many variables, determine if they are mutually consistent. This problem, and its optimization version, capture numerous others (finding optimal strategies of a zero-sum game is one) and the convex optimization techniques used to give the efficient algorithms [68], [65] for it do much more (see e.g. the books [97].)

- **Factoring polynomials.** Given a multivariate polynomial with *rational* coefficients, find its irreducible factors over $\mathbb{Q}$. Again, the tools developed in [73] (mainly regarding "short" bases in lattices in $\mathbb{R}^n$) have numerous other applications.

- **Hereditary graph properties.** Given a finite graph, test if it can be embedded on a fixed surface (like the plane or the torus). A vastly more general result is known, namely testing *any* hereditary property (one which closed under vertex

removal and edge contraction). It follows the monumental structure theory [94] of such properties, including a *finite basis theorem*. and its algorithmic versions.

- **Hyperbolic word problem.** Given any presentation of a hyperbolic group by generators and relations, and a word w in the generators, does w represent the identity element. The techniques give isoperimetric bounds on the Cayley graphs of such groups and more [47].

2.3. Efficient verification and the class $\mathcal{NP}$. Let $C \subset \mathrm{I}$ be a classification problem. We are given an input $x \in \mathrm{I}$ (describing a mathematical object) and are supposed to determine if $x \in C$ or not. It is convenient for this section to view C as defining a property; $x \in C$ are objects having the property, and $x \notin C$ are objects which do not. If we have an efficient algorithm for C, we simply apply it to x. But if we do not, what is the next best thing? One answer is, a *convincing proof* that $x \in C$. Before defining it formally, let us see a couple of motivating examples.

The first example is famous anecdote of a lecture by F. N. Cole, entitled "On the Factorization of Large Numbers", at the 1903 AMS meeting. Without uttering a word, he went to the blackboard, wrote

$$2^{67} - 1 = 147573952589676412927 = 193707721 \times 761838257287$$

and proceeded to perform the long multiplication of the integers on the right hand side to derive the integer on the left: Mersenne's 67th number (which was conjectured to be prime). No one in the audience had any questions.

What has happened there? Cole demonstrated that the number $2^{67}-1$ is *composite*. Indeed, we can see that such a short proof can be given for any (correct) claim of the form $x \in \mathit{COMPOSITES}$, with *COMPOSITES* denoting the set of composite numbers. The proof is simply a nontrivial factor of x. The features we want to extract from this episode are two: The proofs are *short* and *easily verifiable*. The fact that it was extremely hard for Cole to find these factors (he said it took him "three years of Sundays") did not affect in any way that demonstration.

A second example, which we meet daily, is what happens when we read a typical math journal paper. In it, we typically find a (claimed) theorem, followed by an (alleged) proof. Thus, we are verifying claims of the type $x \in \mathit{THEOREMS}$, where *THEOREMS* is the set of all provable statements in, say, set theory. It is taken for granted that the written proof is *short* (page limit) and *easily verifiable* (otherwise the referee/editor would demand clarifications), regardless how long it took to discover.

The class $\mathcal{NP}$ contains all properties C for which membership (namely statements of the form $x \in C$) have *short, efficiently verifiable* proofs. As before, we use polynomials to define both terms. A candidate proof y for the claim $x \in C$ must have length at most polynomial in the length of x. And the verification that y indeed proves this claim must be checkable in polynomial time. Finally, if $x \notin C$, no such y should exist.

Definition 2.3 (The class $\mathcal{NP}$). The set C is in the class $\mathcal{NP}$ if there is a function $V_C \in \mathcal{P}$ and a constant k such that

- If $x \in C$ then $\exists y$ with $|y| \leq |x|^k$ and $V_C(x, y) = 1$.
- If $x \notin C$ then $\forall y$ we have $V_C(x, y) = 0$.

Thus each set C in $\mathcal{NP}$ may be viewed as a set of theorems in the complete and sound proof system defined by the verification process V_C.

A sequence y which "convinces" V_C that $x \in C$ is often called a *witness* or *certificate* for the membership of x in C. Again, we stress that the definition of $\mathcal{NP}$ is not concerned with how difficult it is to come up with a witness y. Indeed, the acronym $\mathcal{NP}$ stands for "nondeterministic polynomial time", where the nondeterminism captures the ability of a *hypothetical* "nondeterministic" machine to "guess" a witness y (if one exists), and then verify it deterministically.

Nonetheless, the complexity of finding a witness is of course important, as it captures the *search problem* associated to $\mathcal{NP}$ sets. Every decision problem C (indeed every verifier V_C for C) in $\mathcal{NP}$ comes with a natural search problem associated to it: Given $x \in C$, *find* a short witness y that "convinces" V_C. A correct solution to this search problem can be easily verified by V_C.

While it is usually the search problems which occupy us, from a computational standpoint it is often more convenient to study the decision versions. Almost always both versions are equivalent[6].

These definitions of $\mathcal{NP}$ were first given (independently and in slightly different forms) by Cook [24] and Levin [74]. There is much more to these seminal papers than this definition, and we shall discuss it later at length.

It is evident that decision problems in $\mathcal{P}$ are also in $\mathcal{NP}$. The verifier V_C is simply taken to be the efficient algorithm for C, and the witness y can be the empty sequence.

Corollary 2.4. $\mathcal{P} \subseteq \mathcal{NP}$.

A final comment is that problems in $\mathcal{NP}$ have trivial *exponential time* algorithms. Such algorithms search through all possible short witnesses, and try to verify each. Can we always speed up this brute-force algorithm?

2.4. The $\mathcal{P}$ vs. $\mathcal{NP}$ question, its meaning and importance. The class $\mathcal{NP}$ is extremely rich (we shall see examples a little later). There are literally thousands of $\mathcal{NP}$ problems in mathematics, optimization, artificial intelligence, biology, physics, economics, industry and more which arise naturally out of different necessities, and whose efficient solutions will benefit us in numerous ways. They beg for efficient algorithms, but decades (and sometimes longer) of effort has only succeeded for a few.

[6] A notable possible exception is the set *COMPOSITES* and the suggested verification procedure to it, accepting as witness a nontrivial factor. Note that while *COMPOSITES* $\in \mathcal{P}$ as a decision problem, the related search problem is equivalent to Integer Factorization, which is not known to have an efficient algorithm.

Is it possible that *all* sets in $\mathcal{NP}$ possess efficient algorithms, and these simply were not discovered yet? This is the celebrated $\mathcal{P}$ vs. $\mathcal{NP}$ question. It appeared explicitly first in the aforementioned papers of Cook and Levin, but had some informal precursors. Of particular interest is a remarkable letter written by Gödel to von Neumann about 15 years earlier which raises this fundamental question quite clearly, and shows how aware Gödel was of its significance (see the surveys [102], [51] for the original letter and translation, as well as much more on the subject at hand).

Open Problem 2.5. Is $\mathcal{P} = \mathcal{NP}$?

What explains the abundance of so many natural, important problems in the class $\mathcal{NP}$? Probing the intuitive meaning of the definition of $\mathcal{NP}$, we see that it captures many tasks of human endeavor *for which a successful completion can be easily recognized*. Consider the following professions, and the typical tasks they are facing (this will be extremely superficial, but nevertheless instructive):

- **Mathematician:** Given a mathematical claim, come up with a proof for it.
- **Scientist:** Given a collection of data on some phenomena, find a theory explaining it.
- **Engineer:** Given a set of constraints (on cost, physical laws, etc.) come up with a design (of an engine, bridge, laptop …) which meets these constraints.
- **Detective:** Given the crime scene, find "who's done it".

What is common to all this multitude of tasks is that we can typically tell a good solution when we see one (or we at least think we can). In various cases "we" may be the academic community, the customers, or the jury, but we expect the solution to be *short*, and *efficiently verifiable*, just as in the definition of $\mathcal{NP}$.

The richness of $\mathcal{NP}$ follows from the simple fact that such tasks abound, and their mathematical formulation is indeed an $\mathcal{NP}$-problem. For all these tasks, efficiency is paramount, and so the importance of the $\mathcal{P}$ vs. $\mathcal{NP}$ problem is evident. The colossal implications of the possibility that $\mathcal{P} = \mathcal{NP}$ are evident as well – every instance of these tasks can be solved, optimally and efficiently.

One (psychological) reason people feel that $\mathcal{P} = \mathcal{NP}$ is unlikely, is that tasks as above often require a degree of *creativity* which we do not expect a simple computer program to have. We admire Wiles' proof of Fermat's Last Theorem, the scientific theories of Newton, Einstein, Darwin, Watson and Crick, the design of the Golden Gate bridge and the Pyramids, and sometimes even Hercule Poirot's and Miss Marple's analysis of a murder, precisely because they seem to require a leap which cannot be made by everyone, let alone a by simple mechanical device. My own view is that when we finally understand the algorithmic processes of the brain, we may indeed be able automate the discovery of these specific achievements, and perhaps many others. But can we automate them *all*? Is it possible that *every* task for which verification

is easy, finding a solution is not much harder? If $\mathcal{P} = \mathcal{NP}$, the answer is positive, and creativity (of this abundant, verifiable kind) can be completely automated. Most computer scientists believe that this is not the case.

Conjecture 2.6. $\mathcal{P} \neq \mathcal{NP}$.

Back to mathematics! Given the discussion above, one may wonder why it is so hard to prove that indeed $\mathcal{P} \neq \mathcal{NP}$ – it seems completely obvious. We shall discuss attempts and difficulties soon, developing a methodology which will enable us to identify the *hardest* problems in $\mathcal{NP}$. But before that, we turn to discuss a related question with a strong relation to mathematics: the $\mathcal{NP}$ versus co$\mathcal{NP}$ question.

2.5. The $\mathcal{NP}$ versus co$\mathcal{NP}$ question, its meaning and importance. Fix a property $C \subseteq \mathrm{I}$. We already have the interpretations

- $C \in \mathcal{P}$ if it is easy to check that object x has property C,
- $C \in \mathcal{NP}$ if it is easy to certify that object x has property C,

to which we now add

- $C \in \mathrm{co}\mathcal{NP}$ if it is easy to certify that object x *does not have* property C,

where we formally define

Definition 2.7 (The class co$\mathcal{NP}$). A set C is in the class co$\mathcal{NP}$ iff its complement $\overline{C} = \mathrm{I} \setminus C$ is in $\mathcal{NP}$.

While the definition of the class $\mathcal{P}$ is symmetric[7], the definition of the class $\mathcal{NP}$ is asymmetric. Having nice certificates that a given object has property C, does not automatically entail having nice certificates that a given object does not have it.

Indeed, when we can do both, we are achieving a mathematics' holy grail of understanding structure, namely *necessary and sufficient* conditions, sometimes phrased as a *duality theorem*. As we know well, such results are rare. When we insist (as we shall do) that the given certificates are *short, efficiently verifiable* ones, they are even rarer. This leads to the conjecture

Conjecture 2.8. $\mathcal{NP} \neq \mathrm{co}\mathcal{NP}$.

First note that this conjecture implies $\mathcal{P} \neq \mathcal{NP}$. We shall discuss at length refinements of this conjecture in Section 4 on proof complexity.

Despite the shortage of such efficient complete characterizations, namely properties which are simultaneously in $\mathcal{NP} \cap \mathrm{co}\mathcal{NP}$, they nontrivially exist. Here is a list of some exemplary ones.

[7] Having a fast algorithm to determine if an object has a property C is equivalent to having a fast algorithm for the complementary set $\overline{C}$.

- **Linear programming.** Systems of consistent linear inequalities.[8]

- **Zero-sum games**[9]**.** Finite zero-sum games in which one player can gain at least (some given value) v.

- **Graph connectivity.** The set of graphs in which *every* pair of vertices is connected by (a given number) k disjoint paths.

- **Partial order width.** Finite partial orders whose largest anti-chain has at most (a given number) w elements.

- **Primes.** Prime numbers.

These examples of problems in $\mathcal{NP} \cap \text{co}\mathcal{NP}$ were chosen to make a point. At the time of their discovery (by Farkas, von Neumann, Menger, Dilworth, and Pratt respectively) these mathematicians were seemingly interested only in characterizing these structures. It is not known if they attempted to find efficient algorithms for these problems. However all of these problems turned out to be in $\mathcal{P}$, with some solutions entering the pantheon of efficient algorithms (e.g. the Ellipsoid method of Khachian [68] and the Interior-Point method of Karmarkar [65], both for Linear Programming, and the recent breakthrough of Agrawal, Kayal and Saxena [3] for Primes[10].

Is there a moral to this story? Only that sometimes, when we have an efficient characterization of structure, we can hope for more – efficient algorithms. And conversely, a natural stepping stone towards an elusive efficient algorithm may be to first get an efficient characterization.

Can we expect this magic to always happen? Is $\mathcal{NP} \cap \text{co}\mathcal{NP} = \mathcal{P}$? At the end of Subsection 2.11 we shall see another list of problems in $\mathcal{NP} \cap \text{co}\mathcal{NP}$ which have resisted efficient algorithms for decades, and for some (e.g. factoring integers), humanity literally banks on their difficulty for electronic commerce security. Indeed, the following is generally believed:

Conjecture 2.9. $\mathcal{NP} \cap \text{co}\mathcal{NP} \neq \mathcal{P}$.

Note again that this conjecture 2.9 implies $\mathcal{P} \neq \mathcal{NP}$, but that it is independent of conjecture 2.8.

We now return to develop the main mechanism which will help us study such questions: efficient reductions.

[8] Indeed this generalizes to other convex bodies given by more general constraints, like *semi-definite* programming.

[9] This problem was later discovered to be equivalent to linear programming.

[10] It is interesting that assuming the Extended Riemann Hypothesis, a simple polynomial time algorithm was given 30 years earlier by Miller [78].

2.6. Reductions – a partial order of computational difficulty. In this subsection we deal with relating the computational difficulty of problems for which we have no efficient solutions (yet).

Recall that we can regard any classification problem (on finitely described objects) as a subset of our set of inputs I. Efficient reductions provide a natural partial order on such problems, that capture their relative difficulty.

Definition 2.10 (Efficient reductions). Let $C, D \subset \mathrm{I}$ be two classification problems. $f : \mathrm{I} \to \mathrm{I}$ is an efficient reduction from C to D if $f \in \mathcal{P}$ and for every $x \in \mathrm{I}$ we have $x \in C$ iff $f(x) \in D$. In this case we call f an *efficient reduction* from C to D. We write $C \leq D$ if there is an efficient reduction from C to D.

The definition of efficient computation allows two immediate observations on the usefulness of efficient reductions. First, that indeed $\leq$ is transitive, and thus defines a partial order. Second, that if $C \leq D$ and $D \in \mathcal{P}$ then also $C \in \mathcal{P}$.

Formally, $C \leq D$ means that solving the classification problem C is *computationally* not much harder than solving D. In some cases one can replace *computationally* by the (vague) term *mathematically*. Often such usefulness in mathematical understanding requires more properties of the reduction f than merely being efficiently computable (e.g. we may want it to be represented as a linear transformation, or a low dimension polynomial map), and indeed in some cases this is possible. When such a connection between two classification problems (which look unrelated) can be proved, it can mean the importability of techniques from one area to another.

The power of efficient reductions to relate "seemingly unrelated" notions will unfold in later sections. We shall see that they can relate not only classification problems, but such diverse concepts as hardness to randomness, average-case to worst case difficulty, proof length to computation time, the relative power of geometric, algebraic and logical proof systems, and last but not least, the security of electronic transactions to the difficulty of factoring integers. In a sense, *efficient reductions are the backbone of computational complexity*. Indeed, given that polynomial time reductions can do all these wonders, no wonder we have a hard time characterizing the class $\mathcal{P}$!

2.7. Completeness. We now return to classification problems. The partial order of their difficulty, provided by efficient reductions, allows us to define the *hardest* problems in a given class. Let $\mathcal{C}$ be any collection of classification problems (namely every element of $\mathcal{C}$ is a subset of I). Of course, here we shall mainly care about the class $\mathcal{C} = \mathcal{NP}$.

Definition 2.11 (Hardness and completeness). A problem D is called $\mathcal{C}$*-hard* if for every $C \in \mathcal{C}$ we have $C \leq D$. If we further have that $D \in \mathcal{C}$ then D is called $\mathcal{C}$*-complete*.

In other words, if D is $\mathcal{C}$-complete, it is a hardest problem in the class $\mathcal{C}$: if we manage to solve D efficiently, we have done so for all other problems in $\mathcal{C}$. It is not

apriori clear that a given class has any complete problems! On the other hand, a given class may have many complete problems, and by definition, they all have essentially the same complexity. If we manage to prove that *any* of them cannot be efficiently solved, then we automatically have done so for *all* of them.

It is trivial, and uninteresting, that every problem in the class $\mathcal{P}$ is in fact $\mathcal{P}$-complete under our definition. It becomes interesting when we find such universal problems in classes of problems for which we do not have efficient algorithms. By far, the most important of all classes is $\mathcal{NP}$.

2.8. $\mathcal{NP}$-completeness. As mentioned earlier, the seminal papers of Cook [24] and Levin [74] defined $\mathcal{NP}$, efficient reducibilities and completeness, but the crown of their achievement was the discovery of a *natural* $\mathcal{NP}$-complete problem.

Definition 2.12 (The problem *SAT*). A Boolean formula is a logical expression over Boolean variables (that can take values in $\{0, 1\}$) with connectives $\wedge$, $\vee$, $\neg$, e.g. $(x_1 \vee x_2) \wedge (\neg x_3)$. Let *SAT* denote the set of all satisfiable Boolean formulae (namely those formulae for which there is a Boolean assignment to the variables which gives it the value 1).

Theorem 2.13 ([24], [74]). *SAT is $\mathcal{NP}$-complete.*

We recall again the meaning of that statement. For *every* set $C \in \mathcal{NP}$ there is an efficient reduction $f : \mathrm{I} \to \mathrm{I}$ such that $x \in C$ iff the formula $f(x)$ is satisfiable! Furthermore, the proof gives an extra bonus which turns out to be extremely useful: given any witness y that $x \in C$ (via some verifier V_C), the same reduction converts the witness y to a Boolean assignment satisfying the formula $f(x)$. In other words, this reduction translates not only between the decision problems, but also between the associated search problems.

You might (justly) wonder how can one prove a theorem like that. Certainly the proof cannot afford to look at all problems $C \in \mathcal{NP}$ separately. The gist of the proof is a generic transformation, taking a description of the verifier V_C for C, and emulating its computation on input x and hypothetical witness y to create a Boolean formula $f(x)$ (whose variables are the bits of y). This formula simply tests the validity of the computation of V_C on (x, y), and that this computation outputs 1. Here the locality of algorithms (say described as Turing machines) plays a central role, as checking the consistency of each step of the computation of V_C amounts simply to a constant size formula on a few bits. To summarize, *SAT* captures the difficulty of the whole class $\mathcal{NP}$. In particular, the $\mathcal{P}$ vs. $\mathcal{NP}$ problem can now be phrased as a question about the complexity of *one* problem, instead of infinitely many.

Corollary 2.14. *$\mathcal{P} = \mathcal{NP}$ iff $SAT \in \mathcal{P}$.*

A great advantage of having one complete problem at hand (like *SAT*), is that now, to prove that another problem (say $D \in \mathcal{NP}$) is $\mathcal{NP}$-complete, we only need to

design a reduction from *SAT* to D (namely prove $SAT \leq D$). We already know that for *every* $C \in \mathcal{NP}$ we have $C \leq SAT$, and transitivity of $\leq$ takes care of the rest.

This idea was used powerfully in the next seminal paper, of Karp [66]. In his paper, he listed 21 problems from logic, graph theory, scheduling and geometry which are $\mathcal{NP}$-complete. This was the first demonstration of the wide spectrum of $\mathcal{NP}$-complete problems, and initiated an industry of finding more. A few years later Gary and Johnson [36] published their book on $\mathcal{NP}$-completeness, which contains hundreds of such problems from diverse branches of science, engineering and mathematics. Today thousands are known.

2.9. The nature and impact of $\mathcal{NP}$-completeness. It is hard to do justice to this notion in a couple of paragraphs, but we shall try. More can be found e.g. in [83].

$\mathcal{NP}$-completeness is a unique scientific discovery – there seems to be no parallel scientific notion which so pervaded so many fields of science and technology. It became a standard for hardness for problems whose difficulty we have yet no means of proving. It has been used both technically and allegorically to illustrate a difficulty or failure to understand natural objects and phenomena. Consequently, it has been used as a justification for channeling effort in less ambitious (but more productive) directions. We elaborate below on this effect within mathematics.

$\mathcal{NP}$-completeness has been an extremely flexible and extendible notion, allowing numerous variants which enabled capturing universality in other (mainly computational, but not only) contexts. It led to the ability of defining whole classes of problems by single, universal ones, with the benefits mentioned above. Much of the whole evolution of computational complexity, the theory of algorithms and most other areas in theoretical computer science have been guided by the powerful approach of reduction and completeness.

It would be extremely interesting to explain the ubiquity of $\mathcal{NP}$-completeness. Being highly speculative for a moment, we can make the following analogies of its mystery with physics. The existence of $\mathcal{NP}$-completeness in such diverse fields of inquiry may be likened to the existence of the same building blocks of matter in remote galaxies, begging for a common explanation of the same nature as the *big bang* theory. We later discuss the near lack of natural objects in the (seemingly huge) void of problems in $\mathcal{NP}$ which are neither in $\mathcal{P}$ nor $\mathcal{NP}$-complete. This raises wonders about possible "dark matter", which we have not developed the means of observing yet.

2.10. Some $\mathcal{NP}$-complete problems. Again, we note that all $\mathcal{NP}$-complete problems are equivalent in a very strong sense. Any algorithm solving one can be simply translated into an equally efficient algorithm solving any other. We can finally see the proof of Theorem 2.1 from the beginning of this section. It follows from the following two theorems.

Theorem 2.15 ([1]). *The set* 2*DIO is* $\mathcal{NP}$*-complete.*

Theorem 2.16 ([2]). *The set KNOT is* $\mathcal{NP}$*-complete.*

Recall that to prove $\mathcal{NP}$-completeness of a set, one has to prove two things: that it is in $\mathcal{NP}$, and that it is $\mathcal{NP}$-hard. In almost all $\mathcal{NP}$-complete problems, membership in $\mathcal{NP}$ (namely the existence of short certificates) is easy to prove. E.g. for $2DIO$ one can easily see that if there is a positive integer solution to $Ax^2 + By + C = 0$ then indeed there is one whose length (in bits) is polynomial in the lengths of A, B, C and so a short witness is simply a root. But *KNOT* is an exception, and the short witnesses for the knot having a small genus requires Haken's algorithmic theory of normal surfaces, considerably enhanced (even short certificates for unknottedness in $\mathbb{R}^3$ are hard to obtain, see [53]). Let us discuss what these $\mathcal{NP}$-completeness results mean, first about the relationship between the two, and then about each individually.

The proofs that these problems are complete both follow by reductions from (variants of) *SAT*. The combinatorial nature of these reductions may put doubt into the possibility that the computational equivalence of these two problems implies the ability of real "technology transfer" between topology and number theory. Nevertheless, now that we know of the equivalence, perhaps simpler and more direct reductions can be found between these problems. Moreover, we stress again that for any instance, say $(M, K, G) \in KNOT$, if we translate it using this reduction to an instance $(A, B, C) \in 2DIO$ and happen (either by sheer luck or special structure of that equation) to find an integer root, the same reduction will translate that root back to a description of a genus G manifold which bounds the knot K. Today many such $\mathcal{NP}$-complete problems are known throughout mathematics, and for some pairs the equivalence can be mathematically meaningful and useful (as it is between some pairs of computational problems).

But regardless of the meaning of the connection between these two problems, there is no doubt what their individual $\mathcal{NP}$-completeness means. Both are mathematically "nasty", as both embed in them the full power of $\mathcal{NP}$. If $\mathcal{P} \neq \mathcal{NP}$, there are no efficient algorithms to describe the objects at hand. Moreover, assuming the stronger $\mathcal{NP} \neq \text{co}\mathcal{NP}$, we should not even expect complete characterization (e.g. above we should not expect short certificates that a given quadratic equation *does not* have an positive integer root).

In short, $\mathcal{NP}$-completeness suggests that we lower our expectations of fully understanding these properties, and study perhaps important special cases, variants etc. Note that such reaction of mathematicians may anyway follow the frustration of unsuccessful attempts at general understanding. However, the stamp of $\mathcal{NP}$-completeness *may* serve as moral justification for this reaction. We stress the word *may*, as the judges for accepting such a stamp can only be the mathematicians working on the problem, and how well the associated $\mathcal{NP}$-completeness result captures the structure they try to reveal. We merely point out the usefulness of a formal stamp of difficulty (as opposed to a general feeling), and its algorithmic meaning.

We now list a few more $\mathcal{NP}$-complete problems of different nature, to give a feeling for the breadth of this phenomena. Some appear already in Karp's original article [66]. Again, hundreds more can be found in [36].

- **3Color.** Given a graph, can its vertices be colored from {Red, Green, Blue} with no adjacent vertices receiving the same color?
- **Knapsack.** Given a sequence of integers $a_1, \ldots, a_n$ and b, decide if there exists a subset J such that $\sum_{i \in J} a_i = b$.
- **Integer programming.** Given a polytope in $\mathbb{R}^n$ (by its bounding hyperplanes), does it contain an integer point?
- **Clique.** Given a graph and an integer k, are there k vertices with all pairs mutually adjacent?
- **Quadratic equations.** Given a system of multivariate polynomial equations of degree at most 2, over a *finite field* (say GF(2)), do they have a common root?
- **Shortest lattice vector.** Given a lattice L in $\mathbb{R}^n$ and an integer k, is the shortest nonzero vector of L of (Euclidean) length $\leq k$?

2.11. Other problems in $\mathcal{NP}$ (and outside it). We have seen that $\mathcal{NP}$ contains a vast number of problems, but that difficulty-wise they seem to fall into two equivalence classes. $\mathcal{P}$, which are all efficiently solvable, and $\mathcal{NP}$-complete. Of course, if $\mathcal{P} = \mathcal{NP}$ the two classes are the same. But assuming $\mathcal{P} \neq \mathcal{NP}$, is there anything else? Ladner [71] proved the following result:

Theorem 2.17 ([71]). *If $\mathcal{P} \neq \mathcal{NP}$, then there are infinitely many levels of difficulty in $\mathcal{NP}$. More precisely, there are sets $C_1, C_2, \ldots$ in $\mathcal{NP}$ such that for all i we have $C_i \leq C_{i+1}$ but $C_{i+1} \not\leq C_i$.*

But are there *natural* problems which do not fall in the main two classes $\mathcal{P}$ and $\mathcal{NP}$-complete? We know only of very precious few: those on the list below, and a handful of others.

- **Integer factoring.** Given an integer, find its prime factors.
- **Approx shortest lattice vector.** Given a lattice L in $\mathbb{R}^n$ and an integer k, does the shortest vector of L has (Euclidean) length in the range $[k, kn]$.
- **Stochastic games.** White, Black and Nature alternate moving a token on the edges of directed graph. Nature's moves are random. Given a graph, a start and target nodes for the token, does White have a strategy which guarantees that the token reach the target with probability $\geq 1/2$?
- **Graph isomorphism.** Given two graphs, are they isomorphic? Namely, is there a bijection between their vertices which preserves the edges?

Clearly, we cannot rule out that efficient algorithms will be found for any of them. But we do know that the first three are in $\mathcal{NP} \cap \text{co}\mathcal{NP}$. Thus assuming $\mathcal{NP} \neq \text{co}\mathcal{NP}$

they cannot be $\mathcal{NP}$-complete! A similar conclusion holds for the fourth problem, which follows from the "interactive proof" for graph non-isomorphism in Section 6.

Finding other natural examples (or better yet, classes of examples) like these will enhance our understanding of the gap $\mathcal{NP} \setminus \mathcal{P}$. Considering the examples above, we expect that mathematics is a more likely source for them than, say, industry.

2.11.1. Average-case complexity and one-way functions. It is important to mention that the "worst-case" analysis we adopted throughout (looking at the time to solve the worst input of each length) is certainly not the only interesting complexity measure. Often "average-case" analysis, focusing on typical complexity, is far more interesting to study. After all, solving a hard problem most of the time may suffice in some applications. Algorithms for natural problems under natural input distributions is an important field. But typically the input distribution is unknown, and defining "average-case" complexity in a meaningful way is highly nontrivial. This was first done by Levin [75], and the reader can find more in [57], [38].

There are also situations where *hardness* on average is crucial, as is the case in cryptography[11]. This important field, which led to the enormous growth of electronic commerce, grew out of computational complexity, and relies on such computational assumptions. We now turn to explain the main one briefly, and recommend [39], [40] for much more.

The most basic primitive of modern cryptography is the *one-way* function, which was first defined in the seminal paper of Diffie and Hellman [29]. Intuitively, these are functions which are easy to compute (on every input) but are hard *on average* to invert. More precisely:

Definition 2.18 (One-way function). A function $f : \mathrm{I} \to \mathrm{I}$ is called *one-way* if $f \in \mathcal{P}$, but for any efficient algorithm A and every n,

$$\Pr[f(A(f(x)) = x] < 1/3$$

where the probability is taken over the uniform distribution of n-bit sequences.

It is not hard to see that decision versions of one-way functions are in $\mathcal{NP} \cap \mathrm{co}\mathcal{NP}$, and thus establishing their existence is harder than proving Conjecture 2.9. Thus cryptography postulates their existence.

Remarkably, only a handful of candidates are known today. The most popular are the multiplication of two primes (whose inverse is Integer Factorization), the exponentiation modulo a prime number (whose inverse is Discrete Logarithm)[12], and a certain linear operator (whose inverse gives the shortest vector in a lattice problem) [4]. We note also that [76] constructed a *complete* one-way function, namely a function which is one way if one-way functions exists at all.

[11] The fact that hardness is useful at all is a surprising fact, and we shall meet it again when discussing pseudorandomness.

[12] This problem has a variant over elliptic curves.

We conclude with noting that one-way functions suffice only for some problems in cryptography, and a seemingly more powerful primitive is the so called *trap-door function*. We recommend the article [57] which deals with the relative strength of such hardness assumptions discussed in this section, and the worlds they "imply". One basic problem is the following.

Open Problem 2.19. Does $\mathcal{P} \neq \mathcal{NP}$ imply that one-way functions exits?

2.11.2. Other types of computational problems. There are many other types of computational problems which arise naturally and do not fall into the class $\mathcal{NP}$. By far the most natural types are

- **Optimization problems.** Fix an $\mathcal{NP}$ problem, and a cost function on solutions (witnesses). Given an input, find the *best* solution for it (e.g find the largest clique, the shortest path, the minimum energy configuration, etc.).

- **Counting problems.** Fix an $\mathcal{NP}$ problem. Given an input, find the *number* of solutions (witnesses) for it. Many problems in enumerative combinatorics and in statistical physics fall in this category.

- **Strategic problems.** Given a game, find an optimal strategy for a player. Equivalently, given a position in the game, find the best move. Many problems in economics, decision theory as well as Chess and Go fall in this category.

- **Total functions.** Finding objects which are guaranteed to exist (like local optima, fixed points, Nash equilibria), usually by nonconstructive arguments [82].

We shall not elaborate on these families of important problems here. We only remark that the methodology of efficient reductions and completeness illuminate much of their computational complexity. They all fit in natural *complexity classes* like $\mathcal{NP}$, have complete problems, and are related in different ways to each other and to the $\mathcal{P}$ vs. $\mathcal{NP}$ problem.

3. Lower bounds, and attacks on $\mathcal{P}$ vs. $\mathcal{NP}$

To prove that $\mathcal{P} \neq \mathcal{NP}$ we must show that for a given problem, no efficient algorithm exists. A result of this type is called a *lower bound* (limiting from below the computational complexity of the problem). Several powerful techniques for proving lower bounds have emerged in the past decades. They apply in two (very different) settings. We now describe both, and try to explain our understanding of why they seem to stop short of proving $\mathcal{P} \neq \mathcal{NP}$. We only mention very briefly the first, diagonalization, and concentrate on the second, Boolean circuits.

3.1. Diagonalization and relativization. The diagonalization technique goes back to Cantor and his argument that there are more real numbers than algebraic numbers. It was used by Gödel in his Incompleteness Theorem, and by Turing in his undecidability results, and then refined to prove computational complexity lower bounds. A typical theorem in this area is that more time buys more computational power, e.g. there are functions computable in time n^3, say, which are not computable in time n^2. The heart of such arguments is the existence of a "universal algorithm", which can simulate every other algorithm with only small loss in efficiency.

Can such arguments be used to separate $\mathcal{P}$ from $\mathcal{NP}$? This depends on what we mean by "such arguments". The paper by Baker, Gill and Solovay [12] suggested a feature shared by many similar complexity results, called *relativization*, and then proceeded to show that relativizing arguments do not suffice to resolve the $\mathcal{P}$ vs. $\mathcal{NP}$ question. In the three decades since that paper complexity theory grew far more sophisticated, but nevertheless almost all new results obtained do relativize (one of the few exceptions is in [110]). However, a few exceptions in the areas of probabilistic proofs (e.g. Theorem 6.3) are known not to relativize, but these are essentially *upper bound* results. More on this subject can be found in Chapter 14.3 in [81], Chapter 9.2 of [101], and even more in [34].

3.2. Boolean circuits. A Boolean circuit may be viewed as the "hardware analog" of an algorithm (software). Computation on the binary input sequence proceeds by a sequence of Boolean operations (called *gates*) from the set $\{\wedge, \vee, \neg\}$ (logical AND, OR and NEGATION) to compute the output(s). We assume that $\wedge, \vee$ are applied to two arguments. We note that while an algorithm can handle inputs of any length, a circuit can only handle one input length (the number of input "wires" it has). A circuit is commonly represented as a (directed, acyclic) graph, with the assignments of gates to its internal vertices. We note that a Boolean formula is simply a circuit whose graph structure is a tree.

Recall that I denotes the set of all binary sequences, and that I_k is the set of sequences of length exactly k. If a circuit has n inputs and m outputs, it is clear that it computes a function $f : \mathrm{I}_n \to \mathrm{I}_m$. The efficiency of a circuit is measured by its *size*, which is the analog of time in algorithms.

Definition 3.1 (Circuit size). Denote by $\mathsf{S}(f)$ the size of the smallest Boolean circuit computing f.

As we care about asymptotic behavior, we shall be interested in sequences of functions $f = \{f_n\}$, where f_n is a function on n input bits. We shall study the complexity $\mathsf{S}(f_n)$ asymptotically as a function of n, and denote it $\mathsf{S}(f)$. E.g. let *PAR* be the parity function, computing if the number of 1's in a binary string is even or odd. Then PAR_n is its restriction to n-bit inputs, and $\mathsf{S}(PAR) = O(n)$.[13]

[13] We use standard asymptotic notation. For integer functions g, h we write $g = O(h)$ (as well as $h = \Omega(g)$) if for some fixed constant $C > 0$ all integers n satisfy $g(n)/h(n) \leq C$. We write $g = o(h)$ if $g(n)/h(n)$ tends to 0 as n tends to infinity.

It is not hard to see that an algorithm (say a Turing machine) for a function f that runs in time T gives rise to a circuit family for the functions f_n of sizes (respectively) $(T(n))^2$, and so efficiency is preserved when moving from algorithms to circuits. Thus proving lower bounds for circuits implies lower bounds for algorithms, and we can try to attack the $\mathcal{P}$ vs. $\mathcal{NP}$ this way.

Definition 3.2 (The class $\mathcal{P}$/poly). Let $\mathcal{P}$/poly denote the set of all functions computable by a family of polynomial size circuits.

Conjecture 3.3. $\mathcal{NP} \not\subseteq \mathcal{P}$/poly.

Is this a reasonable conjecture? As mentioned above, $\mathcal{P} \subseteq \mathcal{P}$/poly. Does the converse hold? It actually fails badly! There exist undecidable functions f (which cannot be computed by Turing machines at all, regardless of their running time), that have linear-size circuits. This extra power comes from the fact that circuits for different input lengths share no common description (and thus this model is sometimes called "non-uniform").

So is not proving circuit lower bounds a much harder task than proving $\mathcal{P} \neq \mathcal{NP}$ question? There is a strong sentiment that the extra power provided by non-uniformity is irrelevant to $\mathcal{P}$ vs. $\mathcal{NP}$. This sentiment comes from a result of Karp and Lipton [67], proving that $\mathcal{NP} \subseteq \mathcal{P}$/poly implies a surprising uniform "collapse", similar to, but weaker than the statement $\mathcal{NP} = \text{co}\mathcal{NP}$.

Still, what motivates replacing the Turing machine by the potentially more powerful circuit families, when seeking lower bounds? The hope is that focusing on a *finite* model will allow for combinatorial techniques to analyze the power and limitations of efficient algorithms. This hope has materialized in the study of restricted classes of circuits (see e.g. Section 3.2.2).

3.2.1. Basic results and questions. We have already mentioned several basic facts about Boolean circuits, in particular the fact that they can efficiently simulate Turing machines. The next basic fact is that *most Boolean functions require exponential size circuits*.

This is due to the gap between the number of functions and the number of small circuits. Fix the number of inputs bits n. The number of possible functions on n bits is precisely 2^{2^n}. On the other hand, the number of circuits of size s is (via a crudely estimating the number of graphs of that size) at most 2^{s^2}. Since every circuit computes one function, we must have $s > 2^{n/3}$ for *most* functions.

Theorem 3.4. *For almost every function* $f : \mathrm{I}_n \to \{0, 1\}$, $\mathsf{S}(f) \geq 2^{n/3}$.

So hard functions for circuits (and hence for Turing machines) abound. However, the hardness above is proved via a counting argument, and thus supplies no way of putting a finger on one hard function. We shall return to the nonconstructive nature of this problem in Section 4. So far, we cannot prove such hardness for any *explicit* function f (e.g., for an $\mathcal{NP}$-complete function like *SAT*).

Conjecture 3.5. $\mathsf{S}(SAT) \neq 2^{o(n)}$.

The situation is even worse – no *nontrivial* lower-bound is known for any explicit function. Note that for any function f on n bits (which depends on all its inputs), we trivially must have $\mathsf{S}(f) \geq n$, just to read the inputs. The main open problem of circuit complexity is beating this trivial bound.

Open Problem 3.6. Find an explicit function $f : \mathrm{I}_n \to \mathrm{I}_n$ for which $\mathsf{S}(f) \neq O(n)$.

A particularly basic special case of this problem, is the question whether addition is easier to perform than multiplication. Let *ADD* and *MULT* denote, respectively, the addition and multiplication functions on a pair of integers (presented in binary). For addition we have an optimal upper bound; that is, $\mathsf{S}(ADD) = O(n)$. For multiplication, the standard (elementary school) quadratic-time algorithm can be greatly improved [96] (via Discrete Fourier Transforms) to slightly super-linear, yielding $\mathsf{S}(MULT) = O(n \log n \log\log n)$. Now, the question is *whether or not there exist linear-size circuits for multiplication* (i.e., is $\mathsf{S}(MULT) = O(n)$)?

Unable to prove any nontrivial lower bound, we now turn to restricted models. There has been some remarkable successes in developing techniques for proving strong lower bounds for natural restricted classes of circuits. We discuss in some detail only one such model.

3.2.2. Monotone circuits. Many natural functions are *monotone* in a natural sense. Here is an example, from our list of $\mathcal{NP}$-complete problems. Let *CLIQUE* be the function that, given a graph on n vertices (say by its adjacency matrix), outputs 1 iff it contains a complete subgraph of size (say) $\sqrt{n}$ (namely, all pairs of vertices in some $\sqrt{n}$ subset are connected by edges). This function is monotone, in the sense that adding edges cannot destroy any clique. More generally, a Boolean function is monotone, if "increasing" the input (flipping input bits from 0 to 1) cannot "decrease" the function value (cause it to flip from 1 to 0).

A natural restriction on circuits comes by removing negation from the set of gates, namely allowing only $\{\wedge, \vee\}$. The resulting circuits are called *monotone circuits* and it is easy to see that they can compute every *monotone function*.

A counting argument similar to the one we used for general circuits, shows that most monotone functions require exponential size monotone circuits. Still, proving a super-polynomial lower bound on an explicit monotone function was open for over 40 years, till the invention of the so-called *approximation method* by Razborov [89].

Theorem 3.7 ([89], [6]). *CLIQUE requires exponential size monotone circuits.*

Very roughly speaking, the approximation method replaces each of the $\{\wedge, \vee\}$ gates of the (presumed small) monotone circuit with other, judiciously chosen (and complex to describe) *approximating* gates, $\{\tilde{\wedge}, \tilde{\vee}\}$ respectively. The choice satisfies two key properties, which together easily rule out small circuits for *CLIQUE*:

1. Replacing one particular gate by its approximator can only affect the output of the circuit on very few (in some natural but nontrivial counting measure) inputs. Thus in a small circuit, having a few gates, even replacing all gates results in a circuit that behaves as the original circuit on most inputs.

2. However, the output of *every* circuit (regardless of size) made of the approximating gates, produces a function which disagrees with *CLIQUE* on many inputs.

The *CLIQUE* function is well known to be $\mathcal{NP}$-complete, and it is natural to wonder if small monotone circuits suffice for monotone functions in $\mathcal{P}$. However, the approximation method was also used by Razborov [90] to prove a super polynomial size lower bound for monotone circuits computing the *Perfect Matching* problem (which is monotone and is in $\mathcal{P}$): given a graph, can one pair up the vertices such that every pair is connected by an edge?

Theorem 3.8 ([90]). *Perfect Matching requires super polynomial size monotone circuits.*

Interestingly, no exponential lower bound is known for monotone circuits for this problem, but different techniques [88] prove that it requires exponential size monotone *formulae* (namely circuits which are trees), and [107] gives exponential size monotone circuit lower bounds for another natural problem in $\mathcal{P}$.

3.2.3. Why is it hard to prove circuit lower bounds? The 1980s have seen a flurry of new techniques for proving circuit lower bounds on natural, restricted classes of circuits. Besides the *Approximation Method*, these include the *Random Restriction* method of Furst, Saxe, Sipser [35] and Ajtai [5] (used to prove lower bounds on constant depth circuits), the *Communication Complexity* method of Karchmer and Wigderson [64] (used to prove lower bounds on monotone formulae), and others (see the survey [18]). But they all fall short of obtaining any nontrivial lower bounds for general circuits, and in particular proving that $\mathcal{P} \neq \mathcal{NP}$.

Is there a fundamental reason for this failure? The same may be asked about any long standing mathematical problem (e.g. the Riemann Hypothesis). A natural (vague!) answer would be that, probably, the current arsenal of tools and ideas (which may well have been successful at attacking related, easier problems) does not suffice.

Remarkably, complexity theory can make this vague statement into a theorem! Thus we have a "formal excuse" for our failure so far: we can classify a general set of ideas and tools, which are responsible for virtually all restricted lower bounds known, yet must necessarily fail for proving general ones. This introspective result, developed by Razborov and Rudich [93], suggests a framework called *Natural Proofs*. Very briefly, a lower bound proof is *natural*, if it applies to a *large, easily recognizable* set of functions. They first show that this framework encapsulates *all known* lower bounds. Then they show that natural proofs of general circuit lower bounds are

unlikely, in the following sense. Any natural proof of a lower bound surprisingly implies, as a side-effect, subexponential algorithms for inverting *every* candidate one-way function.

Specifically, a *natural* (in this formal sense) lower bound would imply subexponential algorithms for such functions as Integer Factoring and Discrete Logarithm, generally believed to be difficult (to the extent that the security of electronic commerce worldwide relies on such assumptions). This connection strongly uses *pseudorandomness* which will be discussed later. A simple corollary is that no natural proof exists to show that integer factoring requires circuits of size $2^{n^{1/100}}$ (the best current upper bound is $2^{n^{1/3}}$).

One interpretation of the aforementioned result, is an "independence result" of general circuit lower bounds from a certain natural fragment of Peano arithmetic. This may suggest that the $\mathcal{P}$ vs. $\mathcal{NP}$ problem may be independent from Peano arithmetic, or even set theory, which is certainly a possibility.

We finally note that it has been over 10 years since the publication of the Natural Proof paper. The challenge it raised: *prove a non natural lower bound* was not yet met!

4. Proof complexity

For extensive surveys on this material see [13] and in [95].

The concept of *proof* is what distinguishes the study of mathematics from all other fields of human inquiry. Mathematicians have gathered millennia of experience to attribute such adjectives to proofs as "insightful, original, deep" and most notably, "difficult". Can one quantify, mathematically, the difficulty of proving various theorems? This is exactly the task undertaken in proof complexity. It seeks to classify theorems according to the difficulty of proving them, much like circuit complexity seeks to classify functions according to the difficulty of computing them. In proofs, just like in computation, there will be a number of models, called *proof systems* capturing the power of reasoning allowed to the prover.

Proof systems abound in all areas of mathematics (and not just in logic). Let us see some examples.

1. Hilbert's Nullstellensatz is a (sound and complete) proof system in which *theorems* are inconsistent sets of polynomial equations. A *proof* expresses the constant 1 as a linear combination of the given polynomials.

2. Each finitely presented group can be viewed as a proof system, in which *theorems* are words that reduce to the identity element. A *proof* is the sequence of substituting relations to generate the identity.

3. Reidemeister moves are a proof system in which *theorems* are trivial, unknotted, knots. A *proof* is the sequences of moves reducing the given plane diagram of the knot into one with no crossings.

4. von Neumann's Minimax theorem gives a proof system for every zero-sum game. A *theorem* is an optimal strategy for White, and its *proof* is a strategy for Black with the same value.

In each of these and many other examples, the *length* of the proof plays a key role, and the quality of the proof system is often related to how short proofs it can provide.

1. In the Nullstellensatz (over fields of characteristic 0), length (of the "coefficient" polynomials, measured usually by their degree and height) usually plays a crucial role in the efficiency of commutative algebra software, e.g. Gröbner basis algorithms.

2. The word problem in general is undecidable. For hyperbolic groups, Gromov's polynomial upper bound on proof length has many uses, perhaps the most recent is in his own construction of finitely presented groups with no uniform embeddings into Hilbert space [48]

3. Reidemeister moves are convenient combinatorially, but the best upper bounds on length in this system to prove that a given knot is unknotted are exponential [52]. Stronger proof systems were developed to give polynomial upper bounds for proving unknottedness [53].

4. In zero-sum games, happily all proofs are of linear size.

We stress that the asymptotic view point – considering *families* of "theorems" and measuring their proof length as a function of the description length of the theorems – is natural and prevalent. As for computation, this asymptotic viewpoint reveals structure of the underlying mathematical objects, and economy (or efficiency) of proof length often means a better understanding. While this viewpoint is appropriate for a large chunk of mathematical work, you may rebel that it cannot help explaining the difficulty of *single* problems, such as the Riemann Hypothesis or $\mathcal{P}$ vs. $\mathcal{NP}$. But even such theorems may be viewed asymptotically (not always illuminating them better though). The Riemann Hypothesis has equivalent formulations as a sequence of finite statements, e.g. about cancellations in the Möbius function. More interestingly, we shall see later a formulation of $\mathcal{P}$/poly vs. $\mathcal{NP}$ problem, as a sequence of finite statements which are strongly related to the Natural Proofs paradigm mentioned above.

All theorems which will concern us in this section are *universal* statements (e.g an inconsistent set of polynomial equations is the statement that *every* assignments to the variables fails to satisfy them). A short proof for a universal statement constitutes an equivalent formulation which is *existential* – the existence of the proof itself (e.g. the existence of the "coefficient" polynomials in Nullstellensatz which implies this inconsistency). The mathematical motivation for this focus is clear – the ability to describe a property both universally and existentially constitutes *necessary and sufficient* conditions – a holy grail of mathematical understanding. Here we shall be picky and quantify that understanding according to our usual computational yardstick – the *length* of the existential certificate.

We shall restrict ourselves to *propositional* tautologies. This will automatically give an exponential (thus a known, finite) upper bound on the proof length, and will restrict the ballpark (as with $\mathcal{P}$ vs. $\mathcal{NP}$) to the range between polynomial and exponential. The type of statements, theorems and proofs we shall deal with is best illustrated by the following example.

4.1. The pigeonhole principle – a motivating example. Consider the well-known "pigeonhole principle", stating that there is no injective mapping from a finite set to a smaller one. While trivial, we note that this principle was essential for the counting argument proving the *existence* of exponentially hard functions (Theorem 3.4) – this partially explains our interest in its proof complexity. More generally, this principle epitomizes *non-constructive* arguments in mathematics, such as Minkowski's theorem that a centrally symmetric convex body of sufficient volume must contain a lattice point. In both results, the proof does not provide any information about the object proved to exist. We note that other natural tautologies capture the combinatorial essence of topological proofs (e.g. Brauer's fixed point theorem, the Borsuk–Ulam theorem and Nash's equilibrium) – see [82] for more.

Let us formulate it and discuss the complexity of proving it. First, we turn it into a sequence of finite statements. Fix $m > n$. Let PHP_n^m stand for the statement *there is no* 1-1 *mapping of m pigeons to n holes*. To formulate it mathematically, imagine an $m \times n$ matrix of Boolean variables x_{ij} describing a hypothetical mapping (with the interpretation that $x_{ij} = 1$ means that the ith pigeon is mapped to the jth hole[14]).

Definition 4.1 (The pigeonhole principle). The pigeonhole principle PHP_n^m now states that

- either pigeon i is not mapped anywhere (namely, *all* x_{ij} for a fixed i are zeros),
- or that some two are mapped to the same hole (namely, for some different i, i' and some j we have $x_{ij} = x_{i'j} = 1$).

These conditions are easily expressible as a formula in the variables x_{ij} (called *propositional formula*), and the pigeonhole principle is the statement that this formula is a *tautology* (namely satisfied by *every* truth assignment to the variables).

Even more conveniently, the negation of this tautology (which is a *contradiction*) can be captured by a collection of constraints on these Boolean variables which are mutually contradictory. These constraints can easily be written in different languages:

- **Algebraic:** as a set of constant degree polynomials over GF(2).
- **Geometric:** as a set of linear inequalities with integer coefficients (to which we seek a $\{0, 1\}$ solution).
- **Logical:** as a set of Boolean formulae.

[14] Note that we do not rule out the possibility that some pigeon is mapped to more than one hole – this condition can be added, but the truth of the principle remains valid without it.

We shall see soon that each setting naturally suggests (several) reasoning tools, such as variants of the Nullstellensatz in the algebraic setting, of Frege systems in the logical setting, and Integer Programming heuristics in the geometric setting. All of these can be formalized as proof systems, that suffice to prove this (and any other) tautology. Our main concern will be in the efficiency of each of these proof systems, and their relative power, measured in *proof length*. Before turning to some of these specific systems, we discuss this concept in full generality.

4.2. Propositional proof systems and $\mathcal{NP}$ vs. co$\mathcal{NP}$. Most definitions and results in this subsection come from the paper which initiated this research direction, by Cook and Reckhow [26]. We define proof systems and the complexity measure of proof length for each, and then relate these to complexity questions we have met already.

All theorems we shall consider will be propositional tautologies. Here are the salient features that we expect[15] from any proof system.

- **Completeness.** Every true statement has a proof.
- **Soundness.** No false statement has a proof.
- **Verification efficiency.** Given a mathematical statement T and a purported proof π for it, it can be easily checked if indeed π proves T in the system. Note that here efficiency of the verification procedure refers to its running-time measured in terms of the *total length of the alleged theorem and proof.*

Remark 4.2. Note that we dropped the requirement used in the definition of $\mathcal{NP}$, limiting the proof to be short (polynomial in the length of the claim). The reason is, of course, that proof length is our measure of complexity.

All these conditions are concisely captured, for propositional statements, by the following definition.

Definition 4.3 (Proof systems, [26]). A (*propositional*) *proof system* is a polynomial-time Turing machine M with the property that T is a tautology if and only if there exists a ("*proof*") π such that $M(\pi, T) = 1$.[16]

As a simple example, consider the following "Truth-Table" proof system M_{TT}. Basically, this machine will declare a formula T a theorem if evaluating it on every possible input makes T true. A bit more formally, for any formula T on n variables, the machine M_{TT} accepts (π, T) if π is a list of *all* binary strings of length n, and for each such string σ, $T(\sigma) = 1$.

Note that M_{TT} runs in polynomial time in its input length, which the combined length of formula and proof. But in the system M_{TT} proofs are (typically) of exponential length in the size of the given formula. This leads us to the definition of the

[15] Actually, even the first two requirements are too much to expect from strong proof systems, as Gödel famously proved in his Incompleteness Theorem. However, for propositional statements which have finite proofs there are such systems.

[16] In agreement with standard formalisms (see below), the proof is seen as coming before the theorem.

efficiency (or complexity) of a general propositional proof system M – how short is the shortest proof of each tautology.

Definition 4.4 (Proof length, [26]). For each tautology T, let $\mathsf{S}_M(T)$ denote the size of the shortest proof of T in M (i.e., the length of the shortest string π such that M accepts (π, T)). Let $\mathsf{S}_M(n)$ denote the maximum of $\mathsf{S}_M(T)$ over all tautologies T of length n. Finally, we call the proof system M *polynomially bounded* iff for all n we have $\mathsf{S}_M(n) = n^{O(1)}$.

Is there a polynomially bounded proof system (namely one which has polynomial size proofs for all tautologies)? The following theorem provides a basic connection of this question with computational complexity, and the major question of Section 2.5. Its proof follows quite straightforwardly from the $\mathcal{NP}$-completeness of *SAT*, the problem of satisfying propositional formulae (and the fact that a formula is unsatisfiable iff its negation is a tautology).

Theorem 4.5 ([26]). *There exists a polynomially bounded proof system if and only if* $\mathcal{NP} = \mathrm{co}\mathcal{NP}$.

In the next section we focus on natural restricted proof systems. We note that a notion of reduction between proof systems, called *polynomial simulation*, was introduced in [26] and allows to create a partial order of the relative power of some systems. This is but one example to the usefulness of the methodology developed within complexity theory after the success of $\mathcal{NP}$-completeness.

4.3. Concrete proof systems. All proof systems in this section are of the familiar variety, starting with the deductive system introduced in *The Elements* of Euclid for plane geometry. We start with a list of formulae, and using simple (and sound!) derivation rules infer new ones (each formula is called a *line* in the proof). In the *contradiction* systems below, we start with a contradictory set of formulae, and derive a basic contradiction (e.g. $\neg x \wedge x$, $1 = 0$, $1 < 0$), depending on the setting. We highlight some results and open problems on the proof length of basic tautologies in algebraic, geometric and logical systems.

4.3.1. Algebraic proof systems. We restrict ourselves to the field GF(2). Here a natural representation of a Boolean contradiction is a set of polynomials with no common root. We always add to such a collection the polynomials $x^2 - x$ (for all variables x) which ensure Boolean values (and so we can imagine that we are working over the algebraic closure).

Hilbert's Nullstellensatz suggests a proof system. If $f_1, f_2, \ldots, f_n$ (with any number of variables) have no common root, there must exist polynomials $g_1, g_2, \ldots, g_n$ such that $\sum_i f_i g_i \equiv 1$. The g_i's constitute a proof, and we may ask how short its description is.

A related, but far more efficient system (intuitively based on computations of Gröbner bases) is Polynomial Calculus, abbreviated PC, which was introduced in [22].

The *lines* in this system are polynomials (represented explicitly by all coefficients), and it has two *deduction rules*, capturing the definition of an *ideal*: For any two polynomials g, h and variable x_i, we can use g, h to derive $g + h$, and we can use g and x_i to derive $x_i g$. It is not hard to see (using linear algebra), that if this system has a proof of length s for some tautology, then this proof can be found in time polynomial in s. Recalling our discussion on $\mathcal{P}$ vs. $\mathcal{NP}$, we do not expect such a property from really strong proof systems.

The PC is known to be exponentially stronger than Nullstellensatz. More precisely, there are tautologies which require exponential length Nullstellensatz proofs, but only polynomial PC-proofs. However, strong size lower bounds (obtained from degree lower bounds) are known for PC system as well. Indeed, the pigeonhole principle is hard for this system. For its natural encoding as a contradictory set of quadratic polynomials, Razborov [91] proved

Theorem 4.6 ([91]). *For every n and every $m > n$, $\mathsf{S}_{\mathrm{PC}}(PHP_n^m) \geq 2^{n/2}$, over every field.*

4.3.2. Geometric proof systems. Yet another natural way to represent Boolean contradictions is by a set of regions in space containing no integer points. A wide source of interesting contradictions are Integer Programs from combinatorial optimization. Here, the constraints are (affine) linear inequalities with integer coefficients (so the regions are subsets of the Boolean cube carved out by halfspaces). A proof system infers new inequalities from old ones in a way which does not eliminate integer points.

The most basic system is called Cutting Planes (CP), introduced by Chvátal [20]. Its *lines* are linear inequalities with integer coefficients. Its *deduction rules* are (the obvious) addition of inequalities, and the (less obvious) dividing the coefficients by a constant (and rounding, taking advantage of the integrality of the solution space)[17].

Let us look at the pigeonhole principle PHP_n^m again. It is easy to express it as a set of contradictory linear inequalities: For every pigeon, the sum of its variables should be *at least* 1. For every hole, the sum of its variables should be *at most* 1. Thus adding up all variables in these two ways implies $m \leq n$, a contradiction. Thus, the pigeonhole principle has polynomial size CP proofs.

While PHP_n^m is easy in this system, exponential lower bounds were proved for other tautologies, and we explain how next. Consider the tautology $CLIQUE_n^k$: No graph on n nodes can simultaneously have a k-clique and a legal $k-1$-coloring. It is easy to formulate it as a propositional formula. Notice that it somehow encodes *many* instances of the pigeonhole principle, one for every k-subset of the vertices.

Theorem 4.7 ([84]). $\mathsf{S}_{\mathsf{CP}}\left(CLIQUE_n^{\sqrt{n}}\right) \geq 2^{n^{1/10}}$.

The proof of this theorem by Pudlak [84] is quite remarkable. It *reduces* this proof complexity lower bound into a circuit complexity lower bound. In other words, he

[17] E.g. from the inequality $2x + 4y \geq 1$ we may infer $x + 2y \geq \frac{1}{2}$, and by integrality, $x + 2y \geq 1$.

shows that any short CP-proof of tautologies of certain structure, yields a small circuit computing a related Boolean function. You probably guessed that for the tautology at hand, the function is indeed the *CLIQUE* function introduced earlier. Moreover, the circuits obtained are *monotone*, but of the following, very strong form. Rather than allowing only $\wedge, \vee$ as basic gates, they allow *any* monotone binary operation on real numbers! Pudlak then goes to generalize Razborov's approximation method (Section 3.2.2) for such circuits and proves an exponential lower bound on the size they require to compute *CLIQUE*.

4.3.3. Logical proof systems. The proof systems in this section will all have *lines* that are Boolean formulae, and the differences between them will be in the structural limits imposed on these formulae. We introduce the most important ones: Frege, capturing "polynomial time reasoning", and Resolution, the most useful system used in automated theorem provers.

The most basic proof system, called Frege system, puts no restriction on the formulae manipulated by the proof. It has one *derivation rule*, called the *cut rule*: from the two formulas $A \vee C$, $B \vee \neg C$ we may infer the formula $A \vee B$. Every basic book in logic has a slightly different way of describing the Frege system – one convenient outcome of the computational approach, especially the notion of efficient reductions between proof systems, is a proof (in [26]) that they are *all* equivalent, in the sense that the shortest proofs (up to polynomial factors) are independent of which variant you pick!

The Frege system can polynomially simulate *both* the Polynomial Calculus and the Cutting Planes systems. In particular, the counting proof described above for the pigeonhole principle can be carried out efficiently in the Frege system (not quite trivially!), yielding

Theorem 4.8 ([19]). $S_{\text{Frege}}(PHP_n^{n+1}) = n^{O(1)}$.

Frege systems are basic in the sense that they are the most common in logic, and in that polynomial length proofs in these systems naturally corresponds to "polynomial-time reasoning" about feasible objects. In short, this is the proof analog of the computational class $\mathcal{P}$. The major open problem in proof complexity is to find any tautology (as usual we mean a family of tautologies) that has no polynomial-size proof in the Frege system.

Open Problem 4.9. Prove superpolynomial lower bounds for the Frege system.

As lower bounds for Frege are hard, we turn to subsystems of Frege which are interesting and natural. The most widely studied system is Resolution. Its importance stems from its use by most propositional (as well as first order) *automated theorem provers*, often called Davis–Putnam or DLL procedures [28]. This family of algorithms is designed to find proofs of Boolean tautologies, arising in diverse applications from testing computer chips or communication protocols, to basic number theory results.

The *lines* in Resolution refutations are *clauses*, namely disjunctions of literals (like $x_1 \vee x_2 \vee \neg x_3$). The *inference cut rule* simplifies to the *resolution rule*: for two clauses A, B and variable x, we can use $A \vee x$ and $B \vee \neg x$ to derive the clause $A \vee B$.

Historically, the first major result of proof complexity was Haken's[18] [49] exponential lower bound on Resolution proofs for the pigeonhole principle.

Theorem 4.10 ([49]). $S_{\text{Resolution}}(PHP_n^{n+1}) = 2^{\Omega(n)}$.

To prove it, Haken developed the *bottleneck method*, which is related to both the random restriction and approximation methods mentioned in the circuit complexity chapter. This lower bound was extended to *random tautologies* (under a natural distribution) in [21]. The *width method* of [15] provides much simpler proofs for both results.

4.4. Proof complexity vs. circuit complexity. These two areas look like very different beasts, despite the syntactic similarity between the local evolution of computation and proof. To begin with, the number of objects they care about differ drastically. There are doubly exponentially number of functions (on n bits), but only exponentially many tautologies of length n. Thus a counting argument shows that some functions (albeit non explicit) require exponential circuit lower bounds (Theorem 3.4), but no similar argument can exist to show that some tautologies require exponential size proofs. So while we prefer lower bounds for natural, explicit tautologies, *existence* results of hard tautologies for strong systems are interesting in this setting as well.

Despite the different nature of the two areas, there are deep connections between them. Quite a few of the techniques used in circuit complexity, most notably *Random Restrictions* were useful for proof complexity as well. The lower bound we saw in the previous subsection is extremely intriguing: a monotone circuit lower bound directly implies a (nonmonotone) proof system lower bound! This particular type of reduction, known as the *Interpolation Method* was successfully used for other, weak, proof systems, like Resolution. It begs the question if one can use reductions of a similar nature to obtain lower bounds for strong system (like Frege), from (yet unproven) circuit lower bounds?

Open Problem 4.11. Does $\mathcal{NP} \not\subseteq \mathcal{P}/\text{poly}$ imply superpolynomial Frege lower bounds?

Why are Frege lower bounds hard? The truth is, we do not know. The Frege system (and its relative, Extended Frege), capture *polynomial time reasoning*, as the basic objects appearing in the proof are polynomial time computable. Thus superpolynomial lower bounds for these systems is the proof complexity analog of proving superpolynomial lower bounds in circuit complexity. As we saw, for circuits we at least understand to some extent the limits of existing techniques, via Natural Proofs. However, there is no known analog of this framework for proof complexity.

[18] Armin Haken, the son of Wolfgang Haken cited earlier for his work on knots.

We conclude with a tautology capturing the $\mathcal{P}$/poly vs. $\mathcal{NP}$ question. Thus we use proof complexity to try showing that proving circuit lower bounds is difficult.

This tautology, suggested by Razborov, simply encodes the statement $\mathcal{NP} \not\subseteq \mathcal{P}$/poly, namely that *SAT* does not have small circuits. More precisely, fix n, an input size to *SAT*, and s, the circuit size lower bound we attempt to prove[19]. The variables of our "Lower Bound" formula LB_n^s encode a circuit C of size s, and the formula simply checks that C disagrees with *SAT* on at least one instance ϕ of length n (namely that either $\phi \in SAT$ and $C(\phi) = 0$ or $\phi \notin SAT$ and $C(\phi) = 1$.) Note that LB_n^s has size $N = 2^{O(n)}$, so we seek a superpolynomial in N lower bound on its proof length[20].

Proving that LB_n^s is hard for Frege will in some sense give another explanation to the difficulty of prove circuit lower bound. Such a result would be analogous to the one provided by Natural Proofs, only without relying on the existence of *one-way* functions. But paradoxically, the same inability to prove circuit lower bounds seems to prevent us from proving this proof complexity lower bound! Even proving that LB_n^s is hard for Resolution has been extremely difficult. It involves proving hardness of a *weak* pigeonhole principle[21] – one with exponentially more pigeons than holes. It was finally achieved with the tour-de-force of Raz [87], and further strengthening of [92].

5. Randomness in computation

The marriage of randomness and computation has been one of the most fertile ideas in computer science, with a wide variety of ideas and models ranging from cryptography to computational learning theory to distributed computing. It enabled new understanding of fundamental concepts such as knowledge, secret, learning, proof, and indeed, randomness itself. In this and the next section we shall just touch the tip of the iceberg, things most closely related to the questions of efficient computation and proofs. The following two subsections tell the contradicting stories on the power and weakness of algorithmic randomness. Good sources are [79], [39] and the relevant chapters in [95].

5.1. The power of randomness in algorithms. Let us start with an example, which illustrates a potential dilemma met by mathematicians who try to prove identities. Assume we work here over the rationals $\mathbb{Q}$. The $n \times n$ Vandermonde matrix $V(x_1, \ldots, x_n)$ in n variables has $(x_i)^{j-1}$ in the (i, j) position. The Vandermonde Identity is:

Proposition 5.1. $\det V(x_1, \ldots, x_n) \equiv \prod_{i<j}(x_i - x_j)$.

While this particular identity is simple to prove, many others like it are far harder. Suppose you conjectured an identity $f(x_1, \ldots, x_n) \equiv 0$, concisely expressed (as

[19] E.g. we may choose $s = n^{\log\log n}$ for a superpolynomial bound, or $s = 2^{n/1000}$ for an exponential one.

[20] Of course, if $\mathcal{NP} \subseteq \mathcal{P}$/poly then this formula is *not* a tautology, and there is no proof at all.

[21] This explicates the connection we mentioned between the pigeonhole principle and the counting argument proving existence of hard functions

above) by a short formula say, and wanted to know if it is true before investing much effort in proving it. Of course, if the number of variables n and the degree d of the polynomial f are large (as in the example), expanding the formula to check that all coefficients vanish will take exponential time and is thus infeasible. Indeed, no subexponential time algorithm for this problem is known! Is there a quick and dirty way to find out?

A natural idea suggests itself: assuming f is *not* identically zero, then the variety it defines has measure zero, and so if we pick *at random* values to the variables, chances are we shall miss it. If f is identically zero, every assignment will evaluate to zero. It turns out that the random choices can be restricted to a finite domain, and the following can be simply proved:

Proposition 5.2 ([98], [113]). *Let f be a* nonzero *polynomial of degree at most d in n variables. Let r_i be uniformly and independently chosen from* $\{1, 2, \ldots, 3d\}$. *Then* $\Pr[f(r_1, \ldots, r_n) = 0] \leq 1/3$.

Note that since evaluating the polynomial at any given point is easy given a formula for f, the above constitutes an efficient *probabilistic* algorithm for verifying polynomial identities. Probabilistic algorithms differ from the algorithms we have seen so far in two ways. First, they postulate the ability to toss coins and generate random bits. Second, they make errors. The beauty is, that if we are willing to accept both (and we should!), we seem to be getting far more efficient algorithms for seemingly hard problems.

The deep issue of whether randomness exists in nature has never stopped humans from assuming it anyway, for gambling, tie breaking, polls and more. A fascinating subject of how to harness seemingly unpredictable *weak sources of randomness* (such as sun spots, radioactive decay, weather, stock-market fluctuations or internet traffic) and converting them into a uniform stream of independent, unbiased coin flips, is the mathematical study of *randomness extractors* which we shall not describe here (see the excellent survey [99]). We shall postulate access of our algorithms to such perfect coin flips, and develop the theory from this assumption. We note that whatever replaces these random bits in practical implementations of probabilistic algorithms seems empirically to work pretty well.

The error seems a more serious issue – we compute to discover a *fact*, not a "maybe". However, we do tolerate uncertainty in real life (not to mention computer hardware and software errors). Observe that the error of probabilistic algorithm is much more controllable – it can be decreased arbitrarily, with small penalty in efficiency. Assume our algorithm makes error at most 1/3 on any input (as the one above). Then running it k times, with independent random choices each time, and taking a majority vote would reduce the error to $\exp(-k)$ on every input!

Thus we revise our notion of efficient computation to allow probabilistic algorithms with small error, and define the probabilistic analog $\mathcal{BPP}$ (for Bounded error, Probabilistic, Polynomial time) of the class $\mathcal{P}$.

Definition 5.3 (The class $\mathcal{BPP}$, [37]). The function $f : \mathrm{I} \to \mathrm{I}$ is in $\mathcal{BPP}$ if there exists a probabilistic polynomial time algorithm A, such that for every input x, $\Pr[A(x) \neq f(x)] \leq 1/3$.

Again, we stress that this probability bound is over the internal coin-tosses of the algorithm, and holds for *every* input. Moreover, replacing the error probability $1/3$ by $\exp(-|x|)$ leaves the definition unchanged (by the amplification idea above).

Probabilistic algorithms were used in statistics (for sampling) and physics (Monte Carlo methods), before computer science existed. However, their introduction into computer science in the 1970s, starting with the probabilistic primality tests of Solovay–Strassen [104] and Rabin [85], was followed by an avalanche that increased the variety and sophistication of problems amenable to such attacks tremendously – a glimpse to this scope can be obtained e.g. from the textbook [79]. We restrict ourselves here only to those which save *time*, and note that randomness seems to help save other resources as well!

We list here a few sample problems which have probabilistic polynomial time algorithms[22], but for which the best known deterministic algorithms require exponential time. These are amongst the greatest achievements of this field.

- **Generating primes ([104], [85]).** Given an integer x (in binary), produce a prime in the interval $[x, 2x]$ (note that the prime number theorem guarantees that a random number in this interval is a prime with probability about $1/|x|$).
- **Polynomial factoring ([63]).** Given an arithmetic formula describing a multivariate polynomial (over a large finite field), find its irreducible factors[23]
- **Permanent approximation ([60]).** Given a nonnegative real matrix, approximate its permanent[24] to within (say) a factor of 2.
- **Volume approximation ([31]).** Given a convex body in high dimension (e.g. a polytope given by its bounding hyperplanes), approximate its volume[25] to within (say) a factor of 2.

The most basic question about this new computational paradigm of probabilistic computation, is whether it really adds any power over deterministic computation.

Open Problem 5.4. Is $\mathcal{BPP} = \mathcal{P}$?

The empirical answer is an emphatically *NO*: we have no idea in sight as to how to solve the problems above, and many others, even in subexponential time deterministically, let alone in polynomial time. However, the next subsection should change this viewpoint.

[22] Strictly speaking they are not in $\mathcal{BPP}$ as they compute relations rather than functions.

[23] Note that it is not even clear that the output has a representation of polynomial length – but it does!

[24] Unlike its relative, the determinant, which can be easily computed efficiently by Gauss elimination, the permanent is known to be $\#\mathcal{P}$-complete (which implies $\mathcal{NP}$-hardness) to compute exactly.

[25] Again, computing the volume exactly is $\#\mathcal{P}$-complete.

5.2. The weakness of randomness in algorithms. Let us start from the end: if any of the numerous $\mathcal{NP}$-complete problems we saw above is *hard* then randomness is *weak*. There is a tradeoff between what the words *hard* and *weak* formally mean. To be concrete, we give perhaps the most dramatic such result of Impagliazzo and Wigderson [58].

Theorem 5.5 ([58]). *If SAT cannot be solved by circuits of size $2^{o(n)}$ then $\mathcal{BPP} = \mathcal{P}$. Moreover, SAT can be replaced in this statement by any problem which has $2^{O(n)}$-time algorithms*[26].

Rephrasing, exponential circuit lower bounds on essentially any problem of interest imply that randomness can be *always* eliminated from algorithms without sacrificing efficiency (up to polynomial). Many variants of this result exist. Weakening the assumed lower bound does weaken the deterministic simulation of randomness, but leaves it highly nontrivial. For example, if $\mathcal{NP} \not\subseteq \mathcal{P}/\text{poly}$ then $\mathcal{BPP}$ has deterministic algorithms with subexponential runtime $\exp(n^{\varepsilon})$ for every $\varepsilon > 0$. Moreover, analogs are known where the hardness assumption is uniform (of the type $\mathcal{P} \neq \mathcal{NP}$), e.g. [59].

Note one remarkable nature of such theorems: if one computational task is hard, than another is easy!

We are now faced with deciding which of two extremely appealing beliefs to drop (as we discover that they are contradictory!). Either that natural problems (e.g. $\mathcal{NP}$-complete ones) cannot be solved efficiently, or that randomness is extremely powerful. Given that our intuition about the former seems far more established, we are compelled to conclude that randomness cannot significantly speed-up algorithms, and indeed $\mathcal{BPP} = \mathcal{P}$.

Conjecture 5.6. $\mathcal{BPP} = \mathcal{P}$.

We now turn to give a high level description of the ideas leading to this surprising set of results, which are generally known under the heading *Hardness vs. Randomness*[27]. We refer the reader to the surveys in [39], [95] for more.

We are clearly after a general way of eliminating the randomness used by any (efficient!) probabilistic algorithm. Let A be such an algorithm, working on input x, and using as randomness the uniform distribution U_n on binary sequences of length n. Assume A computes a function f, and its error on any input is at most $1/3$. The idea is to "fool" A, replacing the distribution U_n by another distribution D, without A noticing it!

This leads to the key definition of *pseudorandomness* of Yao [111].

[26] This class includes most $\mathcal{NP}$-complete problems, but far more complex ones, e.g. determining optimal strategies of games, not believed to be in $\mathcal{NP}$.

[27] The title of Silvio Micali's PhD thesis, who, with his advisor Manuel Blum constructed the first hardness based pseudorandom bit generator.

Definition 5.7 (Pseudorandomness, [111]). Call a distribution D *pseudorandom* if no efficient process[28] can "tell it apart"[29] from the uniform distribution U_n.

By the definition, any such distribution is as good as U_n, as A's computation on x *is* and efficient process.

Remark 5.8. This definition specializes a more general one of *computational indistinguishability* between probability distributions, which originates in the landmark paper of Goldwasser and Micali [43]. This key *behavioristic* definition of randomness underlies the mathematical foundations of modern cryptography which are laid out in that paper. We also note that computational indistinguishability suggests a coarsening of the usual statistical distance (L_1 norm) between probability distributions, and we shall see its importance again in Section 6.2

Back to our derandomization task. Can we efficiently generate a pseudorandom distribution D from only very few random bits? Specifically, we would like to compute $D = G(U_m)$ where G is a deterministic polynomial time algorithm and $m << n$. Such functions G which produce pseudorandom distributions from short random *seeds* are called *pseudorandom generators*. With them, a deterministic simulation will only need to enumerate all possible 2^m seed values (rather than the trivial 2^n). For each such seed it will use the output of G as "randomness" for the computation of A on x, and take a majority vote. As the error of A was at most $1/3$ under U_n, and A's output probability changes by at most $1/9$ between D and U_n, the new error is at most $4/9$, so the majority vote will correctly compute $f(x)$, for *every* x. If m gets down to $O(\log n)$, then $2^m = n^{O(1)}$, and this becomes a deterministic polynomial time algorithm.

But how can we construct such a pseudorandom generator G? Since the definition of pseudorandomness depends on the computational limitations of the algorithm, one might hope to embed some hard function g into the workings of the generator G, and argue as follows. If an efficient process can distinguish the output of G from random, we shall turn it into an efficient algorithm for solving the (assumed hard) function g. This yields a contradiction.

Thus the heart is this conversion of hardness into pseudorandomness. The two main different methods for implementing this idea are the original generator of Blum–Micali and Yao [17], [111] (which must use "one-way" functions, see Definition 2.18, as its hard g's), and the one by Nisan–Wigderson [80] (which can use any function g with an exponential time algorithm). We note that here the hardness required of g is of the *average-case* variety, which is either assumed in the former, or has to be obtained from *worst-case* hardness in the latter. Thus this field invents and uses new types of efficient *reductions*, translating nonstandard computational tasks (from distinguishing a random and pseudorandom distributions, to computing a function well on average, to computing it in the worst case.

[28] This can mean an algorithm or a circuit.

[29] E.g. produce a given output with noticeably different probability, say $1/9$.

We note that this very general line of attack may benefit from specialization. We saw that to derandomize a probabilistic algorithm all we need is a way to efficiently generate a low entropy distribution which *fools it*. But for specific, given algorithms this may be easier that for *all* of them. Indeed, careful analysis of some important probabilistic algorithms, and the way they use their randomness, has enabled making them deterministic via tailor-made generators. These success stories (of which the most dramatic is the recent deterministic primality test of [3]) actually suggest the route of probabilistic algorithms and then derandomization as a paradigm for *deterministic* algorithm design. More in the textbook [79]. Finally, me mention the remarkable result of [62] showing that derandomizing the simple probabilistic algorithm embodied in Proposition 5.2 is *equivalent* to proving certain circuit lower bounds.

We conclude by stressing that randomness remains indispensable in many fields of computer science, including cryptography, distributed computing, and – as we shall see next – probabilistic proofs.

6. Randomness in proofs[29]

The introduction of randomness into proofs has been one of the most powerful ideas in theoretical computer science, with quite a number of unexpected consequences, and in particular new, powerful characterizations of $\mathcal{NP}$. In this section we summarize the main definitions and results of this research direction. Again, we refer the readers to the surveys in [61], [39], [95] and the references therein for more detail.

Let us start again with an example. Consider the graph isomorphism problem mentioned in Section 2.11: given two graphs G and H, determine if they are isomorphic. No polynomial time algorithm is known for this problem. Now assume that an infinitely powerful teacher (who in particular can solve such problems), wants to convince a limited, polynomial time student, that two graphs G, H are isomorphic. This is easy – the teacher simply provides the bijection between the vertices of the two graphs, and the student can verify that edges are preserved. This is merely a rephrasing of the fact that *ISO*, the set of all isomorphic pairs (G, H), is in $\mathcal{NP}$. But is there a similar way for the teacher to convince the student that two given graphs are *not* isomorphic? It is not known if $ISO \in \text{co}\mathcal{NP}$, so we have no such short certificates for nonisomorphism. What can be done?

Here is an idea from [41], which allows the student and teacher more elaborate interaction, as well as coin tossing. The student challenges the teacher as follows. He (secretly) flips a coin to choose one of the two input graphs G or H. He then creates a *random* isomorphic copy K of the selected graph, by randomly permuting the vertex names (again with secret coin tosses). He then presents the teacher with

[29] In this section we do *not* discuss the "probabilistic method", a powerful proof *technique*. An excellent text on it is [7].

K, who is challenged to tell if K is isomorphic to G or H. Observe that if G and H are indeed non isomorphic as claimed, then the answer is unique, and the challenge can always be met (recall that the teacher has infinite computational power). If however G and H are isomorphic, *no* teacher can guess the origin of K with probability greater than 1/2. Simply, the two distributions: random isomorphic copy of G, and random isomorphic copy of H, are *identically distributed*, and so cannot be told apart regardless of computational power. Furthermore, if the teacher succeeds in a 100 independent challenges of this type, his probability of succeeding in all when G and H are isomorphic go down to 2^{-100}, yielding an overwhelmingly convincing *interactive proof* that the graphs are indeed non isomorphic. And we note another remarkable fact: if you are worried about the need for the student to hide his coin tosses, there is another (more sophisticated) interactive proof due to [45] in which all coin tosses of the student are available to the prover!

We return to the general discussion. We have already discussed proof systems in sections 2.3 and 4. In both, the verifier that a given witness to a given claim is indeed a proof was required to be an efficient *deterministic* procedure. In the spirit of the previous section, we now relax this requirement and allow the verifier to toss coins, and err with a tiny probability.

To make the quantifiers in this definition clear, as well as allow more general interaction between the prover and the verifier, it will be convenient to view a proof system for a set S (e.g., of satisfiable formulae) as a *game* between an all-powerful prover and the (efficient, probabilistic) verifier: Both receive an input x, and the prover attempts to convince the verifier that $x \in S$. Completeness dictates that the prover succeeds for every $x \in S$. Soundness dictates that *every* prover fails for every $x \notin S$. In the definition of $\mathcal{NP}$, both of these conditions should hold *with probability* 1 (in which case we may think of the verifier as deterministic). In probabilistic proof systems we relax this condition, and only require that soundness and completeness hold with high probability (e.g. 2/3, as again the error can be reduced arbitrarily via iteration and majority vote). In other words, the verifier will only rarely toss coins that will cause it to mistake the truth of the assertion.

This extension of standard $\mathcal{NP}$ proofs was suggested independently in two papers – one of Goldwasser, Micali and Rackoff [44] (whose motivation was from cryptography, in which interactions of this sort are prevalent), and the other by Babai [10] (whose motivation was to provide such interactive "certificates" for natural problems in group theory which were not known to be in co$\mathcal{NP}$). While the original definitions differed (in whether the coin tosses of the verifier are known to the prover or not), the paper of Goldwasser and Sipser [45] mentioned above showed both models equivalent.

This relaxation of proofs is not suggested as a substitute to the notion of mathematical truth. Rather, much like probabilistic algorithms, it is suggested to greatly increase the set of claims which can be efficiently proved in cases where tiny error is immaterial. As we shall see below, it turns out to yield enormous advances in computer science, while challenging our basic intuition about the very nature of proof.

We exhibit three different remarkable manifestations of that: the first shows that we can prove many more theorems, the second that we can convince others that we have a correct proof of a given theorem without revealing *anything* else about our proof, and the third that verifiers need only look at a handful of bits in a proof to be convinced of its validity.

6.1. Interactive proof systems. When the verifier is deterministic, we can always assume that the prover simply sends a single message (the purported "proof"), and based on this message the verifier decides whether to accept or reject the common input x as a member of the target set S.

When the verifier is probabilistic, *interaction* may add power. We thus consider a (randomized) interaction between the parties, which may be viewed as an "interrogation" by a persistent student, asking the teacher "tough" questions in order to be convinced of correctness. Since the verifier ought to be efficient (i.e., run in time polynomial in $|x|$), the number of such rounds of questions is bounded by a polynomial.

Definition 6.1 (The class $\mathcal{IP}$, [44], [10]). The class $\mathcal{IP}$ (for Interactive Proofs) contains all sets S for which there is a verifier that accepts every $x \in S$ with probability 1 (after interacting with an adequate prover), but rejects any $x \notin S$ with probability at least $1/2$ (no matter what strategy is employed by the prover).

We have already seen the potential power of such proofs in the example of graph isomorphism above, and several others were given. But the full power of $\mathcal{IP}$ begun to unfold only after an even stronger proof system, allowing *multiple provers*, was suggested by Ben-Or et al. [14] (motivated by cryptographic considerations). A lively account of the rapid progress is given in [11]. One milestone was showing that $\mathcal{IP}$ proofs can be given to *every* set in co$\mathcal{NP}$ (indeed, much more, but for classes we have not defined).

Theorem 6.2 ([77]). co$\mathcal{NP} \subseteq \mathcal{IP}$.

This was shortly followed by a complete characterization of $\mathcal{IP}$ by Shamir [100]. He proved it equivalent to $\mathcal{PSPACE}$, the class of sets computable with polynomial memory (and possibly exponential time). We note that this class contains problems which seem much harder than $\mathcal{NP}$ and co$\mathcal{NP}$, e.g. finding optimal strategies of games.

Theorem 6.3 ([100]). $\mathcal{IP} = \mathcal{PSPACE}$.

We conclude by noting that this success story required the confluence and integration of ideas from different "corners" of computational complexity. A central technical tool which was developed for these results, and would play a major role in Section 6.3, is the arithmetic encoding of Boolean formulae by polynomials, and the ultra-fast verification of their properties.

6.2. Zero-knowledge proof systems. Assume you could prove the Riemann Hypothesis. You want to convince the mathematical world of your achievement, but am extremely paranoid that if you revealed the proof, someone else will claim it was his idea. Is there a way to resolve this dilemma? Hold on.

The thrust in this section is not to prove more theorems, but rather to have proofs with additional properties. Randomized and interactive verification procedures as in Section 6.1 allow the (meaningful) introduction of *zero-knowledge proofs*, which are proofs that yield nothing beyond their own validity.

Such proofs seem impossible – how can you convince anyone of anything they do not know already, without giving them any information? In mathematics, whenever we cannot prove a theorem ourselves, we feel that seeing a proof will *necessarily* teach us something we did not know!

Well, the interactive proof above, that two graphs are non isomorphic, at least suggest that in some special cases zero-knowledge proofs are possible! Note that in each round of that proof, the student knew perfectly well what the answer to his challenge was, so he learned nothing. In other words, *if* the graphs were indeed non isomorphic, he could have generated the conversation without the teacher's help! Nevertheless, the conversation convinced him that indeed the graphs were non isomorphic.

How can we define this notion formally? Extending the intuition above, we demand that on every correct claim, the verifier should be able to efficiently generate, *by himself*, (the probability distribution of) his conversation with the prover. More generally, we would be satisfied if what the verifier can generate by himself is *indistinguishable* from the actual conversation (in the same sense as pseudorandom distributions are indistinguishable from the uniform distribution 5.7).

This important definition of zero knowledge proof was suggested in the same seminal paper [44] which defined interactive proofs.

Now which theorems have zero-knowledge proofs? Well, if the verifier can determine the answer with no aid, it is trivial. Thus, any set in $\mathcal{BPP}$ has a zero-knowledge proof, in which the prover says nothing (and the verifier decides by itself). A few examples believed outside $\mathcal{BPP}$ like Graph Non-Isomorphism, are known to have such proofs unconditionally.

What is surprising is that if one allows the standard assumption of cryptography, namely assuming that *one-way functions* exist (see Section 2.11.1), then zero-knowledge proofs exist for *every* theorem of interest! Goldreich, Micali and Wigderson [41] proved:

Theorem 6.4 ([41]). *Assume the existence of one-way functions. Then every set in $\mathcal{NP}$ has a zero-knowledge interactive proof.*

Here again we see the power of reductions and completeness! This theorem is proved in 2 steps. First, [41] gives a zero-knowledge proof for statements of the form *a given graph is* 3*-colorable*, using various structural properties of this problem. Then, it uses the $\mathcal{NP}$-completeness of this problem (in the strong form which allows

efficient translation of witnesses, not just instances, mentioned after Theorem 2.12) to infer that all $\mathcal{NP}$ sets have a zero-knowledge proof.

We stand by the interpretation above of this theorem. If you proved the Riemann Hypothesis, and were nervous to reveal the proof lest the listener would rush to publish it first, you could convince him/her, beyond any reasonable doubt, that you indeed have such a proof, in a way which will reveal no information about it. Simply use the proof that 3Color is $\mathcal{NP}$-complete to translate the statement of the Riemann Hypothesis into the appropriate graph, translate your proof of it into the appropriate legal 3-coloring, and use the protocol of [41].

But the grand impact of this theorem is not in the above toy application. Zero-knowledge proofs are a major tool for forcing participants in cryptographic protocols to behave correctly, without compromising anyone's privacy. This is combined with the *secure evaluation* of functions [112], [42], where (completely different) reductions and completeness are again central to the proof. Together they allow for the implementation of just about any cryptographic task (for a good example for the complexity of such tasks try to imagine playing a game of poker over the telephone).

6.3. Probabilistically checkable proofs. In this section we turn to one of the deepest and most surprising discoveries on the power of probabilistic proofs, and its consequences to the limits of approximation algorithms.

We return to the non-interactive mode, in which the verifier receives a (alleged) written proof. But now we restrict its access to the proof so as to read only a small part of it (which may be randomly selected). An excellent analogy is to imagine a referee trying to decide the correctness of a long proof by sampling a few lines of the proof. It seems hopeless to detect a single "bug" unless the entire proof is read. But this intuition is valid only for the "natural" way of writing down proofs! It fails when *robust* formats of proofs are used (and, as usual, we tolerate a tiny probability of error).

Such robust proof systems are called PCPs (for *Probabilistically Checkable Proofs*). Loosely speaking, a PCP system for a set S consists of a probabilistic polynomial-time verifier having access to individual bits in a string representing the (alleged) proof[31]. The verifier tosses coins and accordingly accesses only a *constant* number of the bits in the alleged proof. It should accepts every $x \in S$ with probability 1 (when given a real proof, adequately encoded), but rejects any $x \notin S$ with probability at least $1/2$ (no matter to which "alleged proof" it is given).

A long sequence of ideas and papers, surveyed in [8], [106], culminated in the "PCP theorem" of Arora et al.:

Theorem 6.5 (The PCP theorem, [9]). *Every set in $\mathcal{NP}$ has a* PCP *system. Furthermore, there exists a polynomial-time procedure for converting any $\mathcal{NP}$-witness to the corresponding, "robust"* PCP*-proof.*

[31] In case of $\mathcal{NP}$-proofs the length of the proof is polynomial in the length of the input.

Indeed, the proof of the PCP theorem suggests a new way of writing "robust" proofs, in which any bug must "spread" all over. Equivalently, if the probability of finding a bug found in these handful of bits scanned by the verifier is small (say <1/10), the theorem is correct! The remarkable PCP theorem was proved with a rather complex and technical proof, which has resisted significant simplification for over a decade. However, a conceptually different proof which is very elegant and much simpler was given last year by Dinur [30].

The reader may find a syntactic similarity between PCPs and error correcting codes. In the latter, if the probability of a bit being flipped in an encoded message is small, then the message can be correctly recovered from its noisy encoding. Indeed there are deep connections, and the cross fertilization between these two areas has been very significant.

The main impact of the PCP theorem (and its variants) is due to its connection, discovered by Feige et al. [33], to *hardness of approximation* (elaborated on in the surveys above). The PCP theorem has revolutionized our ability to argue that certain problems are not only hard to solve exactly, but even to get a rough approximation. We note that in practice, a near-optimal solution to a hard problem may be almost as good as an optimal one. But for decades, till the PCP theorem came along, we had almost no means of proving hardness of approximation results. Even with the PCP theorem, these are typically much harder to prove than standard $\mathcal{NP}$-completeness results. We mention two examples of the strongest such *inapproximability* results, both due to Hastad [54], [55]. Both are nearly tight, in that it is $\mathcal{NP}$-hard to approximate the solution by the factor given, but trivial to do so with slightly bigger factor. In both $\varepsilon > 0$ can be an arbitrarily small constant.

- **Linear equations.** Given a linear system of equations over GF(2), approximate the maximum number of mutually satisfiable ones, to within a factor of $2 - \varepsilon$ (clearly, a factor 2 is trivial: a random assignment will do).
- **Clique.** Given a graph with n vertices, approximate its maximum clique size to within a factor $n^{1-\varepsilon}$ (clearly, a factor n is trivial: one vertex will do).

7. Some concrete open problems

We conclude this paper with a short list of open problems. They were all chosen so as to be free of any reference to computational models. Indeed all have simple elementary definitions, are natural and inviting. However, they all arise from attempts to prove computational lower bounds and have been open for decades. Solving any of them will represent important progress.

In all problems F is a field (of your choice – the questions are of interest for *any* field). We let $\mathrm{M}_n(F)$ denote all $n \times n$ matrices over F and $\mathrm{GL}_n(F)$ all invertible ones. When asking for an *explicit* matrix B, we really mean an infinite family B_n with some finite description.

7.1. Gauss elimination. For a matrix $A \in \mathrm{GL}_n(F)$ let $G(A)$, the *Gauss elimination complexity* of A, denote the smallest number of row and column operations which transform A to a diagonal matrix.

Open Problem 7.1. Find an explicit Boolean matrix B with $G(B) \neq O(n)$.

7.2. Matrix rigidity. A matrix $A \in \mathrm{M}_n(F)$ is (k, r)-*rigid* if for every matrix A' obtained from A by changing (arbitrarily) the values of at most k entries *per row*, $\mathrm{rk}(\mathrm{A}') \geq \mathrm{r}$ (where rk is the rank over F).

Open Problem 7.2. Find an explicit Boolean matrix which is $(\sqrt{n}, n/100)$-rigid.

Find an explicit Boolean matrix which is $(n/100, \sqrt{n})$-rigid.

7.3. Permanent versus determinant. Define as usual the determinant and permanent polynomials by

$$\mathrm{Det}_n(X) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_i X_{i,\sigma(i)}$$

and

$$\mathrm{Per}_n(X) = \sum_{\sigma \in S_n} \prod_i X_{i,\sigma(i)}.$$

Let $m(n)$ be the smallest value m such that Per_n is a projection of Det_m. Namely that the permanent of an $n \times n$ variable matrix X can be written as the determinant of an $m \times m$ matrix every entry of which is either a variable from X or a constant from F.

Open Problem 7.3. Prove that $m(n) \neq n^{O(1)}$.

Note that the field F cannot have characteristic 2.

7.4. Tensor rank (of matrix multiplication). For three $n \times n$ matrices of variables X, Y, Z define the trilinear form $T(X, Y, Z)$ by its action on the standard basis: for every i, j, k we have $T(X_{ij}, Y_{jk}, Z_{ki}) = 1$ and $T = 0$ on all other triples.

A rank 1 tensor is a product of linear forms (one in X, one in Y, one in Z), and the rank of a tensor is the smallest number of rank 1 tensors which add up to it.

Open Problem 7.4. Determine if the rank of T is $O(n^2)$ or not.

7.5. Generalized polynomials for determinant. The notion of tensor rank is slightly extended here to the affine case.

Let X be a set of variables. A *generalized monomial* is simply a product of affine functions over X. A *generalized polynomial* is a sum of generalized monomials.

Clearly generalized polynomials compute "normal" polynomials in $F[X]$, but sometimes they may be sparser (have fewer monomials). For a polynomial $q \in F[X]$ let $s(q)$ denote the minimum number of generalized monomials needed to express q as a generalized polynomial.

Open Problem 7.5. Prove that $s(\mathrm{Det}_n) \neq n^{O(1)}$.

Acknowledgements. We acknowledge support from NSF grant CCR-0324906. Parts of this paper are revisions of material taken from a joint survey on computational complexity with Oded Goldreich, to be published in the Princeton "Compendium to mathematics" edited by Tim Gowers. I am grateful to the following colleagues for careful reading and comments on early versions of this manuscript: Noga Alon, Sanjeev Arora, Bernard Chazelle, Ron Fagin, Oded Goldreich, Nadia Heninger, Alex Lubotzky, Sasha Razborov, Peter Sarnak and Bill Steiger.

References

[1] Adleman, L., and Manders, K., Computational complexity of decision problems for polynomials. *Proceedings of 16th IEEE Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1975, 169–177.

[2] Agol, I., Hass, J., and Thurston, W. P., The Computational Complexity of Knot Genus and Spanning Area. *Trans. Amer. Math. Sci.* **358** (2006), 3821–3850.

[3] Agrawal, M., Kayal, N., and Saxena, N., Primes is in $\mathcal{P}$. *Ann. of Math.* **160** (2) (2004), 781–793.

[4] Ajtai, M., Generating Hard Instances of Lattice Problems. *Proceedings of the 28th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1996, 99–108.

[5] Ajtai, M., Σ_1-formulae on finite structures. *Ann. Pure Appl. Logic* **24** (1) (1983), 1–48.

[6] Alon, N., and Boppana R., The Monotone Circuit Complexity of Boolean Functions. *Combinatorica* **7** (1) (1987), 1–22.

[7] Alon, N. and Spencer, J., *The Probabilistic Method*. 2nd edition, Wiley-Intersci. Ser. Discrete Math. Optim., John Wiley, New York 2000.

[8] Arora, S., Probabilistic checking of proofs and the hardness of approximation problems. Ph.D. Thesis, UC Berkeley, 1994; revised version in http://eccc.hpi-web.de/eccc-local/ECCC-Books/sanjeev_book_readme.html

[9] Arora, S., Lund, C., Motwani, R., Sudan, M., and Szegedy, M., Proof verification and the hardness of approximation problems. *J. ACM* **45** (3) (1998), 501–555.

[10] Babai, L., Trading group theory for randomness. In *Proceedings of the 17th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1985, 421–429.

[11] Babai, L., E-mail and the unexpected power of interaction. In *Proceedings of the 5th Annual Conference on Structure in Complexity Theory*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1990, 30–44.

[12] Baker, T., Gill, J., and Solovay, R., Relativizations of the P = ?NP question. *SIAM J. Comput.* **4** (1975), 431–442.

[13] Beame, P., and Pitassi, T., Propositional Proof Complexity: Past, Present, and Future. *Bull. EATCS* **65** (1998), 66–89.

[14] Ben-Or, M., Goldwasser, S., Kilian, J., Wigderson, A., Efficient Identification Schemes Using Two Prover Interactive Proofs. *Advances in Cryptography* (CRYPTO 89), Lecture Notes in Comput. Sci. 435, Springer-Verlag, Berlin 1989, 498–506.

[15] Ben-Sasson, E., and Wigderson, A., Short Proofs are Narrow - Resolution made Simple. *Proceedings of the 31st annual ACM Symposium on Theory of Computing*, ACM Press, New York 1999, 517–526.

[16] Blum, L., Cucker, F., Shub, M., and Smale, S., *Complexity and Real Computation*. Springer-Verlag, 1998.

[17] Blum, M., and Micali, S., How to generate chryptographically secure sequences of pseudorandom bits. *SIAM J. Comput.* **13** (1984), 850–864.

[18] Boppana, R., and Sipser, M., The complexity of finite functions. In [72], 757–804.

[19] Buss, S., Polynomial size proofs of the propositional pigeonhole principle. *J. Symbolic Logic* **52** (1987), 916–927.

[20] Chvátal, V., Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Math.* **4** (1973), 305–337.

[21] Chvátal, V., and Szemeredi, E., Many hard examples for resolution. *J. ACM* **35** (4) (1988), 759–768.

[22] Clegg, M., Edmonds, J., and Impagliazzo, R., Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability. *Proceedings of the 28th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1996, 174–183.

[23] Cobham, A., The intrinsic computational difficulty of functions. In *Logic, Methodology, and Philosophy of Science*, North Holland, Amsterdam 1965, 24–30.

[24] Cook, S. A., The Complexity of Theorem-Proving Procedures. *Proceedings of the 3rd annual ACM Symposium on Theory of Computing*, ACM Press, New York 1971, 151–158.

[25] Cook, S. A., *The $\mathcal{P}$ vs. $\mathcal{NP}$ Problem*. CLAY Mathematics Foundation Millenium Problems, http://www.claymath.org/millennium.

[26] Cook, S. A., and Reckhow, R. A., The Relative Efficiency of Propositional Proof Systems. *J. Symbolic Logic* **44** (1979), 36–50.

[27] Cormen, T. H., Leiserson, C., and Rivest, R., *Introduction to Algorithms*. 2nd edition, MIT Press, Cambridge, MA; McGraw-Hill Book Co., New York 2001.

[28] Davis, M., Logemann, G., and Loveland, D., A machine program for theorem proving. *J. ACM* **5** (7) (1962), 394–397.

[29] Diffie, W., and Hellman, M., New directions in cryptography. *IEEE Trans. Information Theory* **22** (1976), 644–654.

[30] Dinur, I., The PCP Theorem by gap amplification. *Proceedings of the 38th annual ACM Symposium on Theory of Computing*, ACM Press, New York 2006, 241–250.

[31] Dyer, M., Frieze, A., and Kannan, R., A random polynomial time algorithm for approximating the volume of a convex body. *J. ACM* **38** (1) (1991), 1–17.

[32] Edmonds, J., Paths, Trees, and Flowers. *Canad. J. Math.* **17** (1965), 449–467.

[33] Feige, U., Goldwasser, S., Lovasz, L., Safra, S., and Szegedy, M., Interactive proofs and the hardness of approximating cliques. *J. ACM* **43** (2) (1996), 268–292.

[34] Fortnow, L., The role of relativization in complexity theory. *Bull. EATCS* **52** (1994), 229–244.

[35] Furst, M., Saxe, J., and Sipser, M., Parity, circuits and the polynomial time hierarchy. *Math. Systems Theory* **17** (1984), 13–27.

[36] Garey, M. R., and Johnson, D. S., *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman and Company, New York 1979.

[37] Gill, J., Computational complexity of probabilistic Turing machines. *SIAM J. Comput.* **6** (1977), 675–695.

[38] Goldreich, O., Notes on Levin's Theory of Average-Case Complexity. *ECCC* TR97-058, (1997).

[39] Goldreich, O., *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Algorithms Combin. 17, Springer-Verlag, Berlin 1999.

[40] Goldreich, O., *Foundation of Cryptography*. I. Basic Tools; II. Basic Applications, Cambridge University Press, Cambridge 2001; 2004.

[41] Goldreich, O., Micali, S., and Wigderson, A., Proofs that Yield Nothing but their Validity, or All Languages in NP have Zero-Knowledge Proof Systems. *J. ACM* **38** (1) (1991), 691–729.

[42] Goldreich, O., Micali, S., and Wigderson, A., How to Play any Mental Game. *Proceedings of the 19th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1987, 218–229.

[43] Goldwasser, S., Micali, S., Probabilistic encryption. *J. Comput. System Sci.* **28**, (1984), 270–299.

[44] Goldwasser, S., Micali, S., and Rackoff, C., The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* **18** (1) (1989), 186–208.

[45] Goldwasser, S., and Sipser, M., Private coins versus public coins in interactive proof systems. In *Randomness and Computation* (Silvio Micali, ed.), Advances in Computing Research 5, JAI Press, Inc., Greenwich, CT, 1989, 73–90.

[46] Granville, A., It is easy to determine whether a given integer is prime. *Bull. Amer. Math. Soc.* **42** (2005), 3–38.

[47] Gromov, M., *Hyperbolic groups*. In *Essays in Group Theory* (S. M. Gersten, ed.), Math. Sci. Res. Inst. Publ. 8, Springer-Verlag, New York 1987, 75–264.

[48] Gromov, M., Random walk in random groups. *Geom. Funct. Anal.* **13** (1) (2003), 73–146.

[49] Haken, A., The Intractability of Resolution. *Theor. Comput. Sci.* **39** (1985), 297–308.

[50] Haken, W., Theorie der Normalflächen: Ein Isotopiekriterium für den Kreisknoten. *Acta Math.* **105** (1961), 245–375.

[51] Hartmanis, J., Gödel, von Neumann and the P = ?NP problem. *Bull. EATCS* **38** (1989), 101–107.

[52] Hass, J., Lagarias, J. C., The number of Reidemeister Moves Needed for Unknotting. *J. Amer. Math. Soc.* **14** (2001), 399–428.

[53] Hass, J., Lagarias, J. C., and Pippenger, N., The Computational Complexity of Knot and Link Problems. *J. ACM* **46** (1999), 185–211.

[54] Håstad, J., Clique is hard to approximate within $n^{1-\epsilon}$. *Acta Math.* **182** (1999), 105–142.

[55] Håstad, J., Some optimal inapproximability results. *J. ACM* **48** (2001), 798–859.

[56] Hochbaum, D. (ed.), *Approximation Algorithms for NP-Hard Problems*. PWS Publishing Co., Boston, MA, 1996.

[57] Impagliazzo, R., A personal view of average-case complexity. *Proceedings of the 10th IEEE Annual Conference on Structure in Complexity Theory*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1995, 134–147.

[58] Impagliazzo, R., and Wigderson, A., P = BPP unless E has Subexponential Circuits: Derandomizing the XOR Lemma. *Proceedings of the 29th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1997, 220–229.

[59] Impagliazzo, R., and Wigderson, A., Randomness vs. Time: De-randomization under a uniform assumption. *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1998, 734–743.

[60] Jerrum, M., Sinclair, A., Vigoda, E., A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *J. ACM* **51** (4) (2004), 671–697.

[61] Johnson, D., The Tale of the Second Prover, *J. Algorithms* **13** (3) (1992), 502–524.

[62] Kabanets, V., Impagliazzo, R., Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *Comput. Complexity* **13** (1–2) (2004), 1–46.

[63] Kaltofen, E. Polynomial Factorization. In *Computer Algebra: Symbolic and Algebraic Computation*, 2nd ed., Springer-Verlag, Wien, New York 1983, 95–113.

[64] Karchmer, M., and Wigderson, A., Monotone Circuits for Connectivity require Super-Logarithmic Depth. *SIAM J. Discrete Math.* **3** (2) (1990), 255–265.

[65] Karmarkar, N., A New Polynomial-Time Algorithm for Linear Programming. *Combinatorica* **4** (1984), 373–394.

[66] Karp, R., Reducibility among combinatorial problems. In *Complexity of Computer Computations* (R. E. Miller and J. W. Thatcher, eds.), Plenum Press, New York 1972, 85–103.

[67] Karp, R., and Lipton, R. J., Turing machines that take advice. *Enseign. Math.* (2) **28** (3–4) (1982), 191–209

[68] Khachian, L., A polynomial time algorithm for linear programming. *Soviet Math. Doklady* **10** (1979), 191–194.

[69] Kitaev, A., Shen,A., and Vyalyi, M., *Classical and Quantum Computation*. Grad. Stud. Math. 47, Amer. Math. Soc., Providence, R.I., 2002.

[70] Kushilevitz, E., and Nisan, N., *Communication Complexity*. Cambridge University Press, Cambridge 1997.

[71] Ladner, R., On the Structure of Polynomial Time Reducibility. *J. ACM* **22** (1) (1975), 155–171.

[72] van Leeuwen, J. (ed.), *Handbook of Theoretical Computer Science, Volume A, Algorithms and Complexity*. Elsevier Science Publishers, B.V., Amsterdam; MIT Press, Cambridge, MA, 1990.

[73] Lenstra, A. K., Lenstra Jr., H. W., and Lovász,L. Factoring polynomials with rational coefficients. *Math. Ann.* **261** (1982), 515–534.

[74] Levin, L. A., Universal search problems. *Probl. Peredaci Inform.* **9** (1973), 115–116; English transl. *Probl. Inf. Transm.* **9** (1973), 265–266.

[75] Levin, L. A., Average Case Complete Problems. *SIAM J. Comput.* **15** (1) (1986), 285–286.

[76] Levin, L. A., One-Way Functions and Pseudorandom Generators. *Combinatorica* **7** (4) (1987), 357–363.

[77] Lund, C., Fortnow, L., Karloff, H., Nisan, N., Algebraic Methods for Interactive Proof Systems. *Proceedings of the 31th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1990, 2–10.

[78] Miller, G.L., Riemann's Hypothesis and Tests for Primality. *J. Comput. System Sci.* **13** (3) (1976), 300–317.

[79] Motwani, R., and Raghavan, P., *Randomized Algorithms*. Cambridge University Press, Cambridge 1995.

[80] Nisan, N., and Wigderson, A., Hardness vs. Randomness. *J. Comput. System Sci.* **49** (2) (1994), 149–167.

[81] Papadimitriou, C. H., *Computational Complexity*. Addison Wesley, Reading, MA, 1994.

[82] Papadimitriou, C. H., On the complexity of the parity argument and other inefficient proofs of existence. *J. Comput. System Sci.* **48** (3) (1994), 498–532.

[83] Papadimitriou, C. H., NP-completeness: A retrospective. In *Automata, languages and programming* (ICALP'97), Lecture Notes in Comput. Sci. 1256, Springer-Verlag, Berlin 1997.

[84] Pudlak,P., Lower bounds for resolution and cutting planes proofs and monotone computations. *J. Symbolic Logic* **62** (3) (1997), 981–998.

[85] Rabin, M. O., Probabilistic algorithm for testing primality. *J. Number Theory* **12** (1980), 128–138.

[86] Rabin, M., Mathematical theory of automata. In *Mathematical Aspects of Computer Science*, Proc. Sympos. Appl. Math. 19, Amer. Math. Soc., Providence, R.I., 1967, 153–175.

[87] Raz, R., Resolution lower bounds for the weak pigeonhole principle. *J. ACM* **51** (2) (2004), 115–138.

[88] Raz, R., and Wigderson, A., Monotone Circuits for Matching require Linear Depth. *J. ACM* **39** (1992), 736–744.

[89] Razborov, A. A., Lower bounds for the monotone complexity of some Boolean functions. *Dokl. Akad. Nauk SSSR* **281** (4) (1985), 798–801; English transl. *Soviet Math. Doklady* **31** (1985), 354–357.

[90] Razborov, A. A., Lower bounds of monotone complexity of the logical permanent function. *Mat. Zametki* **37** (6) (1985), 887–900; English transl. *Math. Notes* **37** (1985), 485–493.

[91] Razborov, A. A., Lower Bounds for the Polynomial Calculus. *Comput. Complexity* **7** (4) (1998), 291–324.

[92] Razborov, A. A., Resolution Lower Bounds for Perfect Matching Principles. *J. Comput. System Sci.* **69** (1) (2004), 3–27.

[93] Razborov, A. A., and Rudich, S., Natural Proofs. *J. Comput. System Sci.* **55** (1) (1997), 24–35.

[94] Robertson, N., and Seymour, P., Graph Minors I–XIII. *J. Combin. Theory B* (1983–1995).

[95] Rudich, S., and Wigderson, A. (eds.), *Computational Complexity Theory*. IAS/Park-City Math. Ser. 10, Institute for Advanced Studies/Amer. Math. Soc., 2000.

[96] Schönhage, A., and Strassen, V., Schnelle Multiplikation großer Zahlen. *Computing* **7** (1971), 281– 292.

[97] Schrijver, A., *Combinatorial Optimization. Polyhedra and Efficiency*. Algorithms Combin. 24, Springer-Verlag, Berlin 2003.

[98] Schwartz, J. T., Fast probabilistic algorithms for verification of polynomial identities. *J. ACM* **27** (4) (1980), 701–717.

[99] Shaltiel, R., Recent Developments in Explicit Constructions of Extractors. *Bull. EATCS* **77** (2002), 67–95.

[100] Shamir, A., IP = PSPACE. *J. ACM* **39** (1992), 869–877.

[101] Sipser, M., *Introduction to the Theory of Computation*. PWS Publishing Co., Boston, MA, 1997.

[102] Sipser, M., The History and Status of the P versus NP Question. *Proceedings of the 24th annual ACM Symposium on Theory of Computing*, ACM Press, New York 1992, 603–618.

[103] Smale, S., Mathematical Problems for the Next Century. In *Mathematics: Frontiers and Perspectives*, Amer. Math. Soc., Providence, RI, 2000, 271–294.

[104] Solovay, R. M., and Strassen, V., A fast Monte-Carlo test for primality. *SIAM J. Comput.* **6** (1) (1977), 84–85.

[105] Strassen, V., Algebraic Complexity Theory. In [72], 633–672.

[106] Sudan, M., *Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems*. ACM Distinguished Theses, Lecture Notes in Comput. Sci. 1001, Springer-Verlag, Berlin 1996.

[107] Tardos, E., The Gap Between Monotone and Non-Monotone Circuit Complexity is Exponential. *Combinatorica* **7** (4) (1987), 141–142.

[108] Tarski, A., *A decision method for elementary algebra and geometry*. University of California Press, 1951.

[109] Valiant, L. G., Completeness classes in algebra. In *Proceedings of the eleventh annual ACM Symposium on Theory of Computing* (1979), 249–261.

[110] N. V. Vinodchandran, $\mathrm{AM}_{\mathrm{exp}} \not\subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$. *Inform. Process. Lett.* **89** (2004), 43–47.

[111] Yao, A. C., Theory and application of trapdoor functions. *Proceedings of the 23th annual IEEE Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1982, 80–91.

[112] Yao, A. C., How to generate and exchange secrets. In *Proceedings of the 27th annual IEEE Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1986, 162–167.

[113] Zippel, R. E., Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation* (EUROSCAM '79), Lecture Notes in Comput. Sci. 72, Springer-Verlag, Berlin 1979, 216–226.

School of Mathematics, Institute for Advanced Study, Princeton NJ 08540, U.S.A.
E-mail: avi@ias.edu

The Poincaré Conjecture

John W. Morgan

1. Introduction

It is a great pleasure for me to report on the recent spectacular developments concerning the Poincaré Conjecture.

Grigory Perelman has solved the Poincaré Conjecture. He has shown that, as Poincaré conjectured, any closed, simply connected 3-manifold is homeomorphic to the 3-sphere.

The paper in which Poincaré posed this problem in 1904 ([14]) marked, in my view, the founding of topology as an independent discipline within pure mathematics. Over the intervening 100 years, the problem has been much studied and generalized, and many related problems have been solved. It has been linked, in one way or another, with most of the progress in topology in the last 100 years. While related problems have been solved, the original conjecture stood untouched, resisting all attempts. Before Perelman's work, there had been no progress on toward solving the Poincaré Conjecture, and many viewed it as the siren song of Topology, for many a boat had foundered on the rocks trying to reach it. There have been innumerable proposed proofs and proposed counter-examples, but none, before Perelman's, withstood scrutiny.

Solving the Poincaré Conjecture is a signal achievement for Perelman, but it is also a signal achievement for all of mathematics, for it gives a measure of how far our understanding of the subject has advanced in the last 100 years. To paraphrase Newton, Perelman has seen far, but to do so he stood on the shoulders of giants who came before him. One giant, in particular, stands out. He is Richard Hamilton. Over a period of 25 years, Hamilton painstakingly built the solid and elaborate foundation upon which Perelman constructed the edifice of his proof. Without Hamilton's work, Perelman's would not have been possible.

One of the most interesting aspects of the resolution of the Poincaré Conjecture is the nature of the solution. While the problem is purely topological in its formulation, the proof is not. The proof uses deep techniques and results from other areas of mathematics, namely analysis and differential geometry. It is not at all clear *a priori* that these ideas have any relevance to the Poincaré Conjecture, but in the end they turn out to be the only way (so far) to approach this question successfully.

My goal in this article is to give you a sense of the importance, centrality, and the depth of the Poincaré Conjecture. Then I will discuss surfaces and 3-dimensional spaces and describe how topologists think about them. Next, I will formulate and

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

explain the statement of the conjecture. Then I will give an overview of the ideas that go into the solution – Ricci flow, Ricci flow with surgery, and finite-time extinction for Ricci flow with surgery when applied to a simply connected 3-manifold. The latter will be a very superficial view of the mathematics. I refer the reader to the body of Hamilton's work [2] as well as to Perelman's preprints [11], [13], and [12] for more precise statements of the analytic and geometric results that are needed.

2. Problems in mathematics

2.1. A brief history. The central role of problems in mathematics goes back to the Greeks (at least). From them we have the famous examples of the question of squaring the circle and of doubling the cube using only compass and straightedge, among others[1]. Starting in the 16th century mathematicians challenged each other with problems and by the 18th century learned societies posed problems to the general mathematical community often with prizes awarded for their solution. The most famous set of problems in modern mathematics is Hilbert's 23 problems posed at the International Congress of Mathematicians in Paris in 1900; see [7]. These were posed for an entirely different reason and were of an entirely different order from most of the problems heretofore seen in mathematics. Hilbert's goal was to lay out what he considered central problems across the entire subject, problems, whose solutions and even attempted solutions, he thought would be important, indeed central, for the development of the subject in the century that was about to begin. He introduced his problems, making it clear that he saw them being linked to the future development of the subject by saying "Who among us would not be glad to lift the veil behind which the future lies hidden; to case a glance at the next advances of our science and at the secrets of its development during the future centuries?" Some of the problems were already well known before Hilbert's address, for example the Riemann hypothesis, and others were formulated for the first time by Hilbert. Much progress has been made on many, but not all, of these problems. Some still remain open. And as Hilbert foresaw, they did play an instrumental role in mathematics. They formed the backdrop against which a significant portion of the mathematical development of the 20th century was measured. To solve one of Hilbert's problems was to enter the Mathematical Hall of Fame.

A new list of seven problems was proposed in 2000 by the Clay Mathematics Foundation, the Clay Millennium Problems. As the Clay Foundation makes clear, the choice of the timing (100 years after Hilbert's address) and the location (Paris, the same as the location of Hilbert's address) was explicitly made to honor Hilbert's address and the role his problems had indeed played in twentieth century mathematics. They are also hopeful that their list of problems will have a similar impact on mathematics in the twenty-first century. The problems which they introduced are called the 7 Millennium

[1] For more details on the role of problems in mathematics, see the article by Jeremy Gray in [5].

Problems. Attached to each of the problems is a prize of $1,000,000 for its successful solution. There is one problem on this list in common with Hilbert's list, the Riemann hypothesis. The other six are more recent problems.

One of the Clay Millennium Problems is the Poincaré Conjecture. Aside from the Riemann Hypothesis it is the oldest on the list, dating from 1904. It is the problem whose solution we are celebrating. It is the first of the Millennium Problems to be solved. None of the others seems ripe for solution. But of course, before its solution neither did the Poincaré Conjecture.

2.2. The role of problems. What makes a good problem and what role do problems play in mathematics? Quoting again from Hilbert's address to the International Congress in 1900, "I should still more demand for a mathematical problem if it is to be perfect; for what is clear and easily comprehended attracts, the complicated repels us. Moreover, a mathematical problem should be difficult in order to entice us, yet not completely inaccessible, lest it mock our efforts. It should be to us a signpost on the tortuous paths to hidden truths, ultimately rewarding us by the pleasure in the successful solution."

Hilbert is making several points here. If a problem is sufficiently difficult that it cannot be immediately solved but if it is not so difficult as to be inaccessible, then it will stimulate much mathematical activity and progress as different approaches are tried. History is replete with examples of extraordinary mathematics being created in an attempt to solve a long-standing problem. Sometimes these attempts result in partial solutions or further clarifications of the problem under consideration, other times, the mathematics does not reach its intended target, but ends up being useful in a completely different area. Good problems stimulate mathematical activity both directly related to the problem and in other surrounding areas of mathematics.

Another point that Hilbert is making is that problems become more famous as they resist more and more different attempts at solution, and that, when they reach this status, they are used a measuring stick against which the power of new ideas is tested. If a new idea makes progress on an old and famous problem, then it has demonstrated its originality, depth and power. Of course, solving such long-standing problems bestows honor in the first instance on the solver because he or she has succeeded where all others failed, but also most of the time it is a marker for the progress of the discipline as a whole. Mathematics has matured to the point where rarely, if ever, is the solution of a significant problem the result entirely of the work of a single mathematician. Rather such advances rest on the general advancement of understanding of the subject and the various previously developed techniques available to attack the given problem. In the case of the Poincaré Conjecture I have already referred to the indispensable work of Hamilton on Ricci flow, but Perelman's argument also rests on the modern theory of Riemannian manifolds and the modern theory of various compactness results for spaces of Riemannian manifolds and more general singular objects. This theory has been developed over the last 50 to 60 years by an entire army of mathematicians. Hamilton's work in turn relies on the progress

in partial differential equations on manifolds, especially parabolic equations such as the heat equation and the mean curvature flow equation. Again the workers who developed these techniques are too numerous to list.

To me, the most amazing thing about mathematics is that there are mathematical problems that are hard enough that their solution requires decades if not centuries of work, and yet it is possible by dint of long hard work, many ideas, and incremental advances over time to arrive at a solution. Once the perspective is correct and the technical power is sufficiently developed, they succumb. They are hard not because they are computationally difficult, but because they are conceptually difficult; yet they are not conceptually too difficult that human beings are incapable of solving them. It just takes us a while to get the perspective correct, to get the right position and with the right frame of mind to solve them. That the human race is capable of such advances is cause for celebration by all of us.

3. The Poincaré Conjecture

This brings us to the problem whose solution we are discussing – the Poincaré Conjecture. This problem was originally formulated in 1904 by Henri Poincaré [14] near the end of a long article on 3-dimensional topology. This article laid out many of the basic tenets of topology and marked its beginning as an independent field of mathematical study. At the end of the article, Poincaré states that there remains one central question to be addressed, "Is every simply connected 3-manifold topologically equivalent to the 3-sphere?" In an interesting twist of history, this is not Poincaré's first formulation of such a question. Several years earlier he had asked a similar question where the hypothesis of simply connected is replaced by a related (but we now know) weaker condition. After posing this question, Poincaré realized that he knew how to construct counter-examples to that question and that the way to show that they were indeed counter-examples was to use a topological invariant that he had invented about 10 years before; we call it the fundamental group[2], and in French it is called the 'groupe de Poincaré.' Anyway, using this invariant he showed the answer to his first question was 'no' and then he formulated the question that lasted 100 years.

The Poincaré Conjecture has all the attributes of an excellent problem. It was simple (for the mathematician) to state. It was a generalization of a well-known property of surfaces, so it was a natural guess as to a fundamental fact about 3-dimensional manifolds. While simple to state and while being an obvious generalization of a known mathematical result, it was not easy to resolve, or indeed to make any progress at all on this problem. The problem is a problem purely in topology: the hypotheses are topological and the conclusion is topological. It was attacked by direct topological means for 100 years without any progress; see [18]. Nevertheless, all this effort was not futile. We learned much, just not about this question.

[2]For a formal definition of this group and all other technical terms see the appendix.

3.1. Mathematics generated by the Poincaré Conjecture. The Poincaré Conjecture is an attempt to characterize topologically the simplest of all 3-dimensional manifolds, the 3-sphere. In approaching this question, many techniques were developed to study 3-dimensional manifolds. Some of the most important go back to Papakyriakopoulos [10] in the 1950s. Among these are Dehn's lemma and the loop theorem and the sphere theorem. These are incredibly powerful tools for studying 3-manifolds. For example, they allow one to prove the analogue of the Poincaré Conjecture for knots in the 3-sphere. More precisely, Parakyriakipoulos showed that a knot in the 3-sphere is topologically equivalent to the unknotted circle if and only if the fundamental group of the space obtained by removing the knot from the 3-sphere is the same as the fundamental group of the space obtained by removing the trivial unknotted circle from the 3-sphere. Using these techniques Waldhausen [20], in the 1960s, gave a complete characterization of a large class of 3-manifolds, but unfortunately from the perspective of the Poincaré Conjecture, the class that Waldhausen characterized is at the other end of the spectrum from simply connected 3-manifolds. Here, we see attempts to solve the Poincaré Conjecture leading to enormous progress in a closely related area – the study of other 3-manifolds – but saying nothing about the original conjecture. But this is just the beginning of the story.

In 1960 Smale [17], in one of the most revolutionary advances in topology, realized that it was not the case that manifolds were harder and harder to study as their dimension increased. Before Smale the thinking was: surfaces are understood; we cannot prove central results about 3-dimensional manifolds, so those of higher dimension must be even harder, too hard to even begin to think about until we understand 3-dimensional manifolds. Smale generalized the Poincaré Conjecture to all dimensions (this was fairly obvious) and then proceeded to solve it in the affirmative in all dimensions 5 and higher. This was the revolution. Four years earlier Milnor [8] had shown that a closely related question was false starting in dimension 7. In particular, Milnor showed that the smooth version[3] of the Poincaré Conjecture was not true in higher dimensions. Smale and Milnor each won Fields Medals for the works we have just cited. But this was just the beginning of a 20 year period of unparalleled advances in topology. Using the ideas of Smale and Milnor and others such as René Thom, topologists succeeded in answering almost every question that could possibly be answered about manifolds of dimension 5 and greater. This whole area of topology is known as 'surgery theory,' or 'Browder–Novikov surgery theory' after its two main developers; see [1]. The reason that high dimensional manifolds are easier to study than the ones of dimensions 3 and 4 is that in them there is enough room to move submanifolds (e.g., loops and surfaces) around and put them in good position with respect to each other, whereas in lower dimensional manifolds this is not possible.

By the late 1970s high dimensional manifolds were well understood, and the attention of topologists reverted back to their 'problem children' – dimensions 3 and 4 – and in particular to the Poincaré Conjecture. It was not clear how to proceed. Flushed

[3] See the appendix.

with the success in high dimensions (and dare we say the hubris it engendered), many topologists, myself included, felt that it was just a matter of time before the 'so-called' low dimensions would succumb to our purely topological techniques. Others, in particular Shing-Tung Yau, argued strongly that one needed geometric and analytic tools, for example minimal surfaces and special metrics, to attack these low dimensions. From a different direction, Atiyah and Singer were saying 'Physics takes place in the low dimensions and could well make an impact.' The history of the low dimensions is still being written but the verdict is in and is clear: topologists like myself were wrong; Yau was right; and Atiyah and Singer were right. The evolution to using ever more analysis, geometry, and physics to attack questions about manifolds of dimensions 3 and 4 is the next part of the story of topology and the Poincaré Conjecture.

3.2. Thurston's generalization. The next advance in 3-dimensional topology dates from the late 1970s and early 1980s. Thurston was applying geometric ideas, in particular hyperbolic geometry[4], to 3-dimensional manifolds. His work led him to formulate a general conjecture about all 3-dimensional manifolds, a conjecture that says that they could be cut apart in a very precise way into pieces that had homogeneous 3-dimensional geometries; see [19] and [15], and see also the appendix. The list of all possible 3-dimensional homogeneous geometries was known classically. Examining this list one sees that by far the most interesting case is the hyperbolic geometry that Thurston had been studying. It is also immediate from studying the list of possibilities that the Poincaré Conjecture is a very special case of Thurston's more general conjecture. So here we have the first real progress on the Poincaré Conjecture. This progress consists in embedding the Poincaré Conjecture as a special case of a vastly more general conjecture about all 3-dimensional manifolds. Thurston's work also established many special cases of his general conjecture, but not a case that related directly to the Poincaré Conjecture. One effect of this was that Thurston's work convinced most topologists that his conjecture and therefore the Poincaré Conjecture was most likely true. (Some would have said definitely true.) For his work Thurston received a Fields Medal in 1982.

3.3. Resolution in dimension four. In the early 1980s there were two advances in dimension four. M. Freedman [4] managed to push the higher dimensional arguments down into dimension four and to prove the four-dimensional version of the Poincaré Conjecture, leaving only the original 3-dimensional version of the conjecture open. This argument required crinkling various surfaces inside the four-dimensional manifold infinitely badly in order to get them to fit and the argument could not be made to work with smooth surfaces. Freedman's work not only solved the four-dimensional Poincaré Conjecture, it applied to all simply connected four-manifolds. (Unlike dimension three, there are many simply connected four-manifolds.) At almost the same time, Donaldson [3], using the Yang–Mill's equations from physics, showed that

[4] See appendix.

the analogues of Freedman's results definitely did not hold for smooth manifolds. Freedman and Donaldson each received a Fields Medal in 1986 for their work on four-dimensional manifolds.

At this point, 1986, the situation is the following: The Generalized Poincaré Conjecture has been resolved affirmatively in all dimensions except dimension three. It is understood that in dimensions four and higher there is a difference between studying smooth manifolds and topological manifolds, something that was unsuspected by Poincaré and anyway does not occur in dimension three. Manifolds of dimension five and higher, and simply connected topological 4-manifolds were well understood. For all the work in topology related to the Poincaré Conjecture a total of five Fields Medals over a period of 28 years had been awarded. At the end of this unbelievable fertile period the main outstanding problem was exactly the same as it was at the beginning – the Poincaré Conjecture in its original formulation. Furthermore, all direct topological attacks on this problem had yielded no results at all – no special cases had been solved, no reductions of the problem had been made that showed promise of yielding essential new insights. While there had been incredible advances in understanding manifolds, what had been clear from the 1950s had been confirmed by these advances: the Poincaré Conjecture was the central problem in topology.

4. Method of solution

There was, however, progress being made in a different area of mathematics that would eventually pave the way for a solution of the Poincaré Conjecture. In 1982 Richard Hamilton had developed enough of the theory of the Ricci flow to prove that a compact 3-manifold admitting a Riemannian metric[5] of non-negative Ricci curvature in fact admits a Riemannian metric of constant positive sectional curvature; see [6]. In particular, if such a manifold is simply connected, then a classical theorem, essentially going back to Riemann, implies that the Riemannian manifold is isometric to the 3-spheres. In particular, the manifold is diffeomorphic to the S^3. While this might seem significant progress on toward the Poincaré Conjecture, the fact that the hypothesis of Hamilton's theorem is geometric (non-negative Ricci curvature) and the fact that there was no known way to construct such metrics, meant that while this was a beautiful theorem in geometric analysis it was not apparent that it represented real progress on the Poincaré Conjecture. It suggests that it might be possible to attack the Poincaré Conjecture in this way, but whether this method is fruitful for such an attack had to await further developments. For a general survey of Ricci flow, including most of Hamilton's papers, see [2].

There was, however, an interesting relationship, which according to Hamilton was first pointed out to him by Yau, between Thurston's more general conjecture and Ricci

[5]We discuss Riemannian metrics and curvature in more detail in Section 6 and Ricci flow in more detail in Section 7.

flow. This relationship operates at two levels. To a first approximation, Thurston's conjecture posits that a 3-manifold admits a nice metric. Thus, in this more general conjecture the hypotheses remain topological but the conclusion is geometric. If we are searching for such a nice metric, then we can hope to find it by geometric or analytic techniques. Based on the analogy with the heat flow, one expects Ricci flow to produce such nice metrics. Indeed, in Hamilton's result, cited above, this is exactly what happens. This is the reasoning that led Hamilton to hope to apply his evolution equation for a Riemannian metric, the Ricci flow equation, to the more general problem of constructing homogeneous metrics on 3-manifolds, that is to say to attack Thurston's more general conjecture by using Ricci flow. But this reasoning can be pushed further to operate at a deeper level, Thurston's conjecture requires a cutting or a surgery of 3-manifolds before finding pieces admitting nice metrics. On the other hand, the Ricci flow equation, like most non-linear parabolic equations, develops finite-time singularities that must be dealt with. It seems conceivable that these issues are of a similar nature. Maybe cutting away the finite-time singularities in order to continue the Ricci flow would exactly lead to the cutting process required in Thurston's conjecture. This then was the idea: use the Ricci flow on all 3-manifolds and the singularity development will exactly mimic the cutting process required by Thurston's conjecture.

To study the Ricci flow and to prove results that are relevant to 3-dimensional topology requires a detailed and delicate analytic and geometric analysis of the Ricci flow equation and the properties of its solutions. So approaching the Poincaré Conjecture and the more general geometrization conjecture of Thurston's in this way changes the mathematical techniques and results required to solve the topological problem from topological ones (which had been attempted without success) to geometric and analytical ones, which are more refined and hence hold out the possibility of being more powerful, but of course use many deep analytic results and delicate analytic techniques.

Hamilton established some beautiful results about singularity development in Ricci flow on 3-manifolds which were suggestive that the entire program might be made to work, but he could not get good enough control on the singularities that develop in finite time to prove that he could always do surgery and continue the process. Here is where Perelman enters the story. He realized that in addition to the properties that Hamilton had established there was one more crucial one that Hamilton had not considered, a volume non-collapsing result. Perelman introduced a beautiful new concept, unlike anything in Hamilton's work, that allowed him to establish that this extra property holds in general when dealing with Ricci flow on compact 3-manifolds. Then using a delicate combination of blow-up limits and inductive arguments he was able to show that one could always do surgery, and that after surgery the same properties hold. This allowed him to repeatedly perform surgery and create a more general flow, which is called a Ricci flow with surgery, defined for all positive time. It remained only to show that the limits as time goes to infinity of a Ricci flow with surgery satisfies Thurston's conjecture to conclude that the initial manifold does. In the case

of the simply connected manifolds, Perelman showed that the Ricci flow with surgery eventually leads to an empty manifold. (This is analogous to, though more complicated than, Hamilton's result about what happens when one starts with positive Ricci curvature.) From this Perelman immediately deduced the Poincaré Conjecture.

5. Statement of the Poincaré Conjecture

Poincaré derived his conjecture for 3-manifolds by arguing by analogy from what was well known for surfaces by 1900. Recall the classification of surfaces. (All surfaces are implicitly closed, and oriented.) These are classified by one invariant: the genus g, which is an integer ≥ 0. The two-sphere is the only surface, up to equivalence, of genus 0. The torus, i.e., the surface of a doughnut, is the only surface of genus 1, etc. One can view the surface of genus g as the result of removing from a two-sphere g pairs of disks (with all $2g$ disks being disjoint) and sewing in a cylinder (i.e., an annulus) between each pair of boundary circles, so that g annuli are glued to the sphere with the disks removed.

Let me say a word about what a surface is and what equivalence means in this context. A surface is a space that locally looks like the Euclidean plane. This means that near every point one can impose two local coordinate functions that behave like the x and y coordinates in the plane near some point. For example, on the surface of the earth in a Mercator projection we normally use latitude and longitude. Of course, near the pole we use polar coordinates. On a torus we could use the angles in each of the product circles. There is no requirement here that the coordinates extend over the entire surface or even almost all of it, they need only be defined in a neighborhood of a point. But each point has such local coordinates. There is also no assumption about how different systems of coordinates are related to each other. What I am describing here is technically a topological manifold. A closely related notion is that of a smooth of C^∞-manifold. Here as one passes from one coordinate system to another there is an assumption that the coordinate functions in one system are smooth, i.e., infinitely differentiable, functions when expressed in terms of the other coordinate system. It is important to note that there are not chosen or distinguished coordinates near any point. All possible coordinate systems are on an equal footing. Thus, there is no natural notion of a metric or distance function on a topological or smooth surface. The advantage of smooth manifolds is that one can do calculus, have differential equations, etc. So, for example, a Riemannian metric only makes sense on a smooth manifold, so that the Ricci flow equation exists for smooth manifolds (with Riemannian metrics) but not for topological manifolds.

Now to the notion of equivalence. For topological manifolds it is homeomorphism. Namely, two topological manifolds are equivalent (and hence considered the same object for the purposes of classification) if there is a homeomorphism, i.e., a continuous bijection with a continuous inverse, between them. Two smooth manifolds are equivalent if there is a diffeomorphism, i.e., a continuous bijection with a

continuous inverse with the property that both the map and its inverse are smooth maps, between the manifolds. Milnor's examples were of smooth 7-dimensional manifolds that were topologically equivalent but not smoothly equivalent to the 7-sphere. That is to say, the manifolds were homeomorphic but not diffeomorphic to the 7-sphere. Fortunately, these delicate issues need not concern us here, since in dimensions two and three every topological manifold comes from a smooth manifold and if two smooth manifolds are homeomorphic then they are diffeomorphic. Thus, in studying 3-manifolds, we can pass easily between two notions. Since we shall be doing analysis, we work exclusively with smooth manifolds.

The statement that there is a unique smooth surface up to equivalence for each $g \geq 0$ means that associated to every (closed, oriented) smooth surface is an invariant, called the genus (it is the number of holes), and for every $g \geq 0$ there is a smooth surface of genus g and any two such are diffeomorphic. Above, I have briefly described how to construct a surface of genus g for any $g \geq 0$. Now to the punch line for surfaces, the jumping-off point for Poincaré. For any surface of genus $g > 0$ (i.e., for any surface not equivalent to the sphere) there is a loop on the surface that cannot be continuously deformed to a point; namely, take a loop that 'goes around' one of the holes. The situation for the two-sphere is the opposite. Any loop on the two-sphere can be continuously deformed to a point: Imagine that the loop misses the north pole and then contract it along lines of longitude to the south point.

Thus, the simplest of all surfaces, the 2-sphere, is characterized by the property that every loop on the surface deforms continuously to a point. That is to say, the sphere is, up to equivalence, the only surface with this property. If every loop in a space deforms continuously to a point, then we say that the space is *simply connected*.

Poincaré Conjecture is the conjecture that the analogous statement holds for (closed, oriented) 3-manifolds.

The Poincaré Conjecture. A (closed) 3-manifold is topologically equivalent to the 3-sphere if and only if it is simply connected.

The argument showing that the 2-sphere is simply connected applies equally well to the 3-sphere, or indeed any sphere of any dimension greater than 1. Thus, the real import of the Poincaré Conjecture is that a simply connected 3-manifold is topologically equivalent to the 3-sphere. For more details on the history of the Poincaré Conjecture see [9].

5.1. A description of the 3-sphere. How should we think of the 3-sphere? By definition, it is the subset of points in Euclidean four-space at distance one from the origin:

$$S^3 = \left\{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\right\}.$$

Stereographic projection from the north pole $(0, 0, 0, 1)$ gives an identification of the complement of the north pole in S^3 with the Euclidean 3-space, so that we can view S^3 as a compactification of $\mathbb{R}^3$ by adding one point at infinity. More useful for

what follows, we can identity each of the northern hemisphere $S^3 \cap \{x_4 \geq 0\}$ and the southern hemisphere $S^3 \cap \{x_4 \leq 0\}$ with 3-balls, and then realize S^3 as the union of two 3-balls with their boundaries glued together (or identified with each other).

5.2. Presentation of any 3-manifold. This latter description of the 3-sphere has a generalization that can be used to present every 3-manifold, up to equivalence. This presentation uses solid handlebodies. Consider a compact 3-manifold with boundary obtained in the following way. Begin with the compact 3-ball in 3-space and attach some number, g, of solid handles (two-disks cross the interval) along their ends (two-disks cross the boundary of the interval). This makes a solid subset of 3-space whose boundary is a surface of genus g. The solid (i.e., 3-dimensional object) is called a solid handlebody of genus g. We can make a 3-manifold by taking two solid handlebodies of genus g and gluing their entire boundaries together by a topological equivalence. A note of caution is probably in order here: there are many ways to do this gluing, i.e., many essentially different topological equivalences between the boundaries. Using different equivalences to glue will often result in different 3-manifolds. It is a fairly direct theorem in topology that every 3-manifold is obtained by this construction for some g and some gluing identification. Such a presentation of a 3-manifold is called a Heegaard decomposition and the genus of the handlebodies is called the genus of the Heegaard decomposition. Gluing two 3-balls together by an equivalence of the S^2 always yields a 3-manifold equivalent to S^3. Thus, the 3-sphere is characterized as the only 3-manifold with a Heegaard decomposition of genus 0. It is also a direct computation to deduce from the Heegaard decomposition of a 3-manifold a presentation for the fundamental group of the resulting 3-manifold. Of course, the problem here is that the 3-sphere has many other Heegaard decompositions. In fact every 3-manifold has infinitely many different Heegaard decompositions, and indeed has Heegaard decompositions of arbitrarily high genus. The direct topological approach to proving the Poincaré Conjecture is to use the information that the manifold is simply connected, which gives some information about the Heegaard decomposition, and use this information to show that the Heegaard decomposition can be reduced by the allowable moves to one of genus zero. Fortunately, there is a finite (and quite short) list of 'moves' that describe how to get from one Heegaard decomposition to any other. Unfortunately, this process is ineffective in the sense that knowing, say, the genus of the two-decompositions there is no bound to the number of moves that may be required nor the maximal genus of the Heegaard decompositions that occur in the 'path' of moves connecting the two given ones.

Another possibility, similar in spirit to much of the recent work in low dimensional topology, would be to establish a counter-example to the Poincaré Conjecture by defining a new invariant associated to Heegaard decompositions that remained invariant under the allowable moves, an invariant beyond the fundamental group, and then find a Heegaard decomposition that was simply connected yet where this more refined invariant differed from that of the 3-sphere.

In spite of much effort over a period of 100 years, no one was ever able to carry out either of these approaches successfully.

6. Riemannian metrics and Curvature

There was no progress on the Poincaré Conjecture coming from a direct topological attack. Rather the mathematical progress that would eventually lead to the solution was coming from the study of a certain evolution equation, the Ricci flow equation, for Riemannian metrics on manifolds. In order to set the stage for describing these advances, we leave the realm of topology and pass to differential geometry, in particular Riemannian geometry. A Riemannian metric on a smooth manifold is a smoothly varying, positive definite inner product on the tangent spaces of the manifolds. These inner products allow us to measure lengths of tangent vectors and angles between tangent vectors at the same point of the manifold. To say that the inner products vary smoothly means that the inner product of two smooth vector fields is a smooth function. Once we have a Riemannian metric, we can measure the length of any smooth curve in the manifold, and then by minimizing the lengths of smooth curves with given endpoints we construct an ordinary distance function (i.e., metric) on the manifold. The Riemannian metric however is more subtle and powerful than the resulting distance function. A diffeomorphism between Riemannian manifolds is said to be an *isometry* if it preserves the Riemannian metrics and the manifolds are said to be *isometric*. For example, the 3-sphere receives a Riemannian metric from its natural embedding in Euclidean 4-space. Given two tangent vectors to the 3-sphere, their inner product is their usual inner product in 4-space.

Let us try to understand the nature of the space of all Riemannian metrics on a given manifold. Associated to any manifold there is an infinite dimensional vector space of all smoothly varying contravariant, symmetric two-tensors on that manifold. Inside this vector space is the open cone of positive definitive ones. This positive cone is the space of Riemannian metrics on the manifold. If we work in a set of local coordinates $(x^1, \ldots, x^n)$ on the manifold, then the metric is written as

$$g_{ij}(x^1, \ldots, x^n) dx^i \otimes dx^j$$

where g_{ij} is a symmetric matrix of smooth functions on the coordinate patch, positive definite at every point of the coordinate patch. Of course, if we change the local coordinates the matrix g_{ij} changes; it transforms as a tensor. This means that one cannot view the matrix itself as an invariant of the metric since it depends on the local coordinates we choose to express the metric. One can ask for example, for which (local) metrics are there local coordinates in which the metric is the usual Euclidean metric $g_{ij}(x^1, \ldots, x^n) = \delta_{ij}$? The answer goes back to Riemann, and we will attempt to explain it below. We shall also need the inverse to the metric: in the local coordinates it is denoted g^{ij}, where g^{ij} is the inverse matrix to g_{ij}.

Let us begin with the case of surfaces where the results essentially go back to Gauss. Let Σ be a surface with a Riemannian metric and consider a point $p \in \Sigma$. For each $r > 0$ sufficiently small, the ball $B(p, r)$ of radius r centered at p will have an area $A_{\Sigma,p}(r)$. If Σ is the Euclidean plane then $A_{\Sigma,p}(r) = \pi r^2$. Gauss curvature is a measure of the difference of the area $A_{\Sigma,p}(r)$ and πr^2. More precisely, we consider

$$K_\Sigma(p) = \lim_{r \mapsto 0} \frac{12(\pi r^2 - A_{\Sigma,p}(r))}{\pi r^4}.$$

It turns out that this limit exists and is finite, and the result is a smooth function on Σ. This function is called the Gauss curvature of Σ. The intuitive idea is the following. If we take the cap of an orange peel, then there is less area in this cap than in a disk in the plane of the same radius. This is evident if we press the orange peel flat. It will tear because there is not enough of it to be pushed flat. This deficit of the area as compared to Euclidean area is a reflection of the fact that the orange peel (which is basically part of a 2-sphere) has positive curvature. On the other hand, if we perform the same construction with a small disk on a rolled up cylinder, then it will flatten out without tearing since in fact we could have made the cylinder in the first place from rolling up a flat sheet of paper and this rolling does not change the Riemannian metric. The cylinder is flat, that is to say it has zero Gauss curvature.

For higher dimensional manifolds curvature is a much more complicated algebraic object than a smooth function on the manifold. Every two-dimensional direction at every point in the manifold has a Gauss-type curvature, called the sectional curvature in that direction at that point. These fit together to make a contravariant four-tensor called the Riemannian curvature tensor. The best way to view it is the following: to each two-plane in the tangent space at a point we have a sectional curvature, which is a number. These sectional curvatures fit together to define a quadratic form, the Riemann curvature tensor, on the linear space generated by the two-planes at each point. In terms of local coordinates the Riemann curvature tensor is expressed as

$$\mathrm{Rm} = R_{ijkl} dx^i \otimes dx^j \otimes dx^k \otimes dx^l.$$

It has three symmetry properties: (i) skew symmetry in the first two variables, (ii) skew symmetry in the last two-variables, and (iii) symmetry under interchange of the first pair and the second pair. The first property is expressed by $R_{ijkl} = -R_{jikl}$. It is a direct consequence of the definition. The second property is expressed by $R_{ijlk} = -R_{ijkl}$. It is a consequence of the fact that R_{ij} is an infinitesimal orthogonal automorphism of the tangent spaces, and the usual fact that the Lie algebra of the orthogonal group is the Lie algebra of skew symmetric matrices. The third property is expressed by $R_{klij} = R_{ijkl}$.

We will often denote the Riemann curvature tensor of a Riemannian manifold at a point x by $\mathrm{Rm}(x)$. In the case of a flow of metrics $g(t)$ we will denote the Riemann curvature tensor at the point x under the metric $g(t)$ by $\mathrm{Rm}(x, t)$.

According to results that go back to Riemann, the basic invariant of a Riemannian metric is its curvature, that is to say, its Riemann curvature tensor. For example, there

are local coordinates in a point of a Riemannian manifold in which the metric becomes the usual Euclidean metric if and only if the Riemann curvature tensor vanishes near the point in question. Similarly, a neighborhood of a point p in a Riemannian manifold is isometric to an open subset in the sphere of radius r if and only if all the sectional curvatures are constant and equal to r^{-2} near that point (or equivalently, if the Riemann curvature tensor viewed as a symmetric endomorphism of the second exterior power of the tangent bundle is diagonal with diagonal entries r^{-2}).

In the end, it is this result that is used to finish off the proof of the Poincaré Conjecture. Every smooth manifold has a Riemannian metric; but unfortunately it has an infinite dimensional space of them. Nevertheless, we can view the Poincaré Conjecture as saying that any simply connected manifold has a metric of constant positive curvature. The way to find this metric is to use Ricci flow starting with any Riemannian metric and show that under this evolution the metric tends to a Riemannian metric of constant sectional curvature. From this it is an easy and classical step to show that the Riemannian manifold is isometric to the 3-sphere.

7. Ricci curvature and the Ricci flow equation

A Riemannian metric g on a manifold is a point in an open cone in the infinite dimensional vector space of sections of the symmetric square of the cotangent bundle of the manifold. It follows that, formally at least, the tangent space to the space of all metrics on a manifold is the vector space of sections of the symmetric square of the cotangent bundle of the manifold. The Riemann curvature is a section of the symmetric square of the second exterior power of the cotangent bundle and hence does not have the correct tensor structure to be a tangent vector to the space of Riemannian metrics. There is however a curvature derived from the Riemann curvature tensor that does have the correct tensor structure. That is the Ricci curvature. It is the symmetric two-tensor given in local coordinates by $\mathrm{Ric}(g) = \mathrm{Ric}_{ik}\, dx^i \otimes dx^k$ where

$$\mathrm{Ric}_{ik} = g^{jl} R_{ijkl}$$

is the trace of the Riemannian curvature tensor on the second and fourth indices. The symmetry properties of the Riemannian curvature tensor translate into the fact that $\mathrm{Ric}_{ik} = \mathrm{Ric}_{ki}$, i.e., that the Ricci curvature is a symmetric two-tensor. The Ricci flow equation as written down by Hamilton is

$$\frac{\partial g}{\partial t} = -2\,\mathrm{Ric}_g,$$

or written in local coordinates

$$\frac{\partial g_{ij}}{\partial t} = -2\,\mathrm{Ric}_{ij}\,.$$

A solution, or a *Ricci flow*, is a smooth one-parameter family of metrics $g(t)$, parameterized by t in a non-degenerate interval, on a fixed smooth manifold, a family

satisfying this equation. Again we use the notation $\mathrm{Ric}(x)$ to denote the Ricci curvature at the point x and for a Ricci flow we denote by $\mathrm{Ric}(x, t)$ the Ricci curvature at the point x under the Riemannian metric $g(t)$.

The Ricci flow equation is an evolution equation for the Riemannian metric on a manifold, modeled on the heat equation which is mathematical model for heat flow. The intuition is that this equation should distribute the curvature equally over the manifold in much the same way as the heat equation distributes heat equally. There is one significant difference between these two situations, a difference that arises because the Ricci flow equation is non-linear. It has a correction term that is quadratic in the curvature (but involves no derivatives of the curvature). This quadratic term becomes dominant in regions where the curvature is large. As a consequence, this evolution equation can (and often does) develop singularities in finite-time. As the singularities develop the curvature is becoming unbounded and the non-linearities govern the equation.

There is one other curvature that plays an important role in the story, that is the scalar curvature. It is the trace of the Ricci curvature: $R = g^{ik}\,\mathrm{Ric}_{ik}$. The scalar curvature at a point x is denoted $R(x)$ and in the case of a Ricci flow the scalar curvature at a point x under the metric $g(t)$ is denoted $R(x, t)$.

8. Applying Ricci flow to find good metrics

Hamilton showed that given a compact Riemannian manifold then there is a solution to the Ricci flow equation with this manifold as the initial condition and this solution is unique. Of course, one issue that plays a huge role when one uses this evolution equation is the development of singularities at finite-time $T < \infty$. As we indicated above these occur when the norm of the Riemann curvature (or indeed the scalar curvature) of $(M, g(t))$ becomes unbounded as t approaches T. Let me give one simple example of this phenomenon. Begin with an n-sphere (S^n, g_0) of constant sectional curvature $(n-1)$, then the Ricci curvature is equal to the metric: $\mathrm{Ric}(g_0) = g_0$. We see that $g(t) = (1-2t)g_0$ solves the Ricci flow equation. Notice that this solution becomes singular at $T = 1/2$, and that as t approaches T, the manifold $(M, g(t))$ shrinks to a point in the sense that its diameter goes to zero. Also, notice that its sectional curvatures go uniformly to infinity as we approach the singular time $t = 1/2$.

Another closely related example is to take as the initial manifold $S^2 \times \mathbb{R}$ where the Riemannian metric is the product of a round metric on S^2 with the usual Euclidean metric on $\mathbb{R}$. Then the Ricci flow is the product of a shrinking family of round 2-spheres with the trivial flow on $\mathbb{R}$. Again we have a finite-time singularity and as we approach the singularity the manifold is shrinking to a line.

There is a more general result along these lines due to Hamilton. Suppose that $(M, g(0))$ is any compact Riemannian 3-manifold of positive Ricci curvature. Then the Ricci flow $(M, g(t))$ develops a finite-time singularity at some time $T < \infty$ and as $t \to T$ from below, the manifolds $(M, g(t))$ are shrinking to points and the metric

is becoming round. This example is reassuring in the sense that even though a finite-time singularity develops, as that singularity develops, the metric (rescaled to have a constant diameter) is converging to the metric for which we are searching.

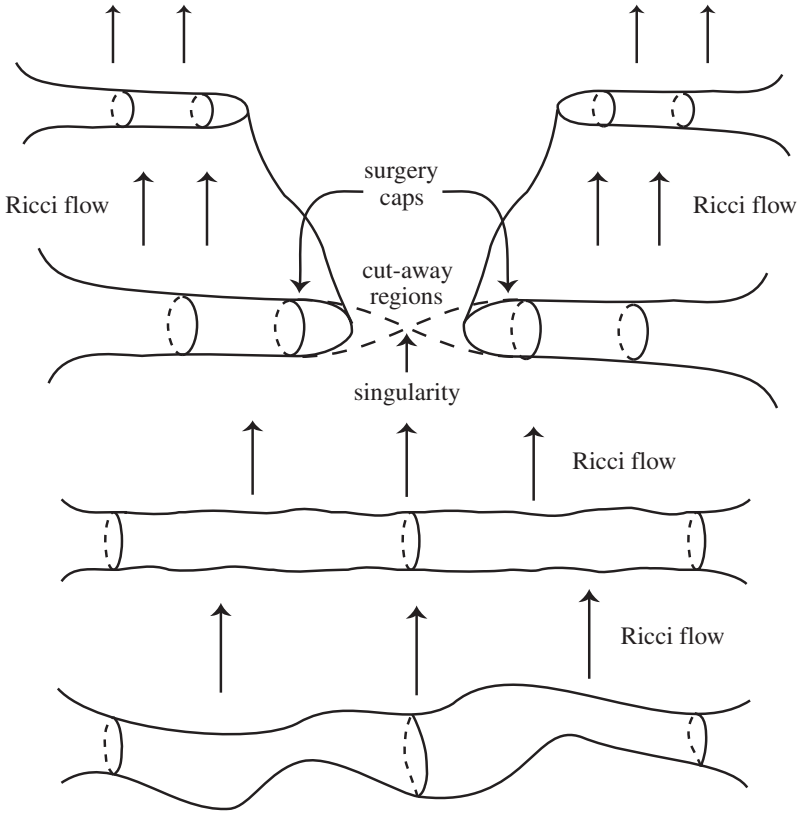
In one way these examples are prototypical; in another they are very special. What is typical is that in general every finite-time singularity is associated with manifolds of non-negative curvature. What is atypical is that, unlike these examples, in general singularities develop along proper subsets of the manifold not everywhere in the manifold. This means that in order to prove results about the topology or geometry of the entire manifold one must extend the Ricci flow past the finite-time singularities. This requires a detailed and refined understanding of models for all singularities that can arise at finite time. It also requires extending all the basic results about Ricci flows to the more general flows that are constructed in extending past the singularities.

Hamilton laid out a program to do this and began a systematic study of the finite-time singularities. His results represented steps in the right direction, but much more was needed. In his first preprint on the subject [11], Perelman introduced a new ingredient, which he calls volume non-collapsing[6]. He showed that as singularities develop, they are volume non-collapsed on the scale of their curvature. With this extra condition Perelman was able to give a complete qualitative classification of models for singularity development: every singularity at finite-time is either modeled on a manifold of positive curvature, modeled on a manifold made up of long thin necks, or modeled on a manifold made up of a long thin neck capped off with a 3-disk or a punctured real projective 3-space, $\mathbb{R}P^3$. Furthermore, Perelman established strong analytic control on the time derivatives and the norm of the gradient of the scalar curvature in regions of high curvature.

9. Ricci flows with surgery

Suppose that we have a 3-dimensional Ricci flow $(M, g(t))$, $a \leq t < T$, going singular at time $T < \infty$. In his second preprint on Ricci flow [13], Perelman extends this flow past time T by constructing a Ricci flow with surgery. To do this he makes use of the classification of finite-time singularities described above. At the singular time T there is a limiting metric (possibly incomplete) defined on an open submanifold $\Omega \subset M$. The ends of Ω are diffeomorphic to $S^2 \times [0, 1)$, with metrics near any point that look like a rescaled version of a product of a round metric on S^2 with the Euclidean metric on the interval, and with the curvature tending to infinity as one approaches the end. Surgery consists in cutting off the ends of these tubes along one of the 2-spheres in the product structure and sewing in a 3-ball to construct a new compact Riemannian 3-manifold $(M', g(T))$ which will be the time-slice of the Ricci flow with surgery at time T. One restarts the Ricci flow at time T using $(M', g(T))$ as the initial metric. This flow will go singular at some time $T' > T$. See the figure below.

[6] See appendix.



Surgery

It is best to view a 3-dimensional Ricci flow with surgery as a 4-dimensional space-time with a given time function t to $\mathbb{R}$. There is a discrete set of singular times (in the above example there is only singular time T). If $T_1 < T_2$ are successive singular times, then the part of space-time, $t^{-1}([T_1, T_2))$, is simply a product of the T-time-slice with the interval $[T_1, T_2)$, and the Ricci flow with surgery on this part of space-time is the usual Ricci flow. As we cross a singular time both the topology and the geometry of the time-slice change, but in a controlled way as indicated above.

In [13] Perelman shows that, starting with any compact Riemannian 3-manifold, this process can be repeated forever to construct a Ricci flow with surgery defined for all positive times. Furthermore, the singular times are discrete, and the topology of the manifold before surgery is easily deduced from the topology after surgery. In particular, it is easy to see from the description of the topological change as one crosses a singular time, that if the manifold after a surgery satisfies Thurston's geometrization conjecture, then the manifold just before that surgery also satisfies Thurston's geometrization conjecture. Arguing by induction we see that if any time-slice of this

Ricci flow with surgery satisfies Thurston's geometrization conjecture, then so does the initial manifold.

10. Completion of the proof of the Poincaré Conjecture

Let M be a closed, simply connected 3-manifold. To prove the Poincaré Conjecture for M, namely to prove that M is diffeomorphic to the 3-sphere, we shall show that it satisfies Thurston's geometrization conjecture, which means that it has a Riemannian metric of constant positive curvature. From there, it is easy to see that it is diffeomorphic to the 3-sphere. Fix any Riemannian metric $g(0)$ on M. (Remember there is an infinite dimensional space of possibilities.) Now construct the Ricci flow with surgery defined for all time with $(M, g(0))$ as the 0 time-slice. As we noted above, if we can show that any time-slice of this Ricci flow satisfies Thurston's geometrization conjecture, then so does M. So the proof of the Poincaré Conjecture is completed by showing that the time-slices of this Ricci flow with surgery at all sufficiently large times are empty, that is to say the Ricci flow with surgery becomes extinct at some finite-time, just as Hamilton showed for the Ricci flow in the case when the Ricci curvature is positive.

The special property that Perelman uses about a homotopy 3-sphere in [12] in order to prove the above finite-time extinction result is the fact that its second homotopy group vanishes and its third homotopy group is non-trivial. Associated to a non-trivial element in the third homotopy group of a Riemannian manifold is a geometric invariant. This invariant is the area of a certain disk related to the homotopy element, so that in particular the invariant is always non-negative. On the other hand, Perelman shows that as long as the Ricci flow with surgery starting with a homotopy 3-sphere does not become extinct, the derivative of this invariant is bounded above by a function that eventually becomes negative and stays bounded away from zero. This means that the invariant would have to become negative in finite-time, if the Ricci flow with surgery does not become extinct. This is impossible, showing that the Ricci flow with surgery does become extinct in finite-time.

11. Status of the Geometrization Conjecture

It seems quite likely that one can apply the existence of a Ricci flow with surgery, starting with any compact manifold, to establish the complete classification of 3-manifolds as posited by Thurston's conjecture. For example, the arguments of the previous section apply to any prime manifold with non-trivial π_2 or π_3. The Ricci flow with surgery starting at such a manifold becomes extinct in finite time, and hence these manifolds satisfy Thurston's conjecture. To classify all 3-manifolds, one must understand the nature of the limits as t tends to infinity of the t time-slices. In [13] Perelman, following similar earlier arguments of Hamilton, showed that for

all sufficiently large t the time t time-slice M_t of a Ricci flow with surgery contains a finite collection of tori (and Klein bottles) whose fundamental groups inject into the fundamental group of M_t. Furthermore, the complementary components are of two general types: those of the first type admit a complete hyperbolic metric of finite volume, and those of the second type are collapsed, in the sense that they are, locally at least, metrically close to lower dimensional spaces, spaces of dimension 1 or 2. To complete the proof of Thurston's conjecture one must show that the complementary components of the second type are unions of generalized circle bundles and 2-torus bundles where the union takes place along boundary tori whose fundamental group injects into the fundamental group of M_t.

Perelman has stated such a result at the end of [13], and there is a closely related result in [16], which relies on an earlier, unpublished result of Perelman. The evidence is quite strong that these arguments will withstand scrutiny, but it is still too early to say that this result has been established.

12. Future applications of Perelman's work

Ironically enough Perelman's proof of the Poincaré Conjecture, and even the proof of the Geometrization Conjecture, assuming that it withstands scrutiny, will have little effect of 3-dimensional topology. Those working in the subject either were already assuming these results were true, were working on hyperbolic 3-manifolds, where by definition Thurston's conjecture holds, or were working on the properties of various algebraic, combinatorial, and geometric invariants of 3-manifolds, invariants that seem, at the present moment, to have little to do with the classification of 3-manifolds. I believe the deepest impact of Perelman's work will lie elsewhere.

One obvious area where these ideas will have impact is in the area of 4-dimensional manifolds. We know much less about smooth 4-manifolds than we do about smooth 3-manifolds, and there are many significant questions to face before there can be full application of the Ricci flow techniques to the study of 4-manifolds. These questions include the nature of Einstein 4-manifolds (the fixed points up to scaling of the Ricci flow), as well as an extension of the curvature pinching results of Hamilton and the collapsing results of Perelman, et al., to four dimensions. Still, this is an area where there seems much possibility for future advances.

Another area, where progress is already being seen, is the area of the Kähler–Ricci flow – Ricci flow on Kähler manifolds. Here many of the analytic problems disappear, and there is much more understood about Ricci flow.

Lastly, and more speculatively, Perelman's techniques give one strong control over singularity development in the Ricci flow for compact 3-manifolds. There are many evolution equations in both mathematics and in mathematical models of physical phenomena that are evolution equations which share many properties with Ricci flow. Understanding of singularity development in these equations could have significant influence both in mathematics and in the study of physical phenomena.

These applications, however significant, lie in the future. What we are discussing today is a milestone – the application of Ricci flow and Perelman's breakthroughs to the proof of one of the most central and long-standing problems in mathematics. That alone is enough to demonstrate the power and originality of the techniques.

Appendix. Formal definitions

The fundamental group: For any topological space X with a chosen point, $x \in X$, called the base point, the *fundamental group* $\pi_1(X, x)$ is defined. The elements of this group are deformation classes of loops based at x. The multiplication is given by composing loops. The identity element of the group is the class of the trivial loop at the base point and the inverse of the class of a loop is the class of the loop with the direction reversed.

Topological and smooth manifolds. By definition every point in a topological n-manifold has a neighborhood that is homeomorphic to a neighborhood in Euclidean n-space. Transferring the usual coordinates on Euclidean space by this homeomorphism gives us local coordinates on this neighborhood of the point. Thus, every point in a topological manifold has a neighborhood with local coordinates like those obtained by restricting the usual Euclidean coordinates to an open subset of Euclidean n-space. If two coordinate systems overlap, then the coordinate functions in one system are continuous functions of the other coordinates. A *smooth manifold* or equivalently a *smooth structure* on a topological manifold is a choice of a subset of coordinate systems covering the entire manifold so that when two of the chosen coordinate systems overlap, the coordinate functions of one system are infinitely differentiable functions of the other coordinates. Amazingly enough, Milnor's results show that starting in dimension 8, it is not always possible to find a smooth structure on a topological manifold, and starting in dimension 7 it is possibly to have non-isomorphic smooth structures on a topological manifold, in fact on the 7-sphere. The work of Freedman [4] and Donaldson [3] show that the theory of smooth 4-manifolds differs enormously from the theory of topological 4-manifolds.

Hyperbolic geometry. Hyperbolic space of dimension n can be thought of as the n-dimension sphere of radius i, and hence of constant curvature -1. The solutions to the equation

$$-x_0^2 + x_1^2 + \cdots + x_n^2 = -1$$

in $(n+1)$-space form a two-sheeted hyperboloid. Hyperbolic n-space is the upper sheet of this hyperboloid, i.e., the intersection of this locus with $\{x_0 > 0\}$. Its group of isometries is the subgroup of index two of the automorphism group preserving the quadratic form $Q(x_0, \ldots, x_n) = -x_0^2 + x_1^2 + \cdots + x_n^2$ preserving the two-sheets. Hyperbolic manifolds are obtained by taking the quotient of hyperbolic space by discrete subgroups of the isometry group that act freely on hyperbolic space.

Homogeneous 3-dimensional manifolds. Homogeneous 3-dimensional manifolds are by definition 3-dimensional manifolds of the form G/H where G is a connected Lie group and $H \subset G$ is a compact, connected subgroup. For example, S^3 is homogenous because it can be written as the quotient $\mathrm{Spin}(4)/\mathrm{Spin}(3)$. Hyperbolic space of dimension three, is written as the quotient $\mathrm{SL}(2,\mathbb{C})/\mathrm{SU}(2)$. There are 9 possibilities that lead to 3-dimensional quotients. A locally homogeneous manifold is then the quotient of G/H by a discrete subgroup $\Gamma \subset G$ that acts freely on G/H. We are only concerned with those G/H that admit cofinite volume discrete subgroups Γ. This leaves only 8 three-dimensional examples. The most interesting locally homogeneous 3-manifolds are the hyperbolic ones. All others are easily classified and give fairly simple examples.

Cutting apart 3-manifolds, Part I: The prime decomposition. Let X and Y be connected, oriented 3-manifolds. The *connected sum* of X and Y, denoted $X \# Y$ is formed by removing from each of X and Y an open 3-ball and then identifying the boundary two-spheres, to create a new 3-manifold. Notice that if X is homeomorphic to the 3-sphere, then $X \# Y$ is homeomorphic to Y. A connected sum decomposition of a 3-manifold M is an equivalence between M and a connected sum $X \# Y$. By definition, it is a non-trivial connected sum decomposition if and only if neither X nor Y is homeomorphic to the 3-sphere. A 3-manifold is *prime* if it does not admit a non-trivial connected sum decomposition. It is a theorem of Kneser's from the 1920s that every 3-manifold can be decomposed as a finite connected sum of prime manifolds, and a result due to Milnor shows that this decomposition is unique up to the order of the pieces. The first step in Thurston's Conjecture is to decompose a general compact 3-manifold into its prime pieces. This is achieved by cutting the 3-manifold open along a finite collection of disjoint 2-spheres and capping off the resulting 2-sphere boundaries with 3-balls. Of course, in general this process will produce a disconnected manifold from a connected one.

Cutting apart 3-manifolds, Part II: The decomposition along tori. Thurston's Conjecture states that every prime 3-manifold can further be decomposed along a disjoint family of tori and Klein bottles (each of which has fundamental group injecting into the fundamental group of the 3-manifold) so that each open complementary component admits a complete, locally homogeneous metric of finite volume.

Curvature and covariant derivatives. There is another way to view the Riemann curvature tensor. A Riemannian metric produces a way to differentiate tensors on the manifold, called covariant differentiation. If X is a vector field on the manifold then covariant differentiation in the X direction is denoted ∇_X. Briefly, there are two types of conditions that determine the covariant differentiation associated to a metric. The first are general rules for covariant differentiation in contexts much more general than this one. They are:

(1) The pairing of vector fields $(X, Y) \mapsto \nabla_X Y$ is bilinear over the scalars ($\mathbb{R}$).

(2) The pairing in the first item is linear over the smooth functions in the first variable:

$$\nabla_{fX} Y = f \nabla_X Y.$$

(3) The pairing in the first item satisfies a Leibniz rule in the second variable:

$$\nabla_X (fY) = f \nabla_X Y + X(f) Y,$$

where $X(f)$ is the usual differentiation of the function f by the vector field X.

The rest of the rules relate the covariant differentiation determined by a Riemannian metric to that metric and to the Lie bracket of vector fields. They are:

(4) Covariant differentiation preserves the metric in the sense that for all vector fields X, Y, Z we have

$$X\langle Y, Z\rangle = \langle \nabla_X Y, Z\rangle + \langle X, \nabla_Y Z\rangle,$$

where the brackets denote the inner product coming from the metric.

(5) The covariant derivative is symmetric in the sense that $\nabla_X Y - \nabla_Y X = [X, Y]$, where $[\,\cdot\,,\cdot\,]$ is the usual Lie bracket of vector fields.

We then examine the extent to which the usual commutation rules fail for covariant differentiation in the coordinate directions. That is to say, suppose that we have local coordinates $(x^1, \ldots, x^n)$ on the Riemannian manifold and denote by ∂_i the (local) vector field $\partial/\partial x^i$, in the ith-coordinate direction. Then the failure of the usual commutativity is given by

$$\mathcal{R}_{ij} = \nabla_{\partial_i} \nabla_{\partial_j} - \nabla_{\partial_j} \nabla_{\partial_i}.$$

Then $\mathcal{R}_{ij}$ acts on vector fields so that we can form

$$R_{ijkl} = \langle \mathcal{R}_{ij} \partial_l, \partial_k \rangle.$$

Here, the inner product is the one determined by the metric between the pair of vector fields. Also notice that reversal of indices between the two sides of the expression. The reason for this is to make the sphere have positive rather than negative curvature. Then we have the symmetry properties of R_{ijkl}: skew-symmetric in the first two variables and in the last two variables, and symmetric under interchange of variables 1 and 2 with 3 and 4.

There are many ways to view this tensor, but one of the most fruitful is to make use of all the symmetries described above and thus to consider it as a symmetric bilinear pairing on the second exterior power of the tangent bundle of the manifold. The associated quadratic form associates a real number to every two-dimensional subspace in the tangent plane to the manifold at a point. This number is the *sectional curvature* in the two-plane direction at the point. These sectional curvatures are the analogues of the Gauss curvature for surfaces. Of course, using the metric we

can transform this symmetric bilinear pairing to a symmetric endomorphism of the second exterior power of the tangent bundle, and that is another useful way to view the Riemann curvature tensor. In the case of a surface, the Riemann curvature tensor is equivalent to the Gauss curvature.

Volume non-collapsing. Suppose that we have a Ricci flow $(M, g(t))$ on an n-dimensional manifold, and a point $p \in M$. The *curvature scale* at (p, t) is the largest $r > 0$ such that the norm of the Riemann curvature tensor is bounded by r^{-2} on the ball of radius r in $(M, g(t))$ centered at p, denoted $B(p, t, r)$, for all the metrics $g(t')$ for $t' \in [t-r^2, t]$. Fix a positive constant κ. We say that $(M, g(t))$ is *κ-non-collapsed on the scale of its curvature at* (p, t) if for r equal to the curvature scale at (p, t) we have Vol $B(p, t, r) \geq \kappa r^n$.

References

[1] Browder, William, *Surgery on simply-connected manifolds*. Ergeb. Math. Grenzgeb. 65, Springer-Verlag, New York 1972.

[2] Cao, H. D., Chow, B., Chu, S. C., and Yau, S. T., (eds.), *Collected papers on Ricci flow*, Series in Geometry and Topology 37, International Press, Somerville, MA, 2003.

[3] Donaldson, S. K., Smooth 4-manifolds with definite intersection form. In *Four-manifold theory* (Durham, N.H., 1982), Contemp. Math. 35, Amer. Math.Soc., Providence, RI, 1984, 201–209.

[4] Freedman, Michael Hartley, The topology of four-dimensional manifolds. *J. Differential Geom.* **17** (3) (1982), 357–453.

[5] Gray, Jeremy, A history of prizes in mathematics. In *The Millennium Prize Problems*, Clay Mathematics Series, Amer. Math. Soc., Providence, RI, 2006, 3–30.

[6] Hamilton, Richard S., Three-manifolds with positive Ricci curvature. *J. Differential Geom.* **17** (2) (1982), 255–306.

[7] Hilbert, David, Mathematical problems. *Bull. Amer. Math. Soc.* (*N.S.*) **37** (4) (2000), 407–436; reprinted from *Bull. Amer. Math. Soc.* **8** (1902), 437–479.

[8] Milnor, John, On manifolds homeomorphic to the 7-sphere. *Ann. of Math.* (2) **64** (1956), 399–405.

[9] Milnor, John, Towards the Poincaré conjecture and the classification of 3-manifolds. *Notices Amer. Math. Soc.* **50** (10) (2003), 1226–1233.

[10] Papakryiakopoulos, C. D., On Dehn's lemma and the asphericity of knots. *Proc. Nat. Acad. Sci. U.S.A* **43** (1957), 169–172.

[11] Perelman, Grisha, The entropy formula for the Ricci flow and its geometric applications. Preprint, 2002; arXiv:math.DG/0211159.

[12] Perelman, Grisha, Finite extinction time for the solutions to the Ricci flow on certain three-manifolds. Preprint, 2003; arXiv:math.DG/0307245.

[13] Perelman, Grisha, Ricci flow with surgery on three-manifolds. Preprint, 2003; arXiv:math.DG/0303109.

[14] Poincaré, Henri, Cinquième complément à l'analysis situs. In *Œuvres. Tome VI*, reprint of the 1953 edition, Grands Class. Gauthier-Villars, Éditions Jacques Gabay, Sceaux 1996.

[15] Scott, Peter, The geometries of 3-manifolds. *Bull. London Math. Soc.* **15** (5) (1983), 401–487.

[16] Shioya, Takashi, and Yamaguchi, Takao, Volume collapsed three-manifolds with a lower curvature bound. *Math. Ann.* **333** (1) (2005), 131–155.

[17] Smale, Stephen, Generalized Poincaré's conjecture in dimensions greater than four. *Ann. of Math.* (2) **74** (1961), 391–406.

[18] Stallings, John, A topological proof of Gruscho's theorem on free products. *Math. Z.* **90** (1965), 1–8.

[19] Thurston, William P., Hyperbolic structures on 3-manifolds. I. Deformation of acylindrical manifolds. *Ann. of Math.* (2) **124** (2) (1986), 203–246.

[20] Waldhausen, Friedhelm, On irreducible 3-manifolds which are sufficiently large. *Ann. of Math.* (2) **87** (1968), 56–88.

Mathematics Department, Columbia University, 2990 Broadway, New York, NY 10027, U.S.A.

E-mail: jm@math.columbia.edu

Panel discussion organised by the European Mathematical Society (EMS)

Should mathematicians care about communicating to broad audiences? Theory and practice

Transcription coordinated by

Jean-Pierre Bourguignon, CNRS-IHÉS, Bures-sur-Yvette, France

In most countries, mathematics is not present in the media at par with other basic sciences. This is especially true regarding the communication of outstanding new results, their significance and perspectives of development of the field.

The main purpose of the panel discussion, an EMS initiative, that took place at the ICM on Wednesday, August 23, between 6 and 8 p.m., was to nurture the debate on whether communicating about mathematics, as a thriving part of science, is needed, and how such a communication can be efficiently tuned to different audiences and a variety of circumstances.

For that purpose, the EMS Executive Committee set up a committee consisting of Jean-Pierre Bourguignon (Centre National de la Recherche Scientifique and Institut des Hautes Études Scientifiques, Bures-sur-Yvette, France), Olga Gil-Medrano (Universitat de València, Spain), Ari Laptev (Kungliga Tekniska Högskolan, Stockholm, Sweden), and Marta Sanz-Solé (Universitat de Barcelona, Barcelona, Spain) to prepare the event and select the panelists. Jean-Pierre Bourguignon was asked more specifically to prepare the event with the panelists and to moderate the discussion itself.

These proceedings include a revised version of the presentations made by the panelists under their signature, and a brief outline of the discussion that took place after their presentations.

A contribution that was later elaborated by a participant from the floor has been added separately from the discussion.

Philippe Tondeur (University of Illinois at Urbana-Champaign, United States of America)

The question to the panelists was, as stated in the title, *"Should mathematicians care about communicating to broad audiences?"*

My view is that of course they should, and the core of the argument is as follows:

(1) Mathematics is a fantastic form of human thought, and historically the basis of rational thinking.

(2) Aside from its intrinsic beauty and power, mathematics is indispensable for the progress of science and the betterment of the human condition.

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

(3) Mathematics is embedded in science and enables the science enterprise, even if this role is often invisible to the outsider.

(4) Mathematics and science are the greatest human enterprises ever undertaken to understand the world. Mathematicians are key partners in this process.

For the purpose of this discussion mathematics is used as shorthand for mathematics and statistics. Stochasticity is an essential and pervasive aspect of the phenomenological world.

The role of mathematics in society at large

Mathematics and science cannot fully progress without the understanding of their purposes and participation by the society in which this enterprise is embedded. In communicating with broad audiences, the message has to be calibrated to the specific audience addressed. This is most effective if done through examples.

There is enormous public interest in the biomedical realm, thus illustrating the role of mathematics in medical progress like biomedical imaging has immediate appeal. If the mysteries of the cosmos and string theory are under discussion, the rich geometric ideas underlying these efforts can be described. Cryptography is used in telecommunication and security issues are of paramount public interest. Everyday use of search engines on the web is based on mathematical page rank algorithms. The logistics of supply chains is encountered ever more frequently in everyday life. There are vast amounts of online visual material on such topics from the mathematical sciences, and public presentations can draw on these abundant sources.

This discussion also points to the critical role that mathematics plays in interdisciplinary activities. Mathematics acts as a lingua franca of interdisciplinary science. While interdisciplinary science is driven by the nature of specific science problems, it frequently operates within a contextual and quantitative framework provided by the mathematical sciences. The foreseeable future is going to be one of unprecedented pervasiveness of mathematical thought throughout the sciences. In a data driven world, mathematical concepts and algorithmic processes will be the primary navigational tools. This makes mathematics increasingly important for many of the science and engineering advances to come. The opportunities for the mathematical sciences seem unprecedented.

What it takes to get mathematics thriving

Much of the public discussion of mathematics and science focuses on the proper level of financial support. But the vitality of the mathematics and science enterprise depends on much more than this. It is a societal activity which is part of the cultural mosaic and which flourishes especially well in an open liberal society. By this I mean a society where inquiry is respected as a fundamental principle independent of the outcome, and where all authority is understood to be provisional.

The international character of the mathematical sciences makes it a model for scientific partnerships across the world. This common purpose is pursued in exemplary fashion by other disciplines like astronomy, physics, chemistry, biology, to name a few. The basic sciences are all working to develop our common patrimony.

The educational needs for success in interdisciplinary activities are manifold: aside from mathematics, modeling, and computation, there is a need for education in the fundamentals of the basic sciences, and the development of communication skills. This requires significant improvement in our current educational paradigm for mathematical scientists.

A paradoxical situation

There is a paradox developing between the increased sophistication of mathematical science research and the worldwide decline of the number of students interested in pursuing mathematics at the university level. A particular threat is the insufficient number of mathematically qualified students willing to become teachers of mathematics. Mathematicians have an educational stewardship responsibility, which is primary in post-secondary mathematics education, but we also share an important responsibility in the training of teachers of mathematics. In a broad sense, mathematical scientists share in the responsibility for the state of mathematical education in the world. I am referring to education in the broadest sense, namely the preparation for lifelong learning of a large segment of the population, however that may be achieved. I would like to compare the need for mathematical skills of future generations to the current need for reading skills. It took a long time to achieve widespread reading literacy, and it will take a long time to achieve widespread mathematical literacy. Yet there is no doubt that this will be a fundamental skill in an increasingly digital world. The participation of research mathematicians in these developments is indispensable.

Conclusion

The gift of mathematical talent allowed us individually to enter the world of mathematics, and to enjoy this most fantastic achievement of mankind as our profession. This privilege gives rise to the responsibility of sharing these insights with our fellow human beings and especially with the next generation. My experience has been that effectiveness in these endeavors is the result of well and strongly articulated convictions, using all communication tools available and adapted to specific audiences.

Marcus du Sautoy (University of Oxford and an EPSRC Senior Media Fellow, United Kingdom)

Maths for the masses

One of the books that excited me as a child about the mysterious and romantic world of mathematics was Hardy's *"A Mathematician's Apology"*. As an adult it is a book I love and hate because it comes with a very mixed message. Anyone who wants to emulate Hardy and bring the subject alive for others lives under the spectre of the opening sentence of the book:

> *"It is a melancholy experience for a professional mathematician to find himself writing about mathematics. The function of a mathematician is to do something, to prove new theorems, to add to mathematics, and not to talk about what he or other mathematicians have done."*

And this is the impression that many in the mathematical community have: anyone who talks about mathematics is a failed mathematician. So it was with a lot of trepidation that I made my own first steps to bring mathematics to the masses.

A personal experience

We must all as mathematicians have had the experience of trying to explain at a party what it is we do provided that discovering we are mathematicians doesn't make the guest flee in the other direction. At one dinner in Oxford my neighbour turned out to be the Features Editor of the Times. He said that what I did sounded very sexy and would I write him an article. The next morning I found his card in my jacket pocket but realised I didn't have the nerve to go in front of my mathematical peers saying the things I'd explained the night before.

But there is an old adage in Oxford that the academics might change but the guests remain the same. So three years later I found myself sitting next to the same journalist. *"You never wrote me that article."* Impressed that he'd even remembered after three years and feeling a little more confident in my position I decided to take him up on the offer. After all Hilbert had declared in his famous 1900 address to the ICM that

> *"A mathematical theory is not to be considered complete until you have made it so clear that you can explain it to the first man whom you meet on the street."*

So I decided to take up the Times and Hilbert's challenge.

I chose to write a piece about the Fields Medals which had been awarded that summer in 1994 which had got no press coverage in the UK. The piece was partly about why it hadn't been reported. I decided to tell people what a Fields medal was (this was before Matt Damon had made them famous in the film *Good Will Hunting*) and what Zelmanov had done to win one. It went out in December 1994 under the banner *"Why doesn't maths have mass appeal?"*

A few months after that article I started a ten year research position with the Royal Society which relieved me of any teaching duties. But I couldn't do research all the time. It would send me crazy. So I decided to dedicate some of the time that I might have been teaching to try to bring maths to the masses. I had a lot of support from the Royal Society who was trying to create better dialogue between Science and Society after a government report criticizing the separation between the two groups.

Since those first beginnings I have written numerous articles about mathematics for the broadsheet newspapers, including a piece on why Beckham chose the 23 shirt to play in for Real Madrid[1]. Some of these articles then formed the basis for a book I subsequently wrote called *The Music of the Primes* about the Riemann Hypothesis. I also started doing radio work. I contacted the BBC and asked if they'd like me to cover the Seattle meeting in 1996 to celebrate the centenary of the Prime Number Theorem. They gave me a tape recorder and we did a five minute piece on the BBC's science programme about the Riemann Hypothesis. Having found a user-friendly

[1] They can be found at plus.maths.org/issue26/features/sautoy/.

mathematician, I've now done extensive work for BBC radio culminating in a series for the BBC called *Five Shapes* which I wrote and presented[2].

A challenge: bringing mathematics to TV screens

The real breakthrough in recent years has been cracking television's fear of doing mathematics. Simon Singh's programme on Fermat's Last Theorem was the last serious television outing for mathematics in England and that was over a decade ago. In the summer of 2005 I made an hour long documentary for the BBC about the Riemann Hypothesis based on my book *The Music of the Primes.* It went out as the centre piece of Maths Night on the BBC. Thanks to CGI effects, I realised a lifelong dream to walk through Riemann's zeta function. Other TV work includes:

- a movie about Euclid's proof of the infinity of primes using my football team who, inspired by the galácticos in Real Madrid, all play in prime numbers[3];
- four movies for teachers[4];
- and I'm currently preparing five one hour programmes that will be broadcasted on national television over Christmas.

Taking a broader view

Communicating mathematics to a broader audience is a rewarding but an exposing experience and you need to have a thick skin to be able to deal with criticism. Mathematicians care about details. It is what makes for a good mathematician. But going for the grand sweep of the story is what is needed when talking to the media. Sitting in some seminars I think we still have a lot to learn about communicating between ourselves not just to a wider audience. An understanding of how to empathize with a broader audience could well help our internal communication within the mathematical community. I have had wonderful support from many colleagues for the efforts I've made especially in my department in Oxford. It is important to support and help those journalists and mathematicians making an effort and not to sit back and carp at an inaccurate description of the Poincaré conjecture.

Why should we take the time to communicate to a broader audience? Our subject dies without new people coming into the subject. Some countries have seen student numbers in mathematics declining so much that they are closing mathematics departments. The next generation of mathematicians depends on the current generation telling them why the subject is so exciting. But our audience should not just be the young. It is politicians and business that hold the money and the power. They will not value our subject if we don't show them it is important.

A personal lesson

One has to be proactive if you want news coverage. This year, unlike in 1994, there was extensive reporting in the UK for the Fields medals and the Perelman story. But it

[2]The series can be found at www.bbc.co.uk/radio4/science/fiveshapes.shtml.

[3]To be found at www.spiked-online.com/Sections/Science/ScienceSurvey/films.shtml.

[4]They can be found at www.teachers.tv/series/4289.

didn't come from nowhere. I rang the Guardian and the BBC and other news outlets to warn them about the upcoming news story. The press office in Madrid worked tirelessly to get the fantastic international coverage that the ICM had this year. If we don't sell them the stories, journalists are not going to come looking for them. The IMU in conjunction with national research councils might sensibly look to establish a network of mathematical ambassadors in each of its member countries who could play the same role that I tried to do this year in the British media.

In the UK the need to have scientists who can communicate their subject to society has been recognised. I have a grant from my research council that goes to my department in Oxford to pay for someone else to do my teaching so that I have that time freed up to do media work. Research councils have to be proactive in encouraging people to communicate rather than expecting them to do it in their spare time, time which is already running in the negative.

I believe Hardy was wrong to say that a mathematician can't do and talk about mathematics at the same time. He would never have been melancholy about someone who is a good teacher suggesting that they must be a failure at research. Many of us combine fantastic teaching with research. So why can't communicating with the masses and being a good researcher go together? We are seeing more examples of people breaking Hardy's picture. Timothy Gowers, Fields Medal winner eight years ago, and Barry Mazur are two leading researchers who have made great efforts to broadcast the mathematical message more broadly.

It is a quote from the Opening address of the 1952 ICM that I would prefer to be remembered rather than Hardy's melancholy message. Oswald Veblen opened the congress by saying:

> *"Mathematics is terribly individual. Any mathematical act, whether of creation or apprehension, takes place in the deepest recesses of the individual mind. Mathematical thoughts must nevertheless be communicated to other individuals and assimilated into the body of general knowledge. Otherwise they can hardly be said to exist."*

We are all involved in telling stories of our mathematical discoveries. That is what the ICM is about. But let us be proud of our subject and share our stories beyond the confines of the ivory tower of the ICM. A recent survey in the New Scientist indicated that readers wanted more maths stories. It is the mathematicians who are best placed to tell those stories.

A. B. Sossinsky (Institute for Problems in Mechanics, Russian Academy of Sciences, and Poncelet Laboratory, Centre National de la Recherche Scientifique and Independent University of Moscow, Moscow, Russia)

Promoting mathematics: why, how, who?

Being Russian, I am supposed to possess this inscrutable Slavic soul, prone to seeing the dark sides of our existence. Accordingly, my talk will be more emotional and

pessimistic than those of my Western colleagues. In it, I will try to express my concern about the problems addressed by this Round Table.

For the outset, we are faced with the following sad and paradoxical fact: *"mathematics, the most universal and useful of all the sciences, is the least known to the general public."*

Everyone knows about Albert Einstein, Werner von Braun, and Sigmund Freud, but who has ever heard of Kurt Gödel, John von Neuman, Serge Novikov, or John Milnor? Most of us here are research mathematicians, and very proud of our profession, yet the man in the street does not even know that such a profession exists! For him mathematics, besides having been the most unpleasant subject in school, is just a specific fixed body of knowledge that some people have to learn and then apply in practice, say in engineering or accounting.

In 45 years of my life as a research mathematician, I have witnessed *the spectacular expansion of mathematics into practically all fields of knowledge.*

Besides its traditional spheres of application (physics and technology), mathematics now plays a key role in chemistry, biology, earth sciences, and even in linguistics, psychology, the social sciences, political and military strategy. During the same period, I have sadly observed – haven't we all – *the degradation of mathematical education at all levels,* followed by what I call *the demonization of mathematics and the deification of the computer.*

By the latter, I mean the common opinion that whenever you want to find out something or solve some problem, all you need to do is ask the computer – it will oblige, immediately and without any possibility of error. It is the Computer (with a capital C) that gives you the answer; the fact that a mathematician invented the algorithm used by the machine and a programmer implemented it remains unnoticed by the general public. On the contrary, it is the mathematician who is viewed by most as a soulless individual using abstruse computations to create new technologies without regard to our well being or the ecology of our planet…

In Russian literature, especially in the writings of the great novelists of the end of the nineteenth century, social and ethical questions are at the forefront. Observing each serious mishap of our sorrowful history, Russian writers traditionally ask the following two sacramental questions:

(1) Who is responsible?
(2) What must be done?

Let me try to answer these two questions in the context of our discussion.

Who is responsible?

To my mind, the answer is clear: *we all are*. We missed the great opportunity that we had, in the past two or three decades, to promote mathematics by capitalizing on its spectacular expansion. We have been overtaken and left far behind by the Bill Gates and Sergey Brin of this world. Why did this happen? One of the principal reasons is that *mathematicians are usually poor communicators*.

This is related to the psychological nature of the typical mathematician: introverted and timid in his teens, he starts doing math, the most competitive and most objective of the school subjects, to assert himself; having succeeded, he develops a sense of his intellectual superiority and tends to become arrogant, at least when discussing his favorite subject. This mixture of timidity and arrogance, which I have observed in many of my colleagues (including myself, I am sorry to say), is the worst possible combination for one who wishes to communicate with others.

You have surely heard both of the following allegations from your colleagues

– *the layman can't possibly understand what I do!*
– *the mathematician can do it better!*

You may even agree with them (I do), but what a disaster if they are in your mind at the starting point of a discussion about your profession with the nonspecialist!

Another trait of mathematicians, disastrous for communication, is *the ivory tower mentality,* the desire to do one's mathematics in peace and isolation from the world. A laudable viewpoint, but hardly productive for the propaganda of mathematics.

What must be done?

To put it succinctly, we must make mathematics *visible* and *appealing.* There are many ways of doing this, and most of them are well known. Let me simply list a few without commentary, and briefly describe one or two that may not be familiar to some of you.

Visibility can be achieved via TV, art, photography (e.g. fractals), movies, exhibitions, internet sites, math-fests, popular science magazines, books, animations. As an example of the latter, let me mention the web site www.etudes.ru, which has numerous captivating and dynamic animations presenting recent mathematical results with clarity, humour, and graphical perfection.

Appeal must be differentiated depending on the targeted audience.

For *teenagers*, our future successors in the mathematical profession, there are olympiads and other individual problem-solving competitions, math circles, team competitions (such as the Kapp Abel contest for the Scandinavian countries), summer camps, "math rooms" in some schools (there is even a "math house" in Iran), so-called math battles.

A few words about the latter, which are practically unknown outside of Russia, but have become extremely popular there in the last decade. This is a team contest: two teams of six are given six problems to solve (with a few hours to prepare), then, as the actual "battle" begins, they take turns in challenging each other to solve one of the problems. During each of the six rounds of the battle, a member of one of the teams is at the board explaining his team's solution, a member of the opposite team asking questions (verifying the presented solution, i.e., trying to find and point out possible mistakes), the jury (usually consisting of two or three ordinary high school teachers, not olympiad wizards) watching the proceedings and dividing the points for each problem between the teams. The problems are ordinary high school math,

the good math teacher and any good student (not especially interested in, or good at, olympiad problems) from an ordinary class are capable of solving them, so that math battles are for the masses, not the elite. Their appeal is due to the pleasure that the students derive from the teamwork involved, to the excitement of the battle itself (as a rule, the proceedings are very emotional), to the active participation and support of the teachers (who usually feel left out in olympiad-style competitions). The result is that many students, including those who are not thinking of a career in mathematics or engineering, learn that math can be fun, that it can be useful not only for engineers and accountants.

Let me note that Russian mathematicians are traditionally good at outreaching to high school students, and a good deal of the Russian experience can be used with success in other countries. An excellent web site for information about this is www.mccme.ru (although the English version does not contain all the material from the one in Cyrillic).

Reaching out to wider communities

A different approach to making math appealing must be used when we are outreaching to other categories of people. Besides teenagers, I would distinguish the following three important categories: *other scientists, businessmen, politicians & bureaucrats*.

Obviously, the approach in each case must be different, but I don't want to go into details, because my own experience here is rather limited (and, I should add, not too successful).

Other aspects of the promotion of mathematics are *icons, logos,* and *catchy titles.*

It would be great if math had a photographic icon as striking as the famous Che Guevarra black and white outline photograph or as the marvelous photo of Albert Einstein absent-mindedly looking around his office with unseeing eyes, obviously engrossed in the workings of his inner mind. Or a simple but original graphic logo (as easily recognizable as the ones for Mercedes or Nike). The IMU has understood this, and recently sponsored a contest for such a graphic design symbolizing mathematics. The winning design is a version of the Borromean rings, which, frankly, I have found disappointing. I would have preferred a nice version of the Möbius band, but that has already been appropriated by Renault.

The choice of terms for various branches of mathematics is also important. An excellent example is the catchy title "catastrophe theory", which became very popular, especially in the UK, due to its promotion by Christopher Zeeman in the 1970s. In public lectures, on TV and radio, Zeeman (a great lecturer and communicator) succeeded in convincing the British public that mathematics consists of the theory describing continuously evolving events (created by Newton and his followers) and the recently created mathematics of catastrophe theory, which describes events occurring discontinuously, by leaps and jumps. Some mathematicians (especially those working in singularity theory, as the theory in question was originally called) felt annoyed by what they regarded as non-objective and demagogical exploitation of their serious work. Personally, although I can easily understand their feeling, I believe that the

campaign for publicizing catastrophe theory was useful in displaying a positive image of mathematics. Of course one shouldn't go too far in publicizing exaggerated claims about the achievements of mathematics, but certainly a lot of oversimplification and a little exaggeration are needed for success.

Besides catastrophe theory, there are several other branches of mathematics with catchy titles: tropical mathematics, quantum computing, open-key cryptography, chaos. These terms will easily catch the attention of the general public if they are used systematically in talking about mathematics.

The influence of a catchy title should not be underestimated, sometimes a clever choice of title will lead to successful promotion of the subject, even when intrinsically it is not really worthwhile (which is not the case of the branches of mathematics with the catchy titles listed above – they are all serious, interesting and useful mathematics). A striking example is so-called "fuzzy mathematics": after a promising start in the well-known paper by Bellman and Zadeh, the topic with that title developed into an industry producing numerous publications and PhDs, which were, in my opinion, devoid of any serious mathematical content. I am sure that if it had been entitled, say, "approximative mathematics" no one would have paid much attention to it.

Yet another way to attract ordinary people to mathematics is by showing them *mathematical machines,* i.e., various mechanisms demonstrating curious mathematical effects. An extremely successful example is the prime time TV programme on one of the national channels in Japan, in which mathematical ideas are described and made visible by demonstrating the functioning of various mechanisms. The name of the creator of this program, Akiyama, is a household word in Japan, as popular as, say, Larry King in the US. Another example of physical models of mathematical ideas is Chris Zeeman's well-known "catastrophe machine".

But all of the above will remain wishful thinking, unless we decide who is going to implement it.

Who must do it?

Again, the answer here is obvious: *all of us should,* each of us doing whatever is suited to his or her position and aptitudes.

The rank and file mathematician, first of all, should not be afraid to talk about mathematics in an attractive, perhaps humorous or emotional way, to friends and relations: his or her spouse, tennis or golf partners, neighbors. The inspiration for such short conversations can be provided by Hilbert's quotation (whose exact phrasing was given in Marc du Sautoy's talk) asserting that any worthwhile mathematics can be explained to the man in the street.

The worst possible thing that you can do is to give definitions of the main concepts involved and then state the result(s) of your own work: your interlocutor will be disoriented and bored. Before trying to explain what your work is about, you might begin by making clear that mathematics is a living, exciting, competitive activity – without declaring this directly, but by talking about your rivals and/or collaborators in other countries, about how long your field of study or the problem you are attacking

has been occupying mathematicians, about the excitement you feel when the result you want is achieved or escapes you.

You might then explain that mathematics differs from all the other sciences is that it does not necessarily have a specific object of study from real life: the same differential equation can describe completely different processes in nature, the same surface can portray all the positions of a mechanical system as well as elementary particles in quantum physics, the same formula be applicable to knots and to the phase transfer that occurs when water is transformed into ice. (You shouldn't worry about the fact that the person you are talking to does not know the formal definition of "differential equation", "knot", "surface", "phase transfer" – after all, everybody talks about television sets and mobile phones without having the least ideas about how these devices work.)

What makes mathematics so effective, you might add, is that one never knows in advance what it may be applied to. You might continue by giving examples of mathematical situations when it turned out that a solution of some problem eventually had spectacular applications to real life situations that the researcher certainly did not have in mind when working on the problem.

When I am engaged in such informal conversations with a friend or acquaintance, I like to give concrete examples from my own research experience. Thus, in answering a question like:

– *"What do you guys in mathematics actually do?"*,

I might say something like this:

–*"Of course I do some teaching, but what I am really interested in, what really excites me, is trying to discover new facts in mathematics."*

–*"There are really new facts to discover in mathematics? Like what?"*

This leaves me with many possibilities of continuing the conversation, usually by referring to some of my own work or something related to it. Thus I might say:

– *"Well, I'm supposed to be an expert in the theory of knots and braids. Let me tell you about braids. A braid is a geometric object that looks like several strings hanging down from a horizontal stick and interlacing with each other. The way they are studied is by means of algebra: we replace the overcrossings by special symbols and develop a calculus with these symbols that allows to answer all the complicated geometric questions about braids by means of simple calculations that I can perform by hand or let my stupid computer work out."*

The reaction to that is usually skeptical or negative:

– *"But what's the use of doing that?"*

This gives me the chance to come to the punch line of the story. I explain how my rival and friend, the French mathematician Patrick Dehornoy, together with one of his graduate students, used the calculus of braids to construct a new "one-way function", then explain how one-way functions are used in electronic banking, and conclude that someday my interlocutor's credit card will be protected from electronic theft by…braids.

I have several ready-to-use stories like that up my sleeve (prime knot decomposition, homology of tolerance spaces and numerical solutions, soap films and random walks). Let me add that I have a new one in preparation: I have done some work related to the Poincaré conjecture, and now that it has been solved by Grigory Perelman, I have a good pretext of telling anyone who wants to listen about the dramatic story of Hamilton and Perelman, the later's refusal of the Fields medal and his apparent disinterest in the Clay Institute's million dollars. In the process of telling it, I will not be afraid to say that the main idea of the proof is the seemingly completely crazy idea to apply something resembling the heat equation to solve a purely topological problem.

I will not bore this audience by retelling these stories here, but I would like to appeal to all mathematicians to have such stories (preferably related to their work) at their disposal, enabling them to give well rehearsed impromptu five-ten minute talks for the benefit of non-mathematical acquaintances and friends.

Of course more formal popular presentations (e.g. public lectures) are also very useful, provided they are well done. But then not everybody can be an Ian Stewart or a Petar Kenderov, and very few people can give such deep and visually striking talks as the one of Étienne Ghys at this Congress. (If it were up to me, I would make a video of that talk and distribute it among all the leading universities of the world.)

The math administrator at a university or college, e.g. the chairperson of the math department, besides all that he or she can do as a mathematician, should feel that it is his or her direct duty to attract the best students of the institution to major in math. This can be done by outlining the advantages of our profession (no 9-to-5 drudgery, lots of travel, sabbaticals, long vacations), the career opportunities outside of research (you can tell the students that banks and other financial institutions prefer to hire, at very high starting salaries, PhDs in math or mathematical physics from Harvard, rather than people with an MBA or a PhD in computer science from the same university, or explain that the most successful people in the computer software industry are usually math majors, not students who majored in computer science).

Of course another important function of the math administrator is to attract money to math research. This can be done by outreaching to those who have the money, via the mass media and in other ways, stressing how useful mathematics can be.

The math research institutes (such as IAS, IHÉS, MSRI) must address a different class of people in their promotion of mathematics: graduate students and post docs should be the first to be targeted, and of course the people and organizations that have money and might agree to part with it. The research institutes can also sponsor other activities. As a positive example, let me mention that the director of MSRI, David Eisenbud, is organizing a conference in Moscow this fall in order to familiarize American mathematicians with the Russian experience in running math circles. I also firmly believe that, in order to make the promotion of mathematics efficient, not withstanding that *"the mathematician will do it better"*, the research institutes should hire experts in public relations to coordinate and organize promotional activities.

The EMS, the AMS, and the IMU, I firmly believe, *should do much more to coordinate the promotion of mathematics at all levels in Europe, America, and worldwide*. First of all, they should motivate and assist their members to advertise their profession and their science. This can be done, in particular, by distributing electronic or hard copy booklets or brochures explaining to individual mathematicians what they can do and how to go about it, and also by supporting and organizing various promotional activities of the kind I described previously. I am convinced, and this is a crucial point, that *math must be promoted in a professional way,* a qualified public relations professional hired by the corresponding Society should be responsible for these activities.

Conclusion

Starting from a pessimistic assessment of the situation, I have progressively drifted to advertising mathematics. When you advertise, you must always end on an optimistic note. So let me say, in conclusion, that if we all pitch in, mathematics will reacquire the prestige and renown that it deserves in our society. And since we are in Spain, let me end with the following slogan:

Adelante, matemáticos!

François Tisseyre[5] (Atelier ÉcoutezVoir, Paris, France)

Producing media with mathematicians

I will be speaking in the name of Atelier ÉcoutezVoir, a non-for-profit organization initiated 30 years ago in Paris. This studio is mainly dedicated to communication of art and science through audiovisual production.

Concerning mathematics, we have been working in the fields of Engineering Science, Applied and Fundamental Mathematics. During the past 25 years, we have had the pleasure to work with a few mathematicians who wished to communicate with various audiences, ranging from children to professional mathematicians. Thus we have produced a number of videos, visual presentations, exhibitions, and taken part in various events like festivals, congresses or meetings. I would like to concentrate on video production, which is what we do most.

In practice, we start working when the mathematician has already answered the global question we are discussing today. For social, or moral, or generational reasons, his or her answer is *"Yes, of course"*. Then quite a few questions arise. Here are some of the ones we have had to cope with.

[5] I want to dedicate this text to Adrien Douady who recently and tragically passed away. In the last twenty years, his fame as mathematician extended to one of a patient and innovative communicator. His contributions to the popularisation of mathematics have taken several forms: as author and scientific director of audiovisual projects (e.g. *La dynamique du Lapin*), of the exhibit *"A fractal world"* that he accompanied in several countries, of many colorful conferences, he reached out to broader and broader types of public, further and further away from his fellow mathematicians. In the decorum of established institutions as well as in a café in rue Mouffetard, in Paris, Adrien always showed an exceptional openess to tirelessly explain the most abstract notions to anybody who was willing to listen to him, most of the time from a surprising angle leading to new fruitful insights. A DVD with his many contributions is under preparation.

Motivation

The mathematical community does not seem to have a unitary attitude in front of transmission and share of knowledge. Many mathematicians just dream to transmit the great pleasure they feel as they do maths. Of course, one has to practice maths before he/she knows it can be a pleasure. Some think that the general population suffers from "innumeracy" and has to be cured. Others feel that it is their duty to transmit what they get payed for, generally through public funding. Quite a number do not want to be disturbed with such questions, because they want to keep concentrated on their work and talk with colleagues only. And many others…

Maths and the media (*France*)

Let us first notice that practically no maths appear on French TV, or so little, and it would certainly be helpful to try and understand why. However, various approaches are available, like: documentaries on the community, presentation and illustration of nice classical problems, introducing new concepts or disciplines, history of ideas, recording exceptional lectures, games, and so on. Fortunately today, television is not the unique horizon for audiovisual diffusion. Producing DVD's or webcasting have become usual practice with results of increasingly good quality. So that there are effective supports for audiovisual publishing. Authors and producers are welcome, including young ones.

A vital need for dialogue

How can there be a fruitful dialogue between audiovisual professionals and mathematicians who intend to publish something together?

When we film makers speak of video or film, we have narration in mind. Images and sounds come continuously and form sequences, by construction. When we make films, we are always telling a kind of story, whatever abstract it may be. But mathematicians do not read maths like a novel, in a continuous way: they will read a paragraph, then stay half an hour studying another one, reading and reading again, then study a formula, or make computations, and so on. If we decide to work together and produce a video, we will have to define what can be presented continuously, because the audiovisual language allows that only.

Another point is that we do not speak the same language. And what's more, we do not have the same appreciation of what we have to learn in order to cooperate with meaningful results.

As non-mathematicians, we producers obviously have to learn maths for every single production we undertake with mathematicians. There's no doubt about that for each of us. And it's very exciting. On the other hand, mathematicians do not call themselves non-producers or non-directors. Just because, like many people, they have the feeling that it is very easy to understand how films are made: writing a script, shooting with cameras, editing, and that's all. I want to plea for a simple idea: if we want to achieve fertile results, we have to constantly make steps towards one another. A good film is found somewhere between our respective fields. So it is vital that we all make efforts to understand each other's approach.

Sense and meaning

But the main problem may not be good will, but rather a matter of sense and meaning. The mathematician wishes to convey something that is meaningful for him or her and colleagues: an article, formulas, a conjecture, that are consistent. Our job is to help this make sense for the audience. This could seem to be a theoretical discussion. In our case, it is what takes place in practice every time we make films with specialists of any domain, especially maths.

Let me give an example: ten years ago, Jean-Pierre Bourguignon proposed us to make a film about a memoir that Lagrange wrote in 1808. This appeared to be a revolutionary one in a certain way, as it opened completely new paths to study the movement of planets and many other abstract problems. During three months, Jean-Pierre tried and explain that to us. But it sounded absolutely abstract and meaningless, like an unfamiliar music. We used to speak of this with late Romain Weingarten, a French poet and writer; he was very excited too, and begged for more explanations. One day, I asked Jean-Pierre to tell us more about the three-body problem, then about Newton, and Kepler. Then we started meeting astronomers and specialists of history of science, but also space engineers, and this is how we finally found the red thread of our film: a poet is dreaming at night at his window, and he sees an artificial satellite in the sky. He asks his friend, a mathematician, to help him understand how the man succeeded in putting man-made objects among celestial ones. When we have had that scenario, it became very exciting to work with an increasing group of contributors to whom we asked to just play their own role: Jean-Pierre Bourguignon as a helpful mathematician, Jean Brette, as a marvellous maths popularizer, Bruno Morando as an astronomer, Huguette Connessa as an engineer and among them Romain Weingarten, a poet who kept dreaming aloud. The film is called *The New Shepherd's Lamp*[6], and we all remind this period with great emotion. There had been a deep transformation, not of the initial subject, but of its approach, and this meant something both to mathematicians and non-mathematicians.

Investing in video math production

How far, and how much are both sides ready to invest of time and energy? Who else is needed? For a mathematician, taking part in a video production actually requires as much time as publishing an article, or even a book. But it takes more, as much patience and pedagogy are still needed to make us at least get a flavour of the topic we are going to deal with. He or she will have to answer 10, 20 times basic or naive questions, till the music becomes familiar. Then we have to get enough practice to let our imagination go. For us, this may be quite a long and hard way to get into the subject.

Here is an example again: in 1992, Adrien Douady wished to produce a series of videos to help students understand basic Holomorphic Dynamics. The first module was entitled *The Dynamics of the Rabbit*[7]; it is the study of a Julia Set. It took us nearly

[6]The French version of the video is available from the CNRS Images/Vidéothèque and the English one in the Videomath series edited and distributed by Springer Verlag.

five years to produce it, and here is why and how. First, as a non mathematician, I had to learn about complex numbers, iteration, etc., and get familiarized with strange pictures (fractals). It took me about a year and a half to know enough to be able to build and discuss a pertinent script. During that period, there has been quite a lot of consulting with other mathematicians, students and teachers. Then we decided to start producing pictures, in order to show the various structures and phenomena that appear in the study. We needed to produce many, and especially animated sequences. So we had to find someone capable of producing thousands and thousands of very accurate pictures (there are 25 pics per second). Dan Sørensen was the man with this singular profile: a mathematician, and an engineer capable of developing adapted software. Dan had to take into account both the needs of the scientist and those of the film director. Then we had to find the way to transfer the computer images to video, which was not common at that time. So we had to develop specific and efficient techniques for that. We calculated more than 150,000 pictures and finally kept something like 25,000 for about 20 minutes of mute video. Adrien Douady then commented these sequences: we proposed the form of spontaneous commentary, obtained thanks to interview and accurate sound editing. After mixing, the final result is a 25 minutes video, with English and Spanish adaptations obtained thanks to mathematicians Shaun Bullett and Nuria Fagella. Finally, to give a perspective, for this project, starting with two persons, we finished with a dozen, acting successively or simultaneously.

About the audience

As we started the Rabbit project, we had in mind a specific audience consisting of advanced students and mathematicians from other fields. But during all the production process, and especially during conception, many objectives had to be re-defined, in particular due to some repeated difficulties we met. So that there has been quite a lot of interactions between us along time. This may be seen as a difficulty. In fact it is an opportunity to make films that make sense for each of us. As we produced sequences, we used to present them to different people, and get interesting and sometimes surprising feedback. We learnt how much such images speak by themselves and give more than a flavour of the subject. This is how the audience became to get broader. Finally, the Rabbit video is presented to rather large audiences, depending on whether it is projected alone, or supported by previous presentation then exploited through discussion.

Actually, the various videos we have produced are intended to these rather large audiences with little focus, as we do not work under the frame of official educational programmes. Roughly, what we now call "broad audience" includes adult people who are fond of science culture, students of various fields, even pupils of secondary school scientific sections. These persons like to understand processes and methodologies more than technical results. They read magazines, watch some rare TV programmes, and love to visit science museums.

[7]This video has been edited by Atelier ÉcoutezVoir, Paris, France (1996) and also reproduced in *Video and Multimedia at 3ecm* (S. Zarzuela, S. Xambó, Editors), Springer VideoMATH Series, Springer Verlag (2000).

Conclusion?

Among the various dimensions we explored in maths popularisation, video is the most difficult and exciting we have experienced. A common idea is that video can be a useful medium to convey mathematical concepts. This is true, as animated images and fine sound/image accordance can be efficient. But we have to keep in mind what the audience's social habits really are. People zap.

And we have to be humble regarding effective results. We are not going to have millions of people love maths thanks to videos, but video can bring a very nice taste of maths, and this might be quite a helpful way of contributing to its popularisation.

Björn Engquist (Royal Institute of Technology, Stockholm, Sweden, and University of Texas at Austin, United States of America)

Audiences to be addressed

Several audiences need to be addressed by mathematicians: the general public, the media, different administrations (government, universities, schools), potential students who are, no matter how one takes it, the mathematicians of the future. The main difficulty is deliver different but coherent messages to these manifold audiences.

The content of the messages to be passed on

The messages have to be articulated around two complementary themes: *the general culture of mathematics* and *its applications*, while keeping always in mind which message you are talking about and to whom you are delivering it.

Along the culture line, one has to give due value to the long history of mathematics and the outstanding personalities that marked it. It also has to encompass the role of mathematics in education, through its role in abstract thinking but should not avoid talking about its recreational side.

Via its applications, mathematics is often viewed as the third pillar of science with a major impact in everyday life, technology, and education. Mathematics is the language of quantative science even for experiments. Its impact in so many different sectors of society has grown so large that illustrative examples are plentiful: from weather prediction to signal processing, medical images, and industrial product development. One should not forget that Google is fundamentally a mathematical product.

Mathematicians should learn from biologists, physicists,…

A key issue is a proper understanding of the interplay between pure and applied research. The discourse that most scientists put forward is that in order to solve problems that society wants to be solved basic research is indispensable. Too often mathematicians tend to be more abrupt, and state their intention of doing basic research that may, some day, be relevant to solve some problems.

The science approach is actually more effective and still does not limit freedom of basic research. From that point of view, mathematicians should not be afraid of using applications as motivation for curiosity driven basic research. Not being shy does not mean that one is allowed to overstate because mathematics is almost always

not solving the real problem alone but mathematicians are important, if not essential, partners in the solution.

The universality of mathematics

The strength of mathematics is its universality. In one of its facets or another, it is needed in almost all aspects of modern life. One should always have examples ready and updated.

It should also not be overlooked that core mathematics also needs to be developed as foundation for all of mathematics. The case should also be made that mathematics is as fast in the relation between basic research and applications as other sciences.

It will not be surprising if, for example, any practical results from the Large Hadron Collider will take longer time than it took from theorems in harmonic analysis, via wavelets, to image compression for the Internet.

Jean-Pierre Bourguignon (Centre National de la Recherche Scientifique/Institut des Hautes Études Scientifiques, Bures-sur-Yvette, France)

A brief summary of the discussion

The discussion triggered by the five presentations was quite lively. Some colleagues wanted to share their experiences, some others to warn against possible abuses, and the possible loss of meaning about the true nature of mathematics.

The need to be very much aware of the audience when making a presentation over mathematics was stressed by several people. A lack of awareness in this direction can often lead to opposite effects than the ones hoped for. This fact is again discussed in the point of view that one of the colleagues who took part in the discussion from the floor wrote up (see an excerpt from the document received by the Panel after the Congress at the end of these proceedings).

The issue that gave rise to the most controversial exchanges is the risk of *"over-selling"* mathematics, and what goes with it, namely the loss of control by scientists of the products of science. What is at stakes is of course the moral value that some colleagues place above all in the practice of mathematics, and more generally of science. For some of them, this generates an extreme uneasiness when making the case for mathematics at all price, as regards the tendency of hiding inappropriate uses of mathematics made by the society at large.

According to them, the risk of losing critical sense vis-à-vis recent developments of the discipline is so high that it prevents them from participating in actions addressing large audiences about mathematics. From this point of view, the fact that the title of the Panel discussion ended with a question mark was certainly welcome. It must be acknowledged that a marked sensitivity to moral issues up to the point of creating an explicit reluctance in addressing the general public about mathematics was not represented among panel members.

Such an attitude is of course related to the fact that mathematicians necessarily wear several hats when acting in society: teachers, researchers, and in a broader sense intellectual and moral references, and finally, for some of them, politically active citizens. It was stressed how difficult it is to draw a line between these different

responsibilities, and how serious the consequences of this situation can be on the credibility of the overall mathematical enterprise. The final issue being: who controls what? Very rarely, are mathematicians running the complete show. In issues like arms production (and the *"modern"* battlefield does involve dealing with a lot of data, many of which of a mathematical nature or subject to a mathematical treatment) recent developments of mathematics or demands made to mathematicians can hardly be considered neutral. The key question is then: how can one keep enough distance to be sure of what is at stakes and not let the technical discussion hide some more fundamental issues?

Actually, it was argued that the move towards an information society increases the mathematicians' responsibilities. It should force them to make sure that the values they believe in are not betrayed in the way the practice of their discipline evolves. They should also make sure that such issues are not well kept secrets when talking about mathematics to various kinds of audiences.

This way of approaching the question under debate made the exchange very valuable and gave a very welcome depth to it. It also gives a reason to revisit it and to consider it with the appropriate focus: indeed, if approached at a too general or too technical level, the debate can miss some essential points.

An excerpt from the document submitted by Jacqui Ramagge (School of Mathematical and Physical Sciences, The University of Newcastle, Australia)

I have been involved in popularizing mathematics[8] at a small and local level for about 10 years. This has included interactions with the press and regular appearances on local radio as well as workshops for children of all ages, teachers (both primary and secondary) and parents.

Communicating and promoting mathematics

To claim that we have nothing to do is to ignore the changes that have taken place in society over the last 30 years and is selfish in the extreme. Students have a greater choice of studies than they had in the past and some areas of study are being marketed forcefully and effectively. Doing nothing is no longer an option unless we are willing to see the demise of mathematics as a discipline and the concomitant effects on other disciplines which are highly dependent on mathematical innovation.

I argue that we need to raise the profile of mathematics significantly. We need to do this for two reasons, one is altruistic and the other pragmatic. The altruistic reason is that we are already at the stage where demand for qualified mathematicians and statisticians outstrips supply. The pragmatic reason is that many universities are now working as competitive environments and mathematics will lose out in terms of funding and influence to disciplines whose profile is higher.

Identifying those who should be involved in the raising of the mathematical profile partly depends on the context. For example, not all of us enjoy talking to the media and

[8]When referring to mathematics and mathematicians, all statements are equally applicable to statistics and statisticians.

some of us might do more harm than good in that context. However, as a community, we should recognise the need for such activities and support and encourage those who do them.

Some people have a talent for stripping ideas down to their very core so that the heart of the concept is exposed and can explain it in a way that makes sense to almost anyone. Those of us less talented in this area we can still improve our performance with sufficient practice.

While it is essential to curtail technicalities when addressing a broad audience we must not mislead the audience. This leads us neatly to the next topic.

Selling and overselling mathematics

Some people argue that outreach activities necessarily involve misleading the public by exaggerating the impact of mathematics. Luckily, there are enough amazing examples of the impact and applications of mathematics that we don't need to make any up.

One mistake in this context is to confuse *selling* with *providing information*. Students are increasingly concerned about their future and ask questions such as *"I don't want to be a teacher so why should I study mathematics?"* We need not be evangelical, but we must give students an accurate impression of what mathematicians do.

It is the responsibility of all enterprises that use mathematics and employ mathematicians to inform the population about the usefulness of mathematics. This group of enterprises is diverse and to achieve maximum impact they require coordination. Mathematicians are the obvious choice to facilitate this endeavour, and we should be proactive in this regard. This could include asking relevant organisations for support to run mathematical outreach activities.

Mathematical games and competition(*s*)

One well-established mechanism for piquing the interest of young people is to run mathematics competitions of various sizes and levels of formality. However, competitions tend to be favoured by the competitive. This may be one factor in the disproportionately low number of women amongst mathematics olympians for example. We could use hybrid approaches such as competitions for groups of students.

One problem is that the overwhelming number of current mathematicians have been attracted to mathematics by the inherent beauty of the subject and/or competitive selection processes. This makes us a surprisingly homogeneous group given that we are spread all over the globe. It is notoriously hard to see the world through the eyes of those whose motivations are completely different from our own, but that is exactly what we have to do if we want to increase diversity in mathematics.

In conclusion, if we are not seen to be passionate about mathematics, then we can hardly expect others to be passionate on our behalf.

ICM 2006 Closing round table

Are pure and applied mathematics drifting apart?

Transcription by

John Ball, IMU President, Mathematical Institute, University of Oxford, United Kingdom

Marta Sanz-Solé, Facultat de Matemàtiques, Universitat de Barcelona, Spain

Mathematics is broadening its scope, developing in many new directions and interacting with a wide range or other disciplines, from information technology, social sciences and politics to engineering, biology and neurology, just to mention a few of them. Such an extraordinary expansion is also fostering a fruitful cross-fertilization between different fields of mathematics. With the ubiquity of computers, many fields of pure mathematics are incorporating experimental methodologies which in the past were only used in applied mathematics. In this new landscape, how do pure and applied mathematics interact with each other?

This was the topic of the panel discussion organized as a closing activity of the ICM 2006 on Tuesday, August 29, between 6 and 8 p.m. It was moderated by John Ball and organized by Marta Sanz-Solé.

This article consists of a genuine transcription of the presentations by the panellists and excerpts of some of the contributions by participants in the discussion.

Introduction of the panellists by John Ball, moderator of the round table

Our panel consists of five very distinguished mathematicians:

Lennart Carleson, Professor Emeritus at the University of Uppsala and a former President of IMU. His research interests are in Harmonic Analysis and Dynamical Systems.

All of our panellists are recipients of many awards, and I have decided that it would take far too much time to list them all, but I make an exception in reminding you that Lennart Carleson was awarded this year's Abel Prize, for which we offer many congratulations. I would like to say how much IMU values its collaboration on several fronts with the Norwegian Academy of Sciences and Letters and the Abel Fund.

Ronald Coifman, who is Professor of Mathematics and Computer Science at Yale University. His research interests are in Analysis, in particular Harmonic Analysis and Wavelets, and applications to Information Processing.

Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006

Yuri Manin, who is Professor of Mathematics at Northwestern University, a former director of the Max Planck Institute of Mathematics in Bonn, and a former chair of the Fields Medal and ICM Program Committees. His research interests lie in Algebra and Geometry, in Number Theory, Differential Equations and Mathematical Physics.

Helmut Neunzert, Professor Emeritus at the University of Kaiserslautern. He is a founding member and former President of the European Consortium for Mathematics in Industry, and his research interests are in Kinetic Theory and Fluid Dynamics.

And finally

Peter Sarnak, Professor of Mathematics at Princeton University, and whose research interests are in Number Theory and Analysis.

Just in case I betray at some point my own views on the subject of the round table, I work in Nonlinear Analysis, especially the Calculus of Variations and its applications to Materials Science.

By way of introduction, perhaps I can show the two earliest instances I know of in which the terms "Pure" and "Applied" Mathematics feature in the literature. Here is the first one, the first issue of the *Journal für die reine und angewandte Mathematik*, Crelle's Journal, which appeared in 1826; in the contents of the first issue you can see several papers by Abel. Ten years later, the first volume of the *Journal de Mathématiques Pures et Appliquées*, Liouville's Journal, appeared, and here you see the papers are much more applied. The authors include Coriolis, Liouville, Ampère, Lamé, Jacobi and Sturm, so these were not bad for first issues of these journals! The old volumes of these journals, incidentally, are retro-digitized and freely accessible, which is where I obtained these images.

So pure and applied mathematics have been explicitly mentioned for nearly two hundred years, and were doubtless recognized as being in some way different before that, and our topic is whether they are drifting apart.

Each of our panellists will give their presentations, and then the subject will be open to the floor, and I hope we will have a lively discussion.

Contributions by the panellists

Lennart Carleson

Mathematics really has three different faces. The first concerns general education, and mathematics is of course just as important as learning to read. This is a very important part of society. The second relation to the outside world is mathematics as the language of science, and this is the way in which I am going to use the term "applied mathematics". The third aspect is of course a subject in its own right – a logical system. This is what most of us who are here right now represent. We must clearly understand that of the three, we are the weak part, and that it is absolutely vital for the continuation of our science that we love so much, to stay with good relations to the other two aspects.

So the answer to the question if pure mathematics and applied mathematics are drifting apart, I would say that we should make every effort that it doesn't happen. I would like to object somehow to the word "drift", because we are not really jellyfish and we can do something about this ourselves. So, I should like to concentrate on the aspect of the issue as far as it concerns the teaching of mathematics.

We like to talk about mathematics and applied mathematics in this order, which seems to indicate that applied mathematics is some kind of corollary of mathematics, and that we are looking for ways of applying this. This of course is completely wrong from the point of view of history. Through the years, mathematics has slowly been built from nature, and we have observed the remarkable fact that the laws of nature can be co-ordinated into groups and they follow rules. This started with geometry, of course, and numbers, and then we all know how difficult it has been to make movements into something logically reasonable. It has been around only for like two hundred years in a logical setting. If we take a subject like Probability – well, it may show that I am old, but anyway, it has been built as a mathematical subject in my lifetime really, and looking into the future, we can see new areas emerging where the mathematics is missing, and the most spectacular there is probably Computer Science.

Nevertheless, teaching of mathematics has always been done in a deductive way, that one goes from the general to the special, either as a logical system or as being applied. This of course is contrary to the traditional way of how things should be taught. Let me mention to you that this also has happened in my lifetime. When I started studying at the University of Uppsala in 1945, the first lecture was devoted to the Dedekind cut; we defined continuous functions with epsilons and deltas, we had axioms and we had definitions, and we had Riemann integrability and I don't know what!

As the number of students has increased, and their interest in the logical structure of the field has decreased, one has successively been cutting off these typically mathematical aspects of the mathematics teaching. To put it in a striking way, I would like to say that it is only applied mathematics that remains.

We have all of us, I guess, experienced how there has been pressure from other fields, from Physics, technical subjects, or even Biology, that they want to teach their own mathematics that we don't teach in the relevant way. I would like to say that I can somehow see their point, because we have not made any real effort to implement any kind of inductive way of teaching, that is, going from examples and cases and applications to the concept. You would think that the use of computers would have changed this in a drastic way, but that doesn't seem to be the case at all. We are still fumbling for ways of using computers in the teaching.

My thesis here today would be to say that we should make a really concentrated effort to make our teaching into inductive teaching. One can think of different ways of accommodating students with different interests. I have made a short list of what one could possibly do to change this. One of the essential points is clearly the attitude of ourselves, so to say, and also of our colleagues. Everybody knows that most – or many – mathematicians are really uninterested in things which are not leading to

theorems or new statements, and there is a scepticism among our colleagues in other areas, that anything useful can come out of contact with mathematicians. And it is my real wish that we would all try to remedy this situation.

So what could be done? I have made three points here. The first is that one should have closer contact between basic mathematics teaching and the applied areas; at least in Sweden most departments which are applied have separate buildings and we don't really see them. Computing stays in one area and the applied people stay in another area. It would be my wish that people with applied interests would be involved already in the construction and the teaching of the basic courses. One would need to change the curricula in some suitable way, and try to speed up the use of computers in the teaching. We should really accept the fact that most students are not really interested in mathematics. Well, many are interested in their lives, but some of them are also interested in other areas, and one should accept that. We should not try to put our values on people who do not really want them.

One could compare these people with how you learn how to drive. Most people have no idea how a car works or why it works, but you can still use it. It is similar with people who learn mathematics; they only want to be able to read books and understand the formulas that they are taught in the other courses. I think one should not criticize this; one should accept that this is a really natural attitude. After all, mathematics as we know it is a rather sophisticated and not really applicable field. Also there should be for example, something like partial differential equations, everybody should have heard about that – they are going to meet it somewhere else.

Finally, there is a movement in the world around us to apply different sections of mathematics. There is pure mathematics and there is industrial mathematics, and there is applied mathematics and there is the teaching of mathematics, which have different organizations, and different meetings, and lead their own lives. I think that makes sense. But nevertheless there should be places where they meet, where the people from these different areas come together and can exchange experiences.

Ronald Coifman

I will try to address some of the issues of "drifting apart". Mathematics is a big ecological system of different species of mathematicians, and each species likes to think of itself as better than the others. The issue, though, is that the world of mathematics has expanded dramatically. Our universe is so much bigger, that everybody is drifting apart from everybody else, but in reality we enrich our lives substantially. What we have seen, I would say, over the last two decades is the insertion of the computer into our lives – of the digital age. Now that insertion is occurring at a variety of levels, I mean on the sort of everyday ability to collect numbers, and collect data, to the ability of the mathematician to actually run experiments in mathematics, and I would say that if Gauss were here he would probably run experiments like crazy. Leibniz too, and all of those. And if you asked them the question "Are they pure or applied?" they would just laugh at you.

In a way, the drift that we seem to see is mostly social, but not necessarily intellectual. We have seen in this congress many, many people, and many of their talks are related to outside scientific fields, or inspired by outside scientific fields, and so on. The way I see it now is that in fact the need for mathematicians, pure mathematicians, not necessarily in the areas of applications, is actually much greater than it ever was. This is sort of a pre-Newtonian time, anyway, and we don't have the mathematics to do the simplest of all things. We don't have a descriptive language to describe various things, and we don't even have the ability to define the geometries that need to be defined in the real world.

I think there is a serious opportunity here for mathematicians. That opportunity, to realize it, we need to follow what Lennart just said: revamp our teaching style. I am not advocating changing what we teach, just the way that we do it, in a way that makes it more transparent for people who don't necessarily want to invest the same effort as somebody who was born with mathematics in his blood. The opportunity is really the same that occurred in the physical scientific revolution in the time of Newton and Leibniz, which is that there is a need to quantify and describe specifically and precisely all kinds of phenomena that surround us. And the number of phenomena and their complexity is really growing exponentially, just because we can't, and so digital data is generated in overwhelming quantities all over the place, whether this is web data, document data, sensor data… and we're stuck!

Let me give you an example. The data may be that you have the results of some medical tests, blood tests, or some number that you get, and you want to evaluate the function, which is how healthy you are, what health score you can have. We are dealing with a very simple object, which depends on ten or twenty parameters, and we don't have the tools to approximate them. We have heard around the board today, telling us something about some potential tools, but this is a most elementary object of mathematics, which is a function, except that unfortunately the function depends on many more parameters than we used to do before computers – the number of parameters may be ten, twenty – in reality we may have ten thousand or ten million of them. And the tools are not there. So what is needed in this context is for somebody to think very deeply and come up with potential solutions – so mathematicians, pure mathematicians, and their modes of thought are necessary. Computer scientists are not trained for the job. I know of a multitude of examples of that, having to do with acoustic calculations, electromagnetic calculations. Unless you completely revamp the mathematics and reorganize everything you need to do, rebuild the language for describing the objects, you can't go anywhere. It doesn't do us any good to just throw a big matrix at some problem and say this is a linear problem, we can invert the matrix and do this or that – it doesn't do anything.

The obstacles confronting us are actually much more monumental than they ever were, and they require the ability to build the language, to organize very complex objects, to organize them in a variety of geometries. I just described a minute ago the acoustics in this hall. That's a problem that, say, twenty years ago nobody could calculate, and even now I doubt if there are more than maybe ten people in the world

who can actually calculate anything, because the object – you hear the echo and everything – and the acoustics here are so complex that, unless you build a language – you cannot use formulas, because formulas will not deal with that – unless you build a new language to describe it, you are dead. So that's one opportunity.

Similarly, by the way, if you go to the social sciences, or to, say, just documents, or machine learning, or other fields of that sort, the language and the geometry to describe the objects that you want to manipulate and their internal relations between them, all of that is yet to be invented. We need people of the kind we had at the beginning, a few of them we had last century, like Shannon, von Neumann, Benoît Mandelbrot, who is here, who recognized certain geometries that people consistently ignored, all of those are opportunities for mathematics, and that mathematics is pure, although the opportunities and the challenges are coming from the outside world, but in the past it has always been that the outside world was probably the most inspirational in actually pushing us towards discovering structures.

It's very nice to be motivated by internal ideas, but I don't think one should be that arrogant in thinking that we know everything that needs to be done – we should let the world tell us. As I said, invention is really what's needed. And that's the crafting of tools, and the people who craft the mathematical tools are people who are interested by the tool and the applications – the test, if you wish, that the tool is effective. But the people who build tools are mathematicians. They may be working, like Shannon, as an engineer, but he built mathematics, and it is pure mathematics, no matter what we say. In fact, it's being used consistently everywhere in pure mathematics. Is Probability an applied field? Of course not; it is motivated by application.

We see in various communities, like the machine learning community, the bio-informatic community, the computer science community, we see emerging a variety of methods which are mysterious, somewhat ad hoc, but extraordinarily successful. The question really is: what are the underlying structures that enable us to assert that certain methods will work or will not work, and what they are capable of achieving? And what are the real deep structures underlying it – this is the job of the pure mathematician.

Yuri Manin

I am certainly a pure mathematician, and what I would like to discuss here is the implicit presupposition that lies at the base of our distinction between pure and applied mathematics; namely that mathematics can tell us something about the external world, that mathematics can be a cognitive tool, although it doesn't look like a cognitive tool. It doesn't study anything specific in the surrounding world.

So in order to understand how mathematics is applied to the understanding of the real world, it will be convenient for me to subdivide it into the following three modes of functioning: model, theory and metaphor. A mathematical model describes a certain range of phenomena, qualitatively or quantitatively, but feels uneasy pretending to be something more. Probably one of the most successful early models is Ptolemy's

model of epicycles describing planetary motions, about 150 years of our era, and one of the latest models which does call itself a model is the standard model describing the interaction of elementary particles, around 1960. Generally quantitative models cling to the observable reality by adjusting numerical values of sometimes dozens of free parameters – at least 20 in the standard model. And such models can be remarkably precise, and there are of course qualitative models offering insights into stability, instability, attractors, critical phenomena.

As an example, I quote a recent report which is dedicated to predicting a surge of homicides in Los Angeles. As a methodology it uses pattern recognition of infrequent events. Result: "We have found that the upward turn of the homicide rate is preceded within eleven months by a specific pattern of the crime statistics; both burglaries and assaults simultaneously escalate, while robberies and homicides decline. Both changes – the escalation and the decline – are not monotonic, but rather occur sporadically, each lasting some 2 to 6 months."

Now the age of computers has seen the proliferation of models which are now produced on an industrial scale, so numerically, and very often used as black boxes with hidden computerized input procedures and oracular outputs prescribing behaviour of human users; for example, in financial transactions.

What distinguishes a mathematically formulated theory from a model is primarily its higher aspirations. A theory, so to speak, is an aristocratic model, or if you wish a model is a democratic theory. A modern physical theory – and also all physical theories – generally postulate that it would describe the world with absolute precision, if and only if the world consisted of some restricted variety of stuff, massive point particles obeying only the law of gravity – things like that. The recurring driving force in generating theories is a concept of reality beyond and above the material world; reality which may be grasped only by mathematical tools, from Plato's solids to Galileo's language of nature, to quantum superstrings.

A mathematical metaphor, when it aspires to be a cognitive tool, postulates that some complex range of phenomena might be compared to a mathematical construction. Probably the most known mathematical metaphor now is the artificial intelligence. We know very complex systems which are processing information because we have constructed them, and we are trying to compare them with the human brain, which we do not understand very well – we do not understand almost at all. So at the moment it is a very interesting mathematical metaphor, and what it allows us to do mostly is to sort of cut out our wrong assumptions. If we start comparing them with some very well-known reality, it turns out that they would not work.

My feeling is that mathematical metaphors… more often than not some models and theories also are used as mathematical metaphors, and as such they then contribute to changing our value systems, or at least influence our value systems. I am a little bit concerned about the proliferation of both mathematical models which are hidden inside computer hardware and software, and also I am concerned about the moral issues that are not often addressed too in discussing implications and in discussing the utility of mathematics for society.

Just to very briefly show you what I am concerned about, I will quote a recent sentence – two sentences, actually – from a recent book "Mathematics and War". I think the sentences were written with bitter irony. "Mathematics can also be an indispensable tool. Thus when the effect of fragmentation bombs on human bodies was to be tested, but humanitarian concerns prohibited testing on pigs, mathematical simulation was put into place."

Helmut Neunzert

Now you get a little bit of a contrast programme. After a meta-theory of applied mathematics, we go back down to Earth. Maybe that is the difference between a pure and an applied mathematician, and you see it now live. But I must say we are not drifting apart. With respect to Yuri Manin's last sentence, I totally agree with him. But from the point of view, I would like to change a little bit our point of view now.

When I have spoken with people – Are pure and applied mathematics drifting apart? – some said. "Oh, this is this old question…". Some say "Yes", some say "No". I believe it is really the question of the department – if the people in each department like each other, then it's fine. If they don't, you have a drifting apart. But I would really like to change…. We always do as if mathematics would be the mathematics we do. We academic mathematicians are the world of mathematics. Are we really?

There is a second world, in my opinion. There's a second world of mathematics, and in this second world of mathematics almost all our graduates live. Those people we educate; they are not in general entering our world of academic mathematics. They go somewhere else. They go into industry, banks, insurance companies, R&D departments. There is a second world of mathematics outside of our world, outside of academia – in industry. And this is what I would call mathematics as a technology. And we should all be very happy that mathematics has become a technology, as Ronald Coifman has already described. It is really, for us also – even if we are pure mathematicians – it helps us a lot. I will come to this point later.

This mathematics as a technology, this second world of mathematics, is it pure, or is it applied? Let me describe to you a little bit the results of a project I had together with a psychologist and a historian. It is nice for a mathematician to work with other people. It was a Volkswagen Foundation project, and we were trying to find out what happened to all the graduates in Germany, in mathematics, in 1998. This is eight years ago. These psychologists are unbelievable. They have really asked in questionnaires these people unbelievable questions. I would have never dared to ask "Are you planning to get children?" and "How is the relation between your profession and your family?", and so on. But she did, and the people answered. And the question is: what have they done in the next eight years? What happened to them? Did their dreams, wishes, come true or not?

We had 3,000 graduates in Germany in 1998. That's quite a lot. I think the number today is even higher. Mathematics is very attractive in Germany – you may ask why.

And of this 3,000, 1, 400 went into high schools, so they normally become high school teachers. The other ones – 1,600 – made their diploma (or nowadays, a Master); 600 of these 1,600 were willing to answer a questionnaire. This is a very good sample. We asked these people again in the following years – in 2001, 2003, 2006. And what happened? What came out?

First of all, of these 1,600 – if you take this as a sample – only 10% became academic people. They entered universities or research centres. So we speak always about this 10%, and we forget the other ones. 80% (10% disappeared somehow) work as software designers in R&D, in banks, in insurance, in consulting, and so on. Do they do mathematics? They don't do much pure mathematics, I must say. I have asked 20 former PhD students of mine who work now in industry, and they were laughing and saying "Are you kidding me? If you ask us, do we do pure mathematics or applied, of course, we do not metaphors but models, and algorithms, if we do mathematics at all".

Not all of them do real mathematics. So if I see it correctly, 25% of all our graduates are doing mathematics in industry. The rest have changed – they do management, they do something which is not really mathematics. Now compare 25% to the 10% who go into academia. I claim that the second world of mathematics is a little bit larger than the first world, and we should keep that in mind.

There was a citation in the German Mathematical Society News from a mathematician who works at IBM. He said we should not overestimate the value of mathematics in industry. It is the midwife but not the mother of innovation. But maybe it's good to be a midwife, a very active midwife, which gives so many births to so many good innovations. So, you see what is the result; in this second world, at least as many people do mathematics as in the first world. But of course they do mainly applied mathematics. Now are these people drifting apart from pure mathematics? What would you say? There is this second world and the first world of pure mathematics – I don't think they know whether they are drifting apart. They don't see each other. It's so far away. How many of this second world are at this conference? If I am very optimistic, I would say 10 (out of 4,000). So you see there is a real, big difference between this applied mathematics in industry and the pure mathematics happening here. And this, of course, is very, very bad. I think this is a damage for both worlds.

It's a damage for the second world, for the world of mathematics in industry. Of course, there were some arguments already – we heard from Coifman and others – of course, we need more mathematics to make it better. It is not at all good in many things. In medicine, for example, we are totally missing good models which really describe the complex system of a body. So we would urgently need good mathematics which deals really with their problems. But are mathematicians really dealing with their problems? Yes, if they fit, in their own way. If not, I doubt it.

And for the first world, for our academic world, mathematics as a technology offers a lot. I think it offers new challenges – that was also already said. Many, many good problems come from this outer world. They add, certainly, public prestige. This second world adds money, if we have contacts with them, and it attracts students.

That's not such a minor thing. I think really that both worlds need each other very urgently, but we have to do something. We in the first world have to have open minds. We have to go into industry and see their problems, to speak with them, to get in contact with them, so they know we care about them, and vice-versa – they would be interested in what we are doing.

Peter Sarnak

I speak as a pure mathematician. I have a very keen interest in mathematics broadly, so I have tried to follow most mathematical topics, and I've tried applied maths too – it is much more difficult. My main credentials here being that I was a double major in math and applied math and in fact I had a difficult time choosing between pure and applied math. My views, I think, are going to be a little extreme towards the pure math side, but I think that a good proportion of the people in the audience are on the pure side, so maybe I shall try that angle. As Helmut says, one's views are highly influenced by one's local daily interactions. What happens in your department, and the discussions you have with your colleagues impacts you, and you'll see my views are impacted by my colleagues.

So firstly, are they (pure and applied math) drifting apart? Well, certainly we have to take into account this inflationary process of everything drifting apart, but even given that, it is my feeling that they are moving apart. I have been in mathematics for thirty years, and in this very short period my own experience is that it's not exactly what it used to be thirty years ago, and I think one of the big impacts is the computer which has changed how we go about our business.

Is the drifting apart a problem? I think it is a problem, but not one that's too serious. I think that math/applied math should evolve naturally like science, with good science surviving, and not such good science going away, and that is what should be allowed to happen here too. However, there are alarms, and we have heard a few suggestions, which sound very good. I will mention some alarms sounded by some of my younger colleagues, who I think we should definitely listen to.

Anyway, I'm going to take what may be a very controversial way of dealing with this question of whether they are drifting apart, by trying to see what is good math and what is good applied math, and if there is anything in common in fact between these two activities.

To give a formal definition of what pure math is would be very dangerous. I am sure I wouldn't get out of the hall by the end! But without defining good mathematics – and I am talking here about pure mathematics – we can all recognize it when we see it, like a fox when it sees a rabbit. You can see something that is really good, exciting and cuts to the bottom of a problem. I think the key ingredients, the cycle of ingredients in mathematics are firstly insight, mathematical insights, which often become conjectures, theories, language – these are crucial. But to me, the Holy Grail of mathematics, and something we can never give up, is that of proof. To me, once there is no proof I am not sure it's mathematics. At least, that is my take on it. That's the difference between mathematics and any other science.

Given the exciting week we have had here, let me give Thurston's geometrization conjecture as the epitome of this sort of good conjecture. It is a conjecture which when put forward immediately clarifies what one is looking for, as with all great conjectures – if they're true, they're great; of course, if it turned out to be false it would be much less interesting – but it appears to have turned out to be true. It's a unifying conjecture. It clarifies the shapes of 3-dimensional topological spaces, and it was not something that was obvious, but something that was built up with many examples and theories that he developed in order to come to that conjecture. So conjecturing is, of course, a major part in our subject, but Thurston, in thinking about this – I have not spoken to him recently – but I think you could say he was driven internally rather than by applications, and it is a damn good conjecture,even if it is driven internally.

Many fields have such powerful conjectures that unify the theories. But in describing this cycle I am not only talking about these special great conjectures, or only about mathematics that is unique and comes once in a blue moon. So there's that part of the cycle, which is conjecture, and then there is proof of the conjecture or more often proofs of approximations to the conjectures. As I have said before, and I will repeat, without proof, it's not our subject. So we really need that part, and as it seems clear now with Thurston's conjecture that Perelman has indeed proved it. This is as good as it gets. There have been other successes of this magnitude but we cannot judge all of mathematics by such high standards. This is what we strive for, and I think many people – young people – very strong people, go into math with such high aims in mind. Of course all of us except very few are disappointed, if our aims are so lofty.

I believe these central conjectures are what drive the subject. So we have a cycle of conjecture, theories built around the conjecture, solutions with good solutions generating good problems, and these develop further conjectures and further theories, and this cycle seems to repeat.

It looks – for someone from the outside – like a recipe for disaster, something completely internally driven. A recipe for a sterile subject. In fact, even within pure mathematics, subjects that are introspective, that interact with no other area, that only three experts in the world can talk to each other about (and one of them submits a paper to the Annals, and you get the second expert's opinion, and it of course says that this is the best thing ever written, but you can't get a third opinion) that's a problem. And such subjects naturally shrink. I think that allowing their natural evolution is the best way to let these things run.

Having indicated that good pure mathematics might seem to be driven solely internally, I want to argue that it is not. In fact I would argue that pure mathematics needs other sciences as badly as they need mathematics.

Now we have heard that we need to develop more mathematical theories for more applications and that there is much demand for such. These are very important to make mathematics as active as it is, but we happen to be living in a golden era of pure mathematics, as is witnessed by the very striking successes that we have seen in

recent years. I don't think such success can happen in a purely introspective world. Are we at this stage only because of the some special giants that have graced our field in recent times? I don't think so; I think that we are impacted from the outside and often in subtle ways.

Let me continue with the Perelman example a little. To repeat what Hamilton said in his talk here last week. Perelman's work depends heavily on Hamilton's work, which in turn is based on Ricci flow, and as Hamilton explained, the Ricci flow was motivated to him by Einstein's equations. In fact, the process he went through was the very process that Einstein went through in writing down his gravitational equations in equating the only invariant second order tensors that are around. So Hamilton when he was forming his Ricci flow equation,25 years ago, and at that point everything was very experimental, relied on this thing that he knew about Einstein's equations. This gave him a lot of confidence that he was on the right track. So this is a very – indirect, you might say – means of saying Physics impacted this particular programme, which on the face of it seems very internal. But it did give Hamilton the confidence to set off in the right direction and also as Perelman has indicated, his entropy idea which is one of his critical breakthroughs was inspired by a physics paper. I could give you many, many examples of similar things, where the input comes often from Physics, but also from other fields, for example Computer Science. Of course, in more complex applied math and engineering, such an impact is a little harder to see, but we do live in a world where we impact each other, and I don't believe we are a closed cycle, and we do need the applied side.

Just on a sociological level let me tell you, based on my experience,how to tell the difference between a theoretical physicist and a pure mathematician (I am not sure where the applied mathematician fits here). A mathematician will come into you office and tell you how complicated what he is doing is "My proof is highly nontrivial it is a thousand pages long" It is a strange discipline where to convince someone of something you have to write or make use of thousands of pages of complex arguments. Probably it means that one hasn't yet really understood the issue at hand. A Physicist comes into your office and he is always trying to tell you how simple and short what he is doing is and moreover it is universal and explains everything. He is lying because he is hiding 50 of more pages of calculations that he declares are trivial. This difference in presentation explains some of the difference in culture between these disciplines. The truth is somewhere in between. The idea that for something to be good it must be long and complicated is something that has evolved in certain quarters of mathematics, and it seems strange and wrong to me. In the end, we are always looking for the simple thing, and the real truth is somewhere in between these extreme views.

So my point is that while it is well recognized that science requires mathematics, progress in mathematics relies directly or indirectly on its applications and sub-areas of mathematics on their interaction with each other as well as with outside applications. When we turn to good applied math, I have very little right to talk, so I asked a few people for their opinions. But let me first take a completely extreme view. I

always remember this article by its title. This is an article by Halmos called 'Applied Mathematics is Bad Mathematics'. I did not read it until I was asked to be on this panel, at which point I thought "I wonder what he's got to say?". So I went and read it, and it is very entertaining. He is a good writer, but I think he is misguided. There are some bad points in the article, even if it is entertaining, and there are some interesting points. One bad point (in my opinion) is very relevant to what I am saying. He argues that mathematics can exist without applications – I am talking about applications generally, not just necessarily applied math but all other sciences. And he says mathematics can exist and will exist without applications, but the converse, he would argue, is false. I don't agree with him at all. I think mathematics cannot exist and flourish without the applications.Even the most pure math would not be where it is today if it were not for the applications.

Now, if you look back far enough, if you talk about Leibniz or Newton, they are philosophers, mathematicians and applied mathematicians simultaneously. But today, with everything requiring people to be very specialized, it's much harder to be universal. Even so, I strongly believe that the impact of applied math or applications is crucial to the development of math. Now I asked a colleague of mine, Weinan E, quite an opinionated young applied mathematician,and whose opinion I value, to give me a definition of what is good applied mathematics. He responded as follows: "It has to be relevant to application areas, whether the application area is in science, engineering, technology or industry". That's one thing he demands. The second thing – and this I found interesting – "It has to help in putting the relevant application area on a solid scientific foundation. This typically requires laying out the mathematical foundation". So he is emphasizing this foundational aspect that the mathematician is supposed to do in another science. Then he added – and this worries me: "Personally I'm very worried that mathematics and applied mathematics are gradually drifting apart", and he says this is particularly a worry in areas in which he works. He works in computational PDE, scientific computation.

Let me end here by saying there is obviously a common ground – and it was always the common ground for mathematics and anything else – and that is the search for those breakthrough ideas and insights. When I was young, I felt it was this common ground that made me feel there was no real difference between pure and applied mathematics. However, I am beginning to feel – and maybe I am just getting old – that there are differences. So as I said, in pure math, I cannot imagine mathematics without proof – or rather I cannot imagine it where proof is not important – where people say, well I do not even care about a proof. That would bother me. In applied math, the big issues or insights in the explanation of some phenomenon are central. It's not clear to me that proof is valued so much in applications. I often go to a lecture and the person ends by saying, especially if it's someone who has got a code or something: "My code works. Why do I need a proof that it works?". Well, it is a little hard to argue with something that works, that it requires a proof, although presumably in an ideal world the proof will give further insight,or an applied insight might lead to a proof. And that was the kind of ideal world that 25 years ago was

what I thought it was all about. But now I think this drifting apart is occurring, and I think you see this with the scientists involved, and I'm just an observer.

So let me end by saying that while it seems that the goals and the requirements of pure and applied math are diverging, even taking into account inflation,I think myself that evolution will take care of things. But I am quite concerned by the comments of Weinan E, and the comments of my fellow panellists, who also seem to be quite concerned (well, maybe not all of them – but some of them).

Contributions from the floor with answers by the panellists

John Neuberger opened the discussion by saying that pure and applied mathematics are drifting apart. "Mathematicians are badly needed in industry, but one should begin to connect with industry", he said. He gave some practical suggestions, like knowing what students will be faced with, and then letting the teaching be influenced by this. For example, since most mathematical questions from industry are phrased in terms of computing, students need to understand about computing. In his opinion, fruitful consulting arrangements are not so easy to come by, but individual efforts to make some connections with industry would help to modify the imbalance. He felt suspicious of a bureaucratic solution trying to pair mathematicians to industry, although this is a possibility. Hard frontier scientific problems demand the abilities of pure mathematicians, and they become applied once they get involved in them.

László Lovász claimed he did not feel so much that these sides of mathematics are drifting apart. He said that "Maybe that's because I grew up in a branch which was considered applied". He considered his fields – discrete mathematics and graph theory – an area of pure mathematics which has good applications. However, he pointed out that applications of mathematics arise in many different ways. "In the programme of this congress one could find excellent examples. For instance, Professor Itô won the Gauss prize for work which he did by motivations that I would consider completely pure and internal mathematical motivations, and it became extremely important in very real life activities, like for stock option pricing. Another kind of application is where the mathematician looks at some phenomenon and begins to think about it – what kind of mathematical phenomena could mimic this, could help to understand this. This is like the Nevanlinna prize-winner Jon Kleinberg – how he was looking at the internet and how it relates to the eigenvalues of the corresponding matrix, or Shannon by looking at channels of communication came up with the fundamental ideas of information theory. And then there is also applied math, which Professor Neunzert was talking about", answering direct questions from the real world. As another example, he mentioned Martin Grötschel's lecture at the congress, describing where one actually has to produce applicable results. To ban any of these different types of research, or to consider any of these as inferior would be a very serious mistake. It is the intellectual content of the work that should matter, and not its particular form. All three are terribly important for us. The level of mathematics

that other scientists need varies very much, and sometimes such a simple thing as solving a quadratic equation could be extremely useful. And in other cases, of course, you really need very sophisticated and new mathematics. But he does not feel pure and applied mathematics are drifting apart, really. He concluded by saying that "in mathematical areas which are thriving, there is always a lot of exciting connections with applications and with areas that come from the real world".

A participant from the floor, who introduced himself as a pure mathematician, was keen to have definitions and in particular one of an applied mathematician. He claimed not to be able to understand who was drifting from him. He asked whether people who are considered applied mathematicians should have a mathematical education.

Peter Sarnak responded: "One of the things that Weinan E was most concerned about was that people that he defines as doing applied math be educated mathematically in the traditional way. He felt this was really important. When he said he was very concerned, he in fact added that one of his concerns in this direction of education of students is that somehow the applied math community was not attracting the very best mathematically talented people. So I am just personally answering your question in connection with what he felt. I agree with you – who is drifting from who? That's a good question, but I think there is a difference in what an applied mathematician does and what a pure mathematician does. Lovász mentioned Itô – he had a major impact on the world, but he was not motivated in what he was doing by applications. Most pure mathematicians feel they are working on problems purely because of trying to understand numbers, geometry, the theory of equations more deeply, but the application which we all hope will come – and if it wasn't for that, it would not be that important a subject – but we do have a different way of going about things. Applied mathematics, I think, has to have applications in mind, and the style is very different. If you pick up a journal in pure mathematics, there is a theorem, there is a proof, or there is an attempt at making a certain kind of discussion. Many applied math or scientific journals you pick up, they are talking about a phenomenon, and there are pictures and phenomenology, which is all very interesting science, but we do things very differently. And I think that where these things surface is in your own department. So I would like to say that I agree with you, that we are all the same, but I think the way we go about things is very different".

Martin Grötschel started by saying that he would like to address one issue that has been implicit in the previous discussion: psychology, or more precisely, the psychology of mathematical institutions. He said: "Often, pure and applied mathematicians are located in different buildings. Lennart Carleson, for instance, stated 'in Sweden most departments which are applied have separate buildings'. This contributes considerably to the feeling of them and us. Many of us have lived alternating mathematical lives. I have been a pure mathematician for a while and now I am very applied, but I value both sides. One of the great experiences in my mathematical life was that, when I moved to TU Berlin, I noticed that there were no separate institutes of applied and pure mathematics – they were all together. Such an organization is actually something very precious, you can observe that people at TU Berlin – re-

search mathematicians and students, scientists from other disciplines – float between the various areas, depending on their current interests, and the distinctions between pure and applied vanish. I find this exchange extremely positive for all sides. This will help keep the various parts of mathematics together. I believe that the process of "cleaning" mathematics – which many universities went through in the last 50 years – by driving certain areas from mathematics into applied mathematics, and from applied mathematics into other institutions had really negative effects. If I look at the USA situation, applied mathematics, by and large, is defined by "dealing with differential equations". The mathematical optimizers are mostly in industrial engineering or management science departments, many discrete mathematicians belong to computer science departments, statisticians are everywhere but rarely in mathematics, and so on. Can one find really good arguments for such a distribution? What is the reason for this? The current separation of pure and applied mathematics is not a "logical consequence" of different ways of doing mathematics. An unbiased look at the historical development reveals that, in most cases, power games, financial considerations, and personal conflicts within the mathematical community considerably contributed to this effect. It is easier to separate people than solving conflicts. This has been a bad evolution resulting in clustering processes which in turn have led to the psychological situation we are faced with at present. It is my belief that we should try to bring these separate groups/clusters back together. I think that the "institutional unification" would resolve many of the issues we are discussing here. I believe that the institutional and spatial separation contributes a lot to the feeling expressed here by many that there are trenches between various parts of mathematics, in particular between pure and applied."

David Levermore thanked the panel for a very thoughtful discussion and commented as follows. "I have a hat that is a pure hat and an applied hat, so if I can try and speak for both sides of the issues. I think Martin raised a very important point – institutionally what can we do? I think the issue is not so much we drift apart, I think that criticism is valid because we do have control of this. I think the phenomenon has to do with the expansion of human knowledge and endeavour, and that all disciplines to some measure are confronted with this, in particular universities, but also all institutions, not just academic". Then he mentioned some models growing in the USA in response of what he termed balkanization: "One model that does exist in the US, and is thriving in some institutions, is the development of centres – centres that focus around maybe an application or an idea, that brings together people, a mathematical paradigm or an engineering paradigm, or whatever, to work together, learn from each other and stimulate each other. Just, for example, the mathematics department at Maryland is tied to a Norbert Wiener centre in applied harmonic analysis, which involves pure mathematicians and engineers. We have a list of several institutes like that. And I think that if we put our minds to it, we can overcome these sort of intellectual barriers that separate us artificially, because ultimately I think the picture the whole panel has painted is that this is a human endeavour and is really the right one, and I look forward to a very good future".

The moderator of the round table, John Ball, described something about his own experiences of applied mathematics. "I work in the calculus of variations, but also in its applications to materials, and I've written papers with electron microscopists. Now I believe in the value of theorems in applied mathematics, and I believe in the value of theorems for telling us when computer codes work. To me, it seems that the three elements of modelling, analysis and computation all feed on each other to improve what goes on. But I think there is an interesting process when you start working in a new area, a new scientific or some new application area, and something gets you interested in it and then you see that there is something mathematical and you learn a bit more about it, and at some point you have to have some confidence that you can offer something to this field. At the same time, you have not done a degree in the bio-sciences or materials or whatever subject it is, and so you have to somehow be humble and put in a lot of work to learn at least a little piece of this area so that you can break down these language barriers. I think that is a really exciting process, but to start with you may encounter some resistance from the people in the area, and one piece of advice I have is always to cut out the middleman – or woman – and talk directly to the person who is doing the experiments and try maybe to avoid some of the intervening theory", he said.

The colleague who previously asked for a definition of an applied mathematician asked the panellists if they believe that an applied mathematician is a mathematician and if he or she should have the qualification of a mathematician.

Peter Sarnak: Well, my answer would definitely be "Yes", but I think I'd better let some of the other people on the panel give their view of it.

Helmut Neunzert: Would you say "Yes" with respect to the question that he must have a mathematical qualification to be a mathematician?

Peter Sarnak: To a certain extent… he needs to know certain basics, absolutely.

Helmut Neunzert: How many mathematicians in this room do not have a mathematical education? I mean, I know many physicists who have become very good mathematicians later on. Would you not count them?

Ronald Coifman: If we follow Peter Sarnak here, he would tell you that anybody who can prove theorems qualifies, right? The only issue is: What do you mean by proving theorems? I know what you mean but I think you did not think about it enough. An applied mathematician would come up, say, with a computational algorithm, then the theorem involved in that algorithm is that he can by a certain scheme compute something to some precision. That's a theorem, right? And the goal there is not to climb the Everest and prove some old conjectures or do something that will impress your colleagues. The goal is to achieve, to solve difficult problems, to find the tools to do it, and it's really the intellectual challenge involved which maybe will qualify him as being a good mathematician or a good applied mathematician – I don't think it makes any difference. It's really the intellectual novelty and content that will allow you to think of the person as a mathematician. I think Shannon was an engineer, right? And there is no way you could say he was not a mathematician.

Robert Kohn found very reassuring that there was some difficulty in defining, in separating the applied mathematicians and the pure mathematicians. "I think that something that nobody took the time to do was to talk about how mathematicians pure and applied are really rather different in our mission, in our world view and in our functioning, from the other sciences. The most important thing here is not that we worry about creating separations between pure and applied mathematicians, or defining those two. It's really more about making sure we don't leave a big gap between mathematics on the one hand and other areas of science on the other. In the areas I work in, which tend mainly to be close to the physical sciences or finance, the mathematician's job is to think about whether the algorithm really works, to think about what are the properties of this model, to solve problems, to look at whether opportunities have been missed by not bringing to bear the right set of tools, to develop new tools sometimes if they are called for in the application area. And there is nobody else out there who is going to do that if we don't. Fortunately, I think that to a large extent we are not drifting apart. I disagree with many panel members, and I think that the talks at this meeting are the best possible proof of that", he said.

Two participants asked whether there is some need to create a new type of mathematics and even a new type of science for investigation of the reality, as was suggested by the Russian mathematician Andrei Kolmogorov in the last years of his life. For example, to deal with self-references, self-organization, as one could find in biological systems.

Ronald Coifman answered: "It's a terrific question. In terms of dealing with the kinds of mathematics that you need to deal with, say, biology or social sciences, or the more complex structures where every piece of information you measure is linked to the others. I think what seems to be emerging is something like what emerged in physics a long time ago, when Einstein decided that physics is geometry, and that you can describe the physical equations as basically the geometry of space-time, and later on in Yang–Mills and gauge field theories, somehow the physicists got to the point that the geometry encapsulates the relationship between all objects around us. I think we see this emerging in the analysis of actual data of various kinds, whether it's data on the web where you can actually do a fast search by relating every unit of the web to each other and doing something on the global geometry of the web, in order to get the Google rank, or some others. It is a subtle and profound idea, possibly, and we see it happen in biology and neurology and everywhere else. It is a web of relations between objects which encapsulates their internal geometry or their content. That's my view at the moment. I think it is just emerging".

Jean Pierre Bourguignon, director of the Institut des Hautes Études Scientifiques in Bures-sur-Yvette, France, and a specialist in differential geometry and global analysis, stressed the need of conducting the discussion at three different levels to avoid further confusion. "Three levels need to be distinguished: the first one is really the science itself, and if you speak about the science itself, I think the terminology separating applied mathematics and mathematics is not a good one, as was pointed out already by some people. The second level concerns us as professionals; most of us are

really making a living by teaching, so it means that what happens to our students is something that should be of primary importance to us, and from that point of view I find the remarks by Professor Neunzert very adequate. That is, if so many of our graduates are really working in the world of technology, I think we, as professionals, need to know more than a little bit what will be our graduates' environment. And the third level takes us as scientists, and because of the growing impact of science on society, we also have another role, namely to provide answers to problems posed by society at large. In this context, we are also asked to interact with other scientists, and more generally with people working in the world of technology. It seems to me that, depending on the level one considers, then the drifting that is the subject of the Round Table has to be measured by different means. It is certainly true that if one takes the first angle, I think there is no drift, because – and this congress provided a very good proof of it – we have ample evidence of the fantastic impact of new questions coming from technology on mathematical research. If one takes the second point of view, then the growing number of our graduates who work for companies, and therefore really using the skills we give them in a very applied way, forces us to get a better knowledge of these applications. And the third level raises the question of the way in which we can contribute to the scientific enterprise, that is more and more shaping the world, and shaping the world means good and bad things at the same time, but certainly new responsibilities – and that is probably the one in which the ethical dimension of our profession is very important –", he said.

Anatole Joffe joined the discussion by pointing out that though the subject under discussion was far from new, the matter was still of great interest. Plutarch (Parallel Lives: Marcellus) in the context of Archimedes' involvement with the defence of Syracuse, had already described the separation between mechanics (applied mathematics) and geometry (pure mathematics) which for Plato was the key to knowledge. He quoted Marc Kac who about forty years ago, mentioned that pure mathematics deals with deep questions in simple situations, while applied mathematics deals with simple questions in extremely complicated models. In Joffe 's opinion, it is very hard to find definitions which will please everybody. The distinction is more likely to be between the pure and the applied mathematician than between pure and applied mathematics. He argued that the pure mathematician is somebody whose motivation comes from inside the subject, while the applied mathematician answers questions asked by other scientists, in order to try to be useful to society. He recommended encouraging all mathematicians to be more receptive to dialogue with scholars of other fields.

Bernhelm Booss-Bavnbek spoke by referring to Harald Bohr and Hardy about the distinction between two phases in sciences: the extending and the consolidating phase. Clearly physics has been in a consolidating phase in the first half of the last century, after a previous period of extension with many new single results at the end of the 19th century. One could claim that mathematics in the first half of the last century still was in a phase of extension, and that what mathematics needed was a new phase of consolidation. Booss addressed Professor Manin asking him whether

he would agree with Peter Sarnak who said that we have had a golden period of about 30 years for pure mathematics, in Booss' terms a phase of truly consolidation, where various fields in pure mathematics showed and proved to be interconnected. Could this be a good starting point to make real valuable contributions to other fields like biology, which in spite of the great achievements of Watson and Crick 50 years ago still is in this phenomenology? More concretely, if on the basis of these last 30 years of mathematics consolidation, there is a new impulse for mathematicians to do something towards contributing to consolidation in these more phenomenologically expanding sciences?

Yuri Manin answered: "Sarnak said the last 30 years were years of great consolidation and maturing of the mathematics of the 20th century. I'm less sure – I mean emotionally less sure – about how to characterize in such admittedly simplistic terms the development that is connected with computers, computer science and internet. Kolmogorov, whose name was mentioned here, introduced the notion of Kolmogorov complexity. Kolmogorov complexity, very roughly speaking, of a piece of information is the length of the shortest programme which can be then used to generate this piece of information. In this respect one can say that classical laws of physics – such fantastic laws as Newton's law of gravity of Einstein's equations – are extremely short programmes to generate a lot of descriptions of real physical world situations. I am not at all sure that Kolmogorov's complexity of data that were uncovered by, say, genetics in the human genome project, or even modern cosmology data – I am not at all sure that their Kolmogorov complexity is sufficiently small that they can be really grasped by the human mind. One should be aware that if a certain large piece of information has very large Kolmogorov complexity, then we are bound not to understand it. We are bound to relegate the processing of this data to computers or computer nets, or whatever. And I have a very strong suspicion that this is a new situation in natural sciences, with which we really do not yet know how to cope. We produce technology, and it might happen that this technology is absolutely indispensable to deal with this data.

The discussion ended with a few words by the moderator, John Ball, who said that he wouldn't dare summarize the discussion, very interesting though it had been. He thanked all those who had participated, Marta Sanz-Solé, who organized the round table, and especially the panel.

From the private to the public: The road from Zurich (1897) to Madrid (2006)

José M. Sánchez-Ron

Abstract. We review the history of the International Congresses of Mathematicians, from Zurich 1897 to Madrid 2006, mentioning some of the most significant personages and events (scientific as well as political) of such meetings (as a matter of fact, that history did not begin 1897 in Zurich, but in 1893 at the Chicago World's Columbian Exposition). We report on Felix Klein, Henri Poincaré, David Hilbert, Vito Volterra, Emmy Noether, Ludwig Prandtl, Laurent Schwartz, Klein's *Encyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, and the role played by the Mathematical Tripos in the education at Cambridge University during the 19th and the first decades of the 20th century (and its influence in the design of the Cambridge 1912 Congress). Some of the further topics discussed here are how the two world wars affected the congresses, the creation of the Fields medals, as well as some of the main changes that mathematics has experienced, internally (i.e., in what it refers to problems, ideas and theories) as well as institutionally (including its manifold connexions with society) during the period covered by the existence of the International Congresses of Mathematicians.

Mathematics Subject Classification (2000). Primary 01A60.

Keywords. International Congresses of Mathematicians.

"What was formerly begun by a single mastermind, we now must seek to accomplish by united efforts and cooperation". The author of these prophetic words was Felix Klein, the distinguished German mathematician, and they were stated at the "World Congress" of mathematicians that took place, from the 21st to the 26th of August, as part of the 1893 Chicago World's Columbian Exposition (Klein was one of the commissioners of the German university exhibit at the Exposition). Forty-five mathematicians attended that meeting, of which only four were foreigners: the Germans Klein and Eduard Study (the only ones who delivered lectures), the Austrian Norbert Hertz, and the Italian Bernard Paladini, although Charles Hermite, David Hilbert, Adolf Hurwitz, Hermann Minkowski, Max Noether, Salvatore Pincherle and Heinrich Weber supported the congress by submitting papers *in absentia*.[1]

The leading role of Klein in promoting in the New World the spirit of international mathematical collaboration and interchanges (also, of course, German culture) is

[1] The proceedings were published as *Mathematical Papers Read at the International Mathematical Congress Held in Connection with the World's Columbian Exposition Chicago 1893*, E. H. Moore *et al*., eds. (Macmillan & Co., New York 1896). About the congress, and Klein's influence in America, see Karen Hunger Parshall and David E. Rowe, *The Emergence of the American Mathematical Research Community, 1876–1900: J. J. Sylvester, Felix Klein, and E. H. Moore* (American Mathematical Society/London Mathematical Society, Providence 1994).

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

clear. Indeed, after the adjournment of the Chicago congress, the Göttingen professor consented to hold a colloquium on mathematics with those members of the meeting which might wish to participate. The Northwestern University at Evanston, Illinois, tendered the use of rooms for such purpose, and there Klein lectured to 23 American mathematicians (Study was also present) from August 28 until September 9. Alfred Clebsch, Sophus Lie, the shape of algebraic curves and surfaces, the transcendency of the numbers e and π, the solution of higher algebraic equations, hyperelliptic and Abelian functions, and the study of mathematics in Göttingen were among the persons and topics he treated.[2]

Obviously, we cannot consider the Chicago meeting as the first international congress of mathematicians, but it certainly was the forerunner of those meetings, which began four years later in Zurich 1897, attended by less than 200 mathematicians (only 4 of them, by the way, women).

More than a century after Klein's above cited statement, looking back from Madrid 2006 at what has happened in mathematics during all those years, we realise how wise the author of the "Erlangen Program" was. It is true that mathematics can still, perhaps more than any other scientific discipline, be practised with outstanding success in the solitude of a room, by an individual, by a "single mastermind", but it is not less true that its scope has grown in such a way that it needs for its development and health, and very much so, "united efforts and cooperation". That this is so is due not only, nor perhaps mainly, to the increasing difficulty of mathematical problems, but to the incredible widening of the range of fields in which mathematical expertise is needed: from aerodynamics and hydrodynamics to economics and meteorology, from architecture to ecology, not forgetting more traditional sites such as physics, or others that appeared during the XXth century, as, for instance, the design of computers. It is because of this, as well as because of the almost dramatic growth of the attendance to the International Congresses of Mathematicians, that in the title of my exposition appears the expression "From the private to the public."

Before turning to the Zurich Congress, let me point out that mathematics was not the first scientific discipline to organise international meetings. Thus, chemists assembled in the famous 1860 Karlsruhe International Congress of Chemists (again, it was the idea of a German, Friedrich August Kekulé).[3] However, that meeting was not followed by others; that is, there was not the continuity that would characterise the International Congresses of Mathematicians. In this sense, the mathematicians meetings opened a new era of international communication that was adopted by other scientific (and non-scientific) disciplines during the XXth century. (Physicists had to wait until 1911, with the Solvay Conseils, but even then their scope was very different, with only a handful of scientists being invited).

[2] Klein's lectures were published as: Felix Klein, *Lectures on Mathematics* (Macmillan, New York 1894; reprinted by AMS Chelsea, Providence 2000).

[3] *Compte rendu des séances du Congrès international des chimistes réuni à Carlsruhe le 3, 4 et 5 septembre 1860*, "Anlage 8" in vol. I of *August Kekulé*, 2 vols. (Verlag Chemie, Berlin 1929), pp. 671–688; reproduced in Mary Jo Nye, ed., *The Question of the Atom. From the Karlsruhe Congress to the First Solvay Conference, 1860–1911* (Tomash Publishers, Los Angeles 1984), pp. 633–650.

The first International Congress of Mathematicians: Zurich (1897)

The ideals of "united efforts and cooperation" which Klein stated in Chicago were taken up by Hermann Minkowski, then professor at the Zürich Polytechnikum, where he was teaching, among other students, Albert Einstein. In a letter dated November 17, 1896, he wrote to his friend David Hilbert (whom he joined a few years later in Göttingen):[4] "It just occurred to me – for several days we have been meeting in regard to the international mathematical congress." Indeed, an announcement of the proposed meeting was circulated at the beginning of the new year under the names of 22 mathematicians, eleven of which were from Zurich (one of them was C. F. Geiser, another of Einstein's teachers at the Polytechnikum). "After considerable correspondence," the announcement read, "the question of the place of holding the Congress has been decided in favour of Switzerland, as a country peculiarly adapted by situation, relation, and traditions of promoting international interests."

The opening lecture of the congress was given by Henri Poincaré ("Sur les rapports de l'analyse pure et de la physique mathématique"),[5] who, however, could not attend the meeting because of illness (a professor of the Polytechnikum, Jérôme Franel, read his contribution), while the closing one was delivered by Felix Klein ("Zur Frage des höheren mathematischen Unterrichts"). It was quite appropriate that Poincaré and Klein, who had spent years competing in mathematics research, were united in that historical First International Congress of Mathematicians. Only two other plenary lectures were delivered, by Adolf Hurwitz (Zurich) and Giuseppe Peano (Turin).

Paris (1900): Hilbert's famous lecture

Some thought improper Poincaré's lecture in Zurich, although posterity has given it a different status. David Hilbert considered whether he should reply to it when he thought about which topic to talk at the next congress, but Minkowski recommended him not to do so. Instead, he advised him in a letter of January 5, 1900, that it would be "most alluring… to attempt to look into the future, in other words, a characterisation of the problems to which the mathematicians should turn into the future. With this you might conceivably have people talking about your speech even decades from now. Of course, prophecy is indeed a difficult thing."[6] Hilbert followed his suggestion.

The Second International Congress of Mathematicians, held in Paris from August 6 to 12, 1900, with Charles Hermite as *Président d'honneur* and Poincaré as effective

[4] Quoted in Donald J. Albers, G. L. Alexanderson and Constance Reid, *International Mathematical Congresses. An Illustrated History, 1893–1986* (Springer-Verlag, New York 1987, revised edition), p. 4.

[5] Henri Poincaré, "Sur les rapports de l'analyse pure et de la physique mathématique", *Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich, 1897*, F. Rubio, ed. (Teubner, Leipzig 1898), pp. 81–90. Poincaré's lecture has been analysed by Jeremy J. Gray, *The Hilbert Challenge* (Oxford University Press, Oxford 2000), pp. 80–83. Besides of appearing in the proceedings of the congress, Poincaré's lecture was inserted in his book *La valeur de la science* (1905), as well as in *Acta Mathematica* 21, 331–341 (1897)).

[6] Quoted in J. Gray, *The Hilbert Challenge*, *op. cit*., p. 57.

President, could have been remembered for many things: perhaps for Poincaré's new intervention, "Du rôle de l'intuition et de la logique en Mathématiques"; maybe, although not likely, for Vito Volterra's lecture "Betti, Brioschi, Casorati, trois analystes italiens et trois manières d'envisager les questions d'analyse" or Gösta Mittag-Leffler's "Une page de la vie de Weierstrass". Maybe even because of some of the short communications, H. Padé's, "Aperçu sur les développements récents de la théorie des fractions continues", or Jacques Hadamard's "Sur les équations aux dérivées partielles à caractéristiques réelles". However, as it is well known, that congress is remembered, even now, more than a century afterwards, for David Hilbert's famous lecture "Mathematische Probleme." Nevertheless, Hilbert's presentation was not the opening lecture of the congress, such honour fell on the leading German historian of mathematics Moritz Cantor from Heidelberg, the author of the monumental *Vorlesungen über Geschichte der Mathematik* (*Lectures on the History of Mathematics*), the first volume of which appeared in 1880. Cantor's lecture (delivered in French) was entitled "Sur l'historiographie des Mathématiques", and was followed by the invited lecture of Volterra already mentioned. As a matter of fact, Hilbert's contribution was only a communication at 9 o'clock in the morning of August 8, followed by two more. The session should have been presided by prince Roland Bonaparte, but Napoléon's descendant did not appear – losing a unique occasion to be present, albeit in a secondary manner, in one of those rare occasions which could be called immortal, that his family had so much valued – and Moritz Cantor assumed the presidency. It is true that in the proceedings of the congress, Hilbert's intervention appeared in the part of "Conférences" (plenary lectures),[7] after Cantor's and Volterra's, but this was so because the editors recognised its importance once the text was received: "On trouvera plus loin," we can read in the proceedings, "le développement de la Communication de M. Hilbert qui, en raison de sa grande importance, a été placée parmi les conférences."[8] Hilbert was well recognised by his French colleagues, but only to give him the presidency of the August 7 and 9 sessions. Indeed, we know from a letter that Poincaré wrote to his good friend, the Swedish Gösta Mittag-Leffler on November 22, 1900, that by then Hilbert's text was not considered yet important or has not been received:[9] "On va mettre sous presse," Poincaré then wrote, "les *Comptes Rendus des travaux du congrès des Mathématicians*; on commençera naturellement par les conférences. Celles de MM. Cantor, Volterra et la mienne sont deja composées."

As to the closing session, it was occupied by the already mentioned lectures of Poincaré and Mittag-Leffler.

By the way, a Spaniard, Zoel García de Galdeano, from Zaragoza, presented a short (one page) communication, which was duly included in the proceedings: "Note

[7] David Hilbert, "Sur les problèmes futurs des mathématiques", *Compte Rendu du Deuxième Congrès International des Mathématiciens* (Gauthier-Villars, Paris 1902), pp. 58–114. In a footnote it was stated that "l'original de la traduction a paru en allemand dans les *Göttinger Nachrichten*, 1900. M. Hilbert a fait ici quelques modifications à l'original au § 13 et quelques additions au § 14 et au § 23".

[8] *Compte Rendu du Deuxième Congrès International des Mathématiciens*, *op. cit*., p. 24.

[9] *La correspondance entre Henri Poincaré et Gösta Mittag-Leffler*, Philippe Nabonnand, ed. (Birkhäuser, Basel 1990), p. 296.

sur la critique mathématique". He was one of the three Spaniards (among the 252 mathematicians) who attended the congress, the other two were Leonardo Torres Quevedo, the famous engineer, and José Rius y Casas, also from Zaragoza. Together with José Echegaray, García de Galdeano was the mathematician who did most to foster advanced mathematics in Spain during the XIXth century.

Among the many outstanding mathematicians participating in the meeting let us mention Émile Borel, Gaston Darboux, Ivar Fredholm, Jacques Hadamard, Tullio Levi-Civita, Hermann Minkowski, Paul Painlevé, Giuseppe Peano, Carl Runge and Giuseppe Veronese, as well as the physicists Joseph Larmor and Edmund Whittaker.

A final comment. Because of the historical importance of Hilbert's talk, we tend to assume that the Paris Congress must have been recognised by Parisians as a special occasion at the time. Not so. As a matter of fact, it was one of some 200 conferences held in Paris that year in connection with the World Exhibition.[10]

Heidelberg (1904), Klein's *Encyklopädie* and Ludwig Prandtl

I shall report on two events of the third congress. One is the presentation of Felix Klein's *Encyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen* (*Encyclopaedia of mathematical sciences, including its applications*), and the other is about one of the participants in the meeting, the applied mathematician and engineer Ludwig Prandtl, no one usually mentioned in the histories dealing with that congress. He was the world's leading expert in aerodynamics, a man who was able to move with equal grace between engineering and applied mathematics. He embodied one of Felix Klein's most dear ideals: the scholar who could promote at the same time both mathematics and an applied subject. In the words of Theodore von Kármán, another outstanding aerodynamics expert:[11] "Perhaps what one must wonder at most in Prandtl's scientific method, the direct connection of general, abstract theorems with experimental facts and practical applications, is pure, unadulterated Göttinger Tradition, which adapted by F. Klein in new form and to the demands of the technological century, has undergone a rejuvenation". It is therefore not surprising that Klein succeeded (in 1904) in getting Prandtl to Göttingen as professor and as one of the two directors (the other was Carl Runge) of a brand new Institute for Applied Mathematics and Mechanics.

That Third International Congress of Mathematicians took place in Heidelberg, organized by Heinrich Weber and was attended by 336 persons, i.e. 107 more than at the previous meeting. The largest delegation was from Germany (173), followed by Russia (30), Austria-Hungary (25), France (24), United States (15), Denmark (13), Italy (12) and Switzerland (12). Only one Spaniard (again García de Galdeano) participated.

[10] J. Gray, *The Hilbert Challenge*, *op. cit*., p. 59.

[11] Theodore von Kármán, "Ludwig Prandtl," *Zeitschrift für Flugtechnik und Motorluftschiffahrt* 16, 37 (1925).

It was there that the first volume of one of Klein's most ambitious mathematical enterprises, the monumental *Encyklopädie der mathematischen Wissenschaften*, which assembled all pure and applied mathematics (meaning not only "technological matters" but most physics branches) was presented. As a matter of fact, at the same time the first volume of the French version of the encyclopedia, the *Encyclopédie des sciences mathématiques*, was introduced. Its main editor, Jules Molk, from Nancy, was in charge of the presentation. As it is less known than its German counterpart, it might be of interest to quote some of Molk's words at the presentation:[12] "J'ai l'honneur de vous presenter le premier fascicule de l'édition française de l'Encyclopédie des sciences mathématiques. Cette édition française vient s'adjoindre à l'édition allemande de la même Encyclopédie. Ce n'est pas une simple traduction : c'est un exposé, fait par des mathematiciens de langue française, des articles contenus dans l'édition allemande ; ces articles son complétés, mis à jour ; le mode d'exposition est d'ailleurs entièrement conforme aux traditions françaises".

It was at Heidelberg, too, that Ludwig Prandtl presented (as one of the eighty papers read) his most admired and enduring scientific contribution: the boundary-layer hypothesis (that a state of flow can be approximated by a wall zone of viscous influence and an outer zone of irrotational motion), which whould later prove essential in the then small core of fundamental concepts constituting the theory of aerodynamics.[13] Apparently, however, it "received only passing attention from the mathematicians who heard it", according to the historians of hydraulics, Hunter Rouse and Simon Ince. Its significance, of course, was not lost on Klein.[14]

I mentioned before Cantor's *Vorlesungen über Geschichte der Mathematik* and said that the first volume had been published in 1880. The second appeared in 1893, and the third in several parts between 1894 and 1898. These volumes covered the history of mathematics from its beginnings up to 1758. It was at the Heidelberg Congress that a fourth volume was planned that would go up to 1799. This volume was published in 1908, written by nine historians of mathematics, with Cantor as editor-in-chief. We may therefore say that the International Congresses of Mathematicians also form part of the historiography of mathematics, or, to express it differently, to the history of the history of mathematics.

As to the general lectures in Heidelberg, they were delivered by: L. Könisgsberger ("Carl Gustav Jacob Jacobi"), P. Painlevé ("Le problème moderne de l'intégration des équations différentielles"), A. G. Greenhill ("The Mathematical Theory of the Top considered historically"), C. Segre ("La Geometria d'oggidì e i suoi legami coll' Analisi"), and W. Wirtinger ("Riemanns Vorlesungen über die hypergeometrische Reihe und ihre Bedeutung").

[12] *Verhandlungen des Dritten Internationalen Mathematiker-Kongresses in Heidelberg vom 8.bis 13. August 1904*, A. Krazer, ed. (Druck und Verlag von B. G. Teubner, Leipzig 1905), p. 36.

[13] Ludwig Prandtl, "Über Flüssigkeitsbewegung bei sehr kleiner Reibung," *Verhandlungen des Dritten Internationalen Mathematiker-Kongresses*, pp. 484–491.

[14] Hunter Rouse and Simon Ince, *History of Hydraulics* (Institute of Hydraulic Research, Iowa City 1957), p. 230; quoted in Paul A. Hanle, *Bringing Aerodynamics to America* (The MIT Press, Cambridge, Mass., 1982), p. 43.

Rome (1908), Volterra's reign

The Fourth International Congress convened in the spring of 1908 in Rome, a fitting tribute to the Italian mathematics eminence. Departing from the tradition of previous congresses, the Italians doubled the number of plenary addresses. Hilbert and Klein were invited but they had to decline. Darboux and Veronese were among the speakers. So was Poincaré, but, again, he felt ill and could not deliver his lecture (it was read by Gaston Darboux, who also was in charge of one of the general lectures, "Les origines, les méthodes et les problèmes de la Géométrie infinitésimale").[15] It was the last time that Poincaré was to attend one of these meetings: he died a few weeks before the next one was inaugurated.

The opening address was entrusted to Vito Volterra, who spoke about "Le Matematiche in Italia nella seconda metà del Secolo XIX."[16] The other main speakers were Walther von Dyck, Andrew R. Forsyth, Gösta Mittag-Leffler, the American astronomer Simon Newcomb, Émile Picard, Giuseppe Veronese, and the physicist Hendrik A. Lorentz, who tackled a fundamental problem which would play a central role in the origins of quantum physics: "Le partage de l'énergie entre la matière pondérable et l'éther." Almost nine years after Max Planck had introduced his radiation law as well as the quanta, Lorentz told his Rome audience how uncertain the situation still was:[17] "… si l'on compare la théorie de Planck et celle de Jeans, on trouve qu'elles ont toutes les deux leurs mérites et leurs défauts. La théorie de Planck est la seule qui nous ait donné une formule conforme aux résultats des expériences, mais nous ne pouvons l'adopter qu'à condition de remanier profondément nos idées fondamentales sur les phénomènes électromagnétiques… La théorie de Jeans, au contraire, nous oblige à attribuer à un hasard pour le moment inexplicable l'accord entre les observations et les lois de Boltzmann et de Wien."

Almost as many of the papers were presented in French (51) as in Italian (53). Max Noether, the noted algebraist, brought his daughter Emmy as a guest. I must confess that I have a special predilection for Emmy Noether. Not only because of all the difficulties she suffered during her life – just because she was a woman, a female mathematician in a men's world – but also for her "Noether's theorems", which relate symmetries to conservations laws. Despite of Hilbert, Klein and Hermann Weyl's support – and of Einstein's – Noether never could get an official, not to say permanent, position in Göttingen. When in January 1933 Hitler assumed the power in Germany, she had to abandon her country, and travelled to the United States, to the Mathematics

[15] H. Poincaré, "L'avenir des mathématiques", *Atti del IV^e Congresso Internazionale dei Matematici*, G. Castelnuovo, ed. (Tipografia della R. Accademia dei Lincei, Roma 1909), vol. I, pp. 167–182; also published in *Rendiconti del Circolo Matematico di Palermo* 26, 152–168 (1908).

[16] During the first congresses, history of mathematics appeared rather frequently among the topics considered. Besides Volterra's lecture, in Rome Gino Loria launched a project for the production of a textbook for training in the history of mathematics. When the project failed because of World War I, Loria published material he had collected as a *Guide allo studio della storia della matematica* (1916; second expanded edition, 1946).

[17] H. A. Lorentz, "Le partage de l'énergie entre la matière pondérable et l'éther", *Atti del IV^e Congresso Internazionale dei Matematici*, op. cit., vol. I, pp. 145–165; p. 163; reprinted in H. A. Lorentz, *Collected Papers*, vol. VII (Martinus Nijhoff, The Hague 1934), pp. 316–342; p. 341.

Department at Bryn Mawr College, a women's college that offered her the hope of a new life. Alas, she died soon, as a consequence of a surgical operation she underwent in April 1935. She was only 52 years old.

Cambridge, 1912, the heritage of the Mathematical Tripos

The Fifth International Congress took place at Cambridge in Great Britain (August 22–28, 1912). It was attended by 574 mathematicians. Lord Rayleigh was the Honorary President and Sir George H. Darwin the effective President, as president of the Cambridge Philosophical Society, which was the institution responsible for the organization of the event. A physicist the first and a geophysicist the second, both were products of the Mathematical Tripos, the educational system that reigned supreme in Cambridge since the eighteenth century.[18] Unfortunately, I have no time here to explain this system that favoured more the development of mathematical physics than of mathematics in Britain; I will only say that its emphasis was on applied mathematics, and that many of the most distinguished British physicists, as well, of course, of mathematicians, were products of the Tripos, among them George Gabriel Stokes (1841)[19], Arthur Cayley (1842), William Thomson (Lord Kelvin) (1845), Peter Tait (1852), Edward Routh (1854), James Clerk Maxwell (1854), John Henry Poynting (1876), Joseph Larmor (1880), Joseph J. Thomson (1880), Bertrand Russell (1893), Edmund Whittaker (1895), James Jeans (1898), Godfrey Harold Hardy (1898), James Chadwick (1900), Arthur Eddington (1904) and John Edensor Littlewood (1905).[20] In general, physicists did better than mathematicians in the Tripos, due to its applied character.

Probably in no other congress, before or afterwards, pure and applied mathematics mixed up more. If we look, for instance, at the plenary lectures, we find that of the eight delivered, half of them were dedicated to applied mathematics: Ernest W. Brown ("Periodicities in the solar system"), Prince B. Galitzin ("The principles of instrumental seismology"), Joseph Larmor ("The Dynamics of Radiation"), and W. H. White ("The place of Mathematics in Engineering Practice"). The remaining four were given by Maxime Bôcher, Émile Borel, Federigo Enriques and Edmund Landau, all "pure" mathematicians. As to the sections, they were dedicated to: "Arithmetic, Algebra, Analysis," "Geometry," "Mechanics, Physical Mathematics, Astronomy" (with 25 communications presented by scientists like Max Abraham, Peter Paul Ewald, Horace Lamb, A. E. H. Love, Ludwig Silberstein, Marian von Smoluchowski, J. J. Thomson, and the Spanish Esteban Terradas, who spoke, in French, "Sur le mouvement d'un fil"), and, finally, the sections "Economics, Actuarial Science, Statistics," and "Philosophy, History, Didactics."

[18] Rayleigh (J. W. Strutt) was *senior wrangler* in 1865, and George Darwin *second wrangler* in 1868.

[19] The year in brackets is the year of graduation.

[20] See Andrew Warwick, *Masters of Theory. Cambridge and the Rise of Mathematical Physics* (The University of Chicago Press, Chicago 2003).

As I said before, Poincaré had died when the congress began. At the opening session, G. H. Darwin remembered him with the following words:[21]

> "Up to a few weeks ago there was one man who alone of all mathematicians might have occupied the place which I hold without misgivings as to his fitness; I mean Henri Poincaré. It was at Rome just four years ago that the first dark shadow fell on us of that illness which has now terminated so fatally. You all remember the dismay which fell on us when the word was passed from man to man 'Poincaré is ill.' We had hoped that we might again have heard from his mouth some such luminous address as that which he gave at Rome; but it was not to be, and the loss of France in his death affects the whole world."

Before remembering Poincaré, Darwin had said something which I also wish to quote:[22] "The Science of Mathematics is now so wide and is already so much specialised that it may be doubted whether there exists to-day any man fully competent to understand mathematical research in all its many diverse branches. I, at least, feel how profoundly ill-equipped I am to represent our Society as regards all that vast field of knowledge which we classify as pure mathematics. I must tell you frankly that when I gaze on some of the papers written by men in this room I feel myself much in the same position as if they were written in Sanskrit".

Perhaps these words of a man like George Darwin, a *second wrangler* in the Tripos, by no means a mathematical ignorant, might console some – or many – of us when we look now upon the titles of the present congress.

Immediately after his confession, Darwin went on to proudly add:

> "But if there is any place in the world in which so one-sided a President of the body which has the honour to bid you welcome is not wholly out of place it is perhaps Cambridge. It is true that there have been in the past at Cambridge great pure mathematicians such as Cayley and Sylvester, but we surely may claim without undue boasting that our University has played a conspicuous part in the advance of applied mathematics. Newton was a glory of all mankind, yet we Cambridge men are proud that fate ordained that he should have been Lucasian Professor here. But as regards the part played by Cambridge I refer rather to the men of the last hundred years, such as Airy, Adams, Maxwell, Stokes, Kelvin, and other lesser lights, who have marked out the lines of research in applied mathematics as studied in this University. Then too there are others such as our Chancellor, Lord Rayleigh, who are happily still with us."

[21] *Proceedings of the Fifth International Congress of Mathematicians* (*Cambridge, 22–28 August 1912*), E. W. Hobson and A. E. H. Love, eds. (Cambridge University Press, Cambridge 1913), vol. I, p. 34.

[22] Ibid., pp. 33–34.

Mathematics and politics: Strasbourg (1920), Toronto (1924), Bologna (1928)

Two years after the Cambridge Congress, the Great War, later called World War I, broke out, and the mathematical congresses suffered from that. Not only there were no meetings until 1920, but the consequences of the war affected the mathematical community for years.

The 1920 congress should have taken place in Stockholm, the site elected in Cambridge for the 1916 meeting, but politics interfered and Strasbourg, which had been annexed by the Germans after the Franco–Prussian war of 1870–1871 and reclaimed by the French at the Treaty of Versailles along with the rest of Alsace and Lorraine, took its place. It was, of course, a demonstration of political power – and revenge – by the victors of the war. Moreover, German mathematicians were not invited. Some, as Hardy, Littlewood or Mittag-Leffler objected, but to no avail. In his address for the closing ceremony, Émile Picard, who presided with Camille Jordan as Honorary President, stated:[23]

> "En ce qui regarde spécialement notre Congrès, nous n'avons jamais dissimulé que nous entendions lui donner une signification particulière, en le réunissant à Strasbourg. Aussi avons-nous été extrêmement touchés de l'empressement avec lequel nos amis étrangers ont répondu à notre appel… Des liens plus intimes ont été formés, qui resteront précieux. Nous continuerons ainsi, entre peuples amis, nos travaux scientifiques, apportant dans cette collaboration nos qualités diverses, sans qu'aucun prétende exercer une insupportable hégémonie et sans nous soucier de certaines menaces, qu'avec une impudeur qui ne nous étonne pas, on a osé proférer.
>
> Quant à certaines relations, qui ont été rompues par la tragédie de ces dernières années, nos successeurs verront si un temps suffisamment long et un repentir sincère pourront permettre de les reprendre un jour, et si ceux qui se sont exclus du concert des nations civilisées sont dignes d'y rentrer. Pour nous, trop proches des événements, nous faisons encore nôtre la belle parole prononcée pendant la guerre par le cardinal Mercier, que, pardonner à certains crimes, c'est s'en faire le complice."

Mathematicians from 27 countries attended the congress, which was held from September 22 to September 30. Not surprising, the great majority (82 per cent) of the talks were in French and just 17 per cent were given in English. Only one speaker – Rudolf Fueter, from Zurich – lectured in German. One of the American participants of the congress was Norbert Wiener, who attended as MIT's representative and presented a paper on Brownian motion. It was his first International Congress of

[23] *Comptes Rendus du Congrès International des Mathématiciens. Strasbourg, 1920*, Henry Villat, ed. (Imprimerie et Librairie Privat, Toulouse 1921), pp. xxxi–xxxiii; quoted in Angelo Guerraggio and Pietro Nastasi, *Italian Mathematics Between the Two World Wars* (Birkhäuser, Basel 2005), pp. 57–58.

Mathematicians.

Toronto 1924, followed (it should have been New York, but in April 1922 the Americans withdrew – for reasons not stated in their *Bulletin* – in favour of the Canadian city). Again, no Germans were present. The plenary lecturers were Leonard Dickson, Joseph Larmor, Niels Nörlund, Charles de la Vallée-Poussin, and Vito Volterra.

A German delegation of 67 mathematicians, headed by Hilbert, attended the next congress, Bologna 1928, ten years after the end of the war. Not all the German mathematicians were in favour of that decision. One group opposed it. Its leader was Ludwig Bieberbach, who when Hitler assumed power in 1933 propagated a *Deutsche Mathematik*; that is, a mathematics free from the "Jewish spirit," whatever that might had meant, and, of course, from mathematicians of Jewish origin. There is, however, a fact we must not forget: Italy was then Mussolini's Italy, the future ally of Hitler's Germany. As a matter of fact, when we look over the *Atti* (proceedings) of the congress, we find that the *Comitato d'onore* was presided by "S. E. Cav. Benito Mussolini, Capo del Governo". Among the other members of the committee were T. Tittoni, *Presidente del Senato*, A. Casertano, *Presidente della Camera dei Deputati*, A. Turati, *Segretario del Partito Fascista*, and P. Badoglio, *Maresciallo d'Italia, Capo di Stato Maggiore Generale*.

Constance Reid, Hilbert's biographer, described what happened during the opening ceremony. I will use her words:[24]

> "At the opening session, as the Germans came into an international meeting for the first time since the war, the delegates saw a familiar figure, more frail than they remembered, marching at their head. For a few minutes there was not a sound in the hall. Then, spontaneously, every person present rose and applauded.
>
> 'It makes me very happy,' Hilbert told them in the familiar accent, 'that after a long, hard time all the mathematicians of the world are represented here. This is as it should be and as it must be for the prosperity of our beloved science.
>
> 'Let us consider that we as mathematicians stand on the highest pinnacle of the cultivation of the exact sciences. We have no other choice than to assume this highest place, because all limits, especially national ones, are contrary to the nature of mathematics. It is a complete misunderstanding of our science to construct differences according to peoples and races, and the reasons for which this has been done are very shabby ones.
>
> 'Mathematics knows no races… For mathematics, the whole cultural world is a single country.' "

This is the sort of words we must remember, the jewels of history. They are as valid today as they were when Hilbert pronounced them, and we can very easily understand the emotion they aroused in the people that heard them.

[24] Constance Reid, *Hilbert* (Springer-Verlag, Berlin 1970), p. 188.

In the paper he read in Bologna, Hilbert considered a very important problem, the so-called *Entscheidungsproblem*, or "decision problem": to show whether there exists an algorithm for deciding if a mathematical proposition is a logical consequence of others. He had already considered it in his 1900 Paris lecture as part of problem number 2 ("the compatibility of the arithmetic axioms"). This line of research would culminate in the works of Alonzo Church, Alan Turing and Kurt Gödel.

Besides Hilbert's talk, plenary lectures were delivered also by: Luigi Amoroso ("Le equazioni differenziali della dinamica economica"), George D. Birkhoff ("Quelques éléments mathématiques de l'art"), Émile Borel ("Le Calcul des probabilités et les sciences exactes"), Guido Castelnuovo ("La geometria algebrica e la scuola italiana"), Maurice Fréchet ("L'analyse générale et les Espaces Abstraits"), Jacques Hadamard ("Le développement et le rôle scientifique du Calcul fonctionnel"), Theodore von Kármán ("Mathematische Probleme der modernen Aerodynamik"), Nikolai Lusin ("Sur les voies de la théorie des ensembles"), Roberto Marcolongo ("Leonardo da Vinci nella storia della matematica e della meccanica"), Umberto Puppini ("Le boniche in Italia"), Leonida Tonelli ("Il contributo italiano alla teoria delle funzioni di variabili reali"), Oswald Veblen ("Differential Invariants and Geometry"), Vito Volterra ("La teoria dei funzionali applicata ai fenomeni ereditari"), Hermann Weyl ("Kontinuierliche Gruppen und ihre Darstellungen durch lineare Transformationen") and William Young ("The mathematical method and its limitations").

Zurich (1932): A woman plenary lecturer

I mentioned before Emmy Noether and the problems she had because of being a woman. The International Congresses of Mathematicians treated her better than the authorities of her country; in particular the 1932 International Congress of Mathematicians, held in September in Zurich again (there will be a third time, in 1994). She delivered one of the plenary lectures, the first woman to achieve such honour in the history of the congresses.[25] On September 7, she spoke on "Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie" ("Hypercomplex systems in their relations to commutative algebra and to number theory").[26]

[25] It is interesting what D. J. Albers, G. L. Alexanderson and C. Reid (*International Mathematical Congresses. An Illustrated History, 1893–1986*, *op. cit*., p. 23) wrote concerning the presence of women at the congresses of mathematicians: "Since the World Congress held in Chicago, women mathematicians had been in attendance at all but one of the international congresses. At Zurich in 1897, however, they were listed under 'Damen,' which classification consisted otherwise of the wives and daughters of the attending mathematicians. Attendance of women mathematicians through the second Zurich congress was as follows: Chicago, 3; Zurich, 4; Paris, 6; Heidelberg, 0; Rome, 19; Cambridge, 37; Strasbourg, 6; Toronto, 25; Bologna, 69; and Zurich, 35 (total congress attendance having declined)."

[26] As a proof that tensions were not absent in the mathematical community, we have that a year later, and referring to this talk, George Birkhoff accused Noether of intentional ignorance of Anglo-American scientists. Maria Georgiadou, *Constantin Carathéodory. Mathematics and Politics in Turbulent Times* (Springer-Verlag, Berlin 2004), p. 272.

247 official delegates and 420 participants attended this congress. It was presided by Karl Rudolf Fueter, professor at the Zurich University, which, together with the Polytechnic (or Federal Institute of Technology), sponsored the meeting. After Fueter's opening speech, Constantin Carathéodory delivered the lecture "Über die analytischen Abbildungen von mehrdimensionalen Räumen" ("On analytic mappings of multidimensional spaces").

Together with Noether and Carathéodory, and among others, plenary lecturers were: James Alexander (who spoke about "Some problems in topology"), Ludwig Bieberbach ("Operationsbereiche von Funktionen"), Harald Bohr ("Fastperiodische Funktionen einer komplexen Veränderlichen"), Élie Cartan ("Les espaces riemanniens symétriques"), Gaston Julia ("Essai sur le développement de la théorie des fonctions de variables complexes"), Karl Menger ("Neuere Methoden und Probleme der Geometrie"), Marston Morse ("The calculus of variations in the large"), as well as the physicist Wolfgang Pauli, professor at Zurich, who spoke about the "Mathematische Methoden der Quantenmechanik." Also present, although no plenary lecturers, were Edmund Landau, Hermann Weyl, Richard Courant, and the splendid mathematician and unforgettable author of *A Mathematician's Apology* (1940), Godfrey Hardy. By the way, according to George Pólya, Landau claimed that he went to Zurich to play bridge with Hardy. I do not know if they played, but Landau must have been a difficult adversary: he was a very rich person, a millionaire.[27]

It was in Zurich 1932 that it was announced a bequest from the will of the Canadian John Charles Fields (1863–1932), who as a mathematician had cultivated the theory of algebraic functions and algebra. Fields died on August 8, 1932, just one month before the congress opened, but he had been working on the establishment of a prize for mathematicians. His friend, the mathematician and physicist John Lighton Synge (who had worked with Fields on the organization of the 1924 Toronto Congress) presented the proposal to the executive committee of the Zurich Congress. According to Michael Monastyrsky, the "session of the ad hoc committee that considered the question of the prize was stormy. Not all the members of the committee supported the establishment of a prize. In particular Oswald Veblen spoke against it, perhaps motivated by the thesis that the study of science is its own reward, so the researcher has no need of additional encouragement. Nevertheless, most of the committee members favoured Fields' proposal. At the plenary session of the congress, the question was finally decided in the affirmative."[28]

Oslo (1936). The first Fields medals

The next congress was held in Oslo. It can be remembered mainly for two facts. The first is that since 1933 Germany was already Hitler's Germany, and some of the

[27] George Pólya, *The Pólya Picture Album. Encounters of a Mathematician* (Birkhäuser, Basel 1987), p. 88.

[28] M. Monastyrsky, *Modern Mathematics in the Light of the Fields Medals* (AK Peters, Wellesley, Mass. 1988), p. 7.

best German mathematicians had fled their native country. Hermann Weyl, Richard Courant, Felix Bernstein, and Emmy Noether were no longer in Göttingen, nor were the young *Privatdozenten* Paul Bernays, Hans Lewy and Otto Neugebauer, who lost their *venia legendi*. Also Richard von Mises (he went first to Turkey, and afterwards to the United States) and Kurt Gödel left Germany. Edmund Landau had lost his chair, although he did not live to see the worst (he died in 1938). The cases of Felix Hausdorff and Otto Blumenthal were worse. Hausdorff stayed in Germany, but in January 1942, when he learnt that he was going to be interned in a concentration camp, he committed suicide. Blumenthal left Germany for Holland, but when this country was taken by the Germans, he was interned and died in a camp.

Italian mathematics also suffered. Between July and November 1938, Benito Mussolini introduced racial laws that led to the removal of many mathematicians from their university positions, because of their Jewish origins. This concerned, among others, Guido Ascoli, Federigo Enriques, Gino Fano, Beppo Levi and Tullio Levi-Civita. Most of them had attended the Bologna congress in 1928 presided by the *Duce*.

The second event at the Oslo Congress that deserves to be remembered is that it was there that the first Fields medals were awarded. They were given to Lars Ahlfors (then 29 years old) and to Jesse Douglas (39), for their work in complex analysis and the solution of the Plateau's problem (i.e., the theory of minimal surfaces), respectively.[29] By the way, Ahlfors only learnt that he was the winner on the eve of the ceremony and was officially notified one hour before the congress opened. Such secrecy apparently resulted in Douglas, the other winner, not coming to the congress at all.[30]

In Oslo, it was decided that the next congress would be celebrated in America, at Harvard University, Cambridge, Massachusetts, in 1940, organised by the American Mathematical Society. Still in June 1939, advertisements appeared in journals announcing its celebration, due to be from September 4th to 12th. The provisional program included sections on: I. Algebra and number theory; II. Analysis; III. Geometry; IV. Probability calculus and economy; V. Mathematical physics and applied mathematics; VI. Logic, philosophy, history and didactics.[31] It took place there, but ten years later, in 1950.

Cambridge, Mass. (1950), the Fields medal to Laurent Schwartz and the road toward mathematical purity

Indeed, the first post-war International Congress of Mathematicians was held in 1950 in the US Cambridge (Massachusetts). Many things had changed since the times of the mathematics congress associated with the Chicago 1893 World's Fair: no longer,

[29] J. Plateau was a Belgian physicist, who in 1847 performed a series of experiments with soap films that led to the creation of the theory of minimal surfaces.

[30] Michael Monastyrsky, *Modern Mathematics in the Light of the Fields Medals*, *op. cit*., p. 16.

[31] I have consulted an announcement that appeared in *La Ricerca Scientifica* (June 1939), pp. 604–605.

for instance, were American mathematicians so dependant on European mathematics as it had been then.

The proceedings of the Cambridge congress provide us with a rather good idea of the new and now enlarged space occupied by the discipline. Mathematicians whose wartime activities had enriched their disciplines – such as John von Neumann (theory of shock waves), Norbert Wiener (theory of statistics of prediction), Claude Shannon (information theory) and Abraham Wald (statistics) – were invited to present their latest results alongside speakers on pure mathematics – Oscar Zariski (algebraic varieties), André Weil (algebraic geometry), Henri Cartan (theory of analytic manifolds), Withold Hurewitz (homotopy), Claude Chevalley (algebraic groups) – whose work belonged to the tradition of the most prestigious mathematical sub-disciplines. It was, probably, the last occasion in which that happened. In the next congresses, "a clean 'take-over of power' by structural Hilbertian mathematicians", using Amy Dahan Dalmedico's words,[32] took place. The number of sessions on, for example, algebra, algebraic geometry, and algebraic topology increased from congress to congress, while the number of sessions dedicated to mathematical physics, statistics and applied branches fell regularly. Large parts of classical analysis and differential equations were going to be considered for some time as more or less exhausted of interest. The interaction between mathematics and the social sciences almost disappeared from international congresses, at least until more recent congresses. Of the 21 Fields medals awarded between 1950 and 1978, four were for number theory – Atle Selberg (1950), Klaus Roth (1958), Alan Baker (1970), Enrico Bombieri (1974) – seven for algebraic geometry, five for differential topology and algebra, while only three were for analysis (Laurent Schwartz (1950), Lars Hörmander (1962), Charles Fefferman (1978)), and there were none for probability theory. The domain associated with partial differential equations was only given the medal in 1994 (Jean-Christophe Yoccoz). I think that this trend has begun to change a bit recently, with the new development of applied mathematics helped by computers, but it is too early to judge. Perhaps significant in this context is the Fields medal awarded in 1990 to Edward Witten, a man formally educated as a physicist and interested essentially in physics problems (string theories, mainly). "In honouring him," wrote Monastyrsky, "the mathematical community was recognizing the exceptional importance of the penetration of physical ideas and methods into modern mathematics. Recent papers of medallists Jones and Drinfel'd also concern to a degree mathematical physics, or, from a different point of view, physical mathematics."[33]

The Fields medals are now well known throughout the world. This was not so, however, in the beginning, a development which, in accord with the title of this article, reflects the road from the private to the public. The case of Laurent Schwartz, the analyst who received the prize for his work in the theory of generalized functions (distributions), is a good example of this.

[32] Amy Dahan Dalmedico, "Mathematics in the twentieth century", in John Krige and Dominique Pestre, eds., *Science in the Twentieth Century* (Harwood Academic Publishers, Amsterdam 1997), pp. 651–667; p. 659.

[33] M. Monastyrsky, *Modern Mathematics in the Light of the Fields Medals*, *op. cit*., p. 105.

Schwartz received the Fields medal at the 1950 Cambridge congress (the other Fields medallist was Atle Selberg, honoured for his work in number theory, more specifically on the zeros of the Riemann zeta function and for developing an extraordinarily efficient method of estimating the distribution of primes). It is interesting to recall that Schwartz had problems to enter the United States: he was a former Trotskyst and decided leftist, and so he was denied a visa. It was thanks to the efforts of the American Mathematical Society, which pleaded his cause with president Truman, so that he got his visa some months before the meeting. Jacques Hadamard, then 85 years old, who was not a Communist but had visited the Soviet Union several times and who was one of the Honorary Presidents, was also denied a visa. His case was solved only five days before the opening of the congress.

It was the second time that the medals were awarded, since, as I said, there had been no congresses since 1936, due to World War II. In his autobiography, Schwartz remembered the events connected with his medal.[34] "During the summer of 1949, Marie-Hélène [his wife] sent me to Canada a letter that informed me that I will receive the Fields medal at the next International Congress of Mathematicians, that was to be held in the summer of 1950. I did not know at all what that was [*j'ignorais absolutement ce que c'était*]. I was to receive a gold medal, together with 500 Canadian dollars (six thousand francs), given to two mathematicians every four years, during an international congress, for my works on the distributions. The letter gave me all the necessary explications, pointing out everything would be confidential until the day of the Cambridge, Massachusetts, Congress". And Schwartz added: "The recompense was equivalent to less than two months of my monthly salary".

Thus, we have that this now very much valued medals, which today receive world attention when they are presented, were a much humble award at first. A long road has been covered to go from the private to the public.

Following the road: from Amsterdam (1954) to Madrid (2006)

After Cambridge, other congresses came, always with an increasing number of audiences. Amsterdam (1954), Edinburgh (1958), Stockholm (1962), Moscow (1966), Nice (1970), Vancouver (1974), Helsinki (1978), Warsaw (1983; the one-year delay was due to political reasons), Berkeley (1986), Kyoto (1990), Zurich (1994), Berlin (1998), Beijing (2002), and the last one, for the time being, Madrid (2006). It would be not just difficult but certainly impossible to cover all of them in a single lecture. In Edinburgh, 1958, for instance, the number of one-hour lectures by invitation of the organizing committee was already 19, with speakers such as Aleksandr Aleksandrov, Aleksei Bogolyubov, Henri Cartan, Claude Chevalley, Cornelius Lancos, Lev Pontryagyn, Stephen Kleene, René Thom, George Temple, and the physicist George Uhlenbeck.[35]

[34] Laurent Schwartz, *Un mathématicien aux prises avec le siècle* (Edtions Odile Jacob, Paris 1997), pp. 319–321.

Perhaps I should remember the Moscow 1966 Congress. More than 4 300 attended it from 54 countries, including delegations from Cuba, North Korea and North Vietnam, and more than a dozen others from Latin American, African and Asian countries. Of course, politics melt there quite clearly with mathematics, but anyhow it was an important occasion. A special stamp was issued to commemorate the Congress, the same that happened in 1978, when Finland issued another to mark the Helsinki Congress, and as has again happened in Spain 2006. And what is more public than a stamp? Another demonstration of the road that has taken the international community of mathematicians from the private to the public.

Departamento de Física Teórica, Universidad Autónoma de Madrid, Módulo C-XI,
Cantoblanco, 28049 Madrid, Spain
E-mail: josem.sanchez@uam.es

[35] See *Proceedings of the International Congress of Mathematicians, 14–21 August 1958*, J. A. Todd, ed. (Cambridge University Press, Cambridge 1960), p. xiv.

List of participants

Abad, Julio (Spain)
Abanades, Miguel (Spain)
Abardia Bochaca, Judit (Spain)
Abd Al-kader, Gamal (Egypt)
Abdellaoui, Boumediene (Spain)
Abe, Yoshihiro (Japan)
Abeles, Francine (USA)
Abellanas Oar, Manuel (Spain)
Abia Llera, Luis M. (Spain)
Abramovich, Shoshana (Israel)
Abril Bucero, Marta (Spain)
Acar, Robert (Puerto Rico)
Aceto, Lidia (Italy)
Acharyya, Sudip Kumar (India)
Ackerson, Leah (The Netherlands)
Acosta Vigil, Maria Dolores (Spain)
Adamczak, Radoslaw (Poland)
Adams, Meter (Australia)
Adán, Miguel (Spain)
Adell Pascual, José A. (Spain)
Afsharnejad, Zahra (Iran)
Ageev, Oleg N. (Australia)
Ageeva, Aleksandra O. (Australia)
Aginagalde Nafarrete, Alexander (Spain)
Agirre Basurko, Elena (Spain)
Agol, Ian (USA)
Agrawal, Manindra (India)
Agudo Agüero, Esther (Spain)
Águeda Mate, Raquel (Spain)
Aguilar Baltar, Adolfo (Spain)
Airault, Helene (France)
Akbari Feyzaabaadi, Saieed (Iran)
Akira, Ishii (Japan)
Akrami, Musa (Iran)
Alamo, Nieves (Spain)
Alana Pena, Virginia Isabel (Spain)
Alarcon Cotillas, Begoña (Spain)
Alarcón, McGrath (Spain)
Alavez Ramírez, Justino (Mexico)
Alba Valdés, Guillermo (Spain)
Alberdi Celaya, Elisabete (Spain)
Albin, Sainte Cluque (France)
Alcalde Mas, Adriana (Spain)
Alcántara-Bode, Julio (Peru)
Alcolea Banegas, Jesús (Spain)
Alcón Díaz, Rosa (Spain)
Aldana Bermúdez, Eliécer (Colombia)
Aldana Malmaceda, Carmen Enriqueta (Spain)
Ale Olawale, Samson (Nigeria)
Alegre Rueda, Pablo (Spain)
Alegría Ezquerra, Pedro (Spain)
Alejo Agudo, Alexandra (Spain)
Alestalo, Pekka (Finland)
Alexeev, Boris (USA)
Alexeev, Valery (USA)
Alexeyeva, Lyudmila (Kazakhstan)
Alfaro, Manuel (Spain)
Alfaya Sánchez, David (Spain)
Alfonseca, Maria Angeles (USA)
Alfonsín Galiñanes, Beatriz (Spain)
Alias, Luis José (Spain)
Aljadeff, Eliahu (Israel)
Allanegui Andrés, María (Spain)
Allen, Benjamin (USA)
Allison, Bruce (Canada)
Almeida Rodríguez, Ángel José (Spain)
Alon, Noga (Israel)
Alonso Gómez, Ángel José (Spain)
Alonso Morón, Manuel (Spain)
Alonso Navarro, Francisco de Borja (Spain)
Alonso Revenga, Juana María (Spain)
Alonso Sastre, Ana Isabel (Spain)
Alonso Tarrío, Leovigildo (Spain)
Alonso, Alberto (Spain)
Alonso, Javier (Spain)
Alonso, Mª Emilia (Spain)
Alonso-Mallo, Isaías (Spain)
Alpay, Safak (Turkey)
Al-Rashed, Maryam (United Kingdom)
Alshin, Alexander (Russian Federation)
Alshina, Elena (Russian Federation)
Alsina, Montserrat (Spain)
Alvarado, Mayra T. (Panama)
Álvarez Cónsul, Luis (Spain)
Álvarez Flandez, Bárbara (Spain)
Álvarez García, Miguel (Spain)
Álvarez Morán, Sara (Spain)
Álvarez Sánchez, Amelia (Spain)

Álvarez Vázquez, Lino J. (Spain)
Álvarez-Nodarse, Renato (Spain)
Álvarez-Samaniego, Borys (France)
Alves, Manuel (Mozambique)
Amann, Manuel (Germany)
Amaral Abreu, Teresa (Portugal)
Amat Plata, Sergio (Spain)
Ambat, Vijayakumar (India)
Amigo, Jose Maria (Spain)
Amir, Dan (Israel)
Amiraliyev, Gabil (Turkey)
Amirdjanova, Anna (USA)
Amornwichet, Saitong (Thailand)
Amoros Canet, Cristina (Spain)
Amoros Torrent, Jaume (Spain)
Amster, Pablo (Argentina)
Anantharaman, Claire (France)
Anatole, Joffe (Canada)
Anderegg, Martin (Switzerland)
Andersen, Lars D. (Denmark)
Andrada, Adrián (Argentina)
Andradas, Carlos (Spain)
Andre Alves Simoes, María Manuela (Portugal)
Andreev, Pavel (Russian Federation)
Andrié, Manfred (Germany)
Aneiros Vivas, Eva (Spain)
Anguiano Moreno, Maria (Spain)
Angulo Ardoy, Pablo (USA)
Angulo Torga, Oscar (Spain)
Anichini, Giuseppe (Italy)
Anisca, Razvan (Canada)
Annadeva Sagayamani, Joseph Kennedy (India)
Anquela Vicente, José Ángel (Spain)
Antezana, Jorge (Argentina)
Antolín Ontaneda, Celia (Spain)
Antolín Pichel, Yago (Spain)
Antón Lagares, Mª Ángeles (Spain)
Antón Marazuela, Cristina (Spain)
Antón Sancho, Álvaro (Spain)
Antonakoudis, Stergios (United Kingdom)
Antonio Goncalves, Rosivaldo (Spain)
Aparicio Arroyo, Marta (Spain)
Appell, Jurgen (Germany)
Applebaum, Mark (Israel)
Apraiz Iza, Jone (Spain)
Ara Bertran, Pere (Spain)
Arabia Arabia, Alberto (France)
Araki, Huzihiro (Japan)
Aranda García, Ana María (Spain)
Aranda Ortega, Ernesto (Spain)
Aranda-Godlewski, Eduardo (United Kingdom)
Arandiga Llaudes, Francesc (Spain)
Arango, Jaime (Colombia)
Araujo Gómez, Jesús (Spain)
Araujo, Carolina (Brazil)
Arbarello, Enrico (Italy)
Arbieto, Alexander (Brazil)
Arboleda Castilla, Jaime (Spain)
Arbolí López, Servando Miguel (Spain)
Arcaya Garranchan, Ignacia (Venezuela)
Ardanza-Trevijano, Sergio (Spain)
Aretakis, Stefanos (Greece)
Arévalo Escudero, inmaculada (Spain)
Arias de Reyna, Juan (Spain)
Arias de Reyna, Sara (Spain)
Arias Marco, Teresa (Spain)
Arias Mosquera, Daniel (Spain)
Arias, Juan Pablo (Spain)
Arigita, Rodrigo (Spain)
Arkhipov, Victor (Russian Federation)
Armas Sanabria, Lorena (Mexico)
Armero Ibáñez, Emilia Belén (Spain)
Armesto Álvarez, José Antonio (United Kingdom)
Arnaiz Tovar, Gonzalo (Spain)
Arnanz Monreal, Santiago (Spain)
Arnold, Douglas A. (USA)
Aroca, Fuensanta (Mexico)
Aroca, José M. (Spain)
Arrabal, Manuel (Spain)
Arratia Quesada, Argimiro (Spain)
Arredondo, Juan (Mexico)
Arrieta, Jose M. (Spain)
Arroyo González, María Encina (Spain)
Artal Bartolo, Enrique M (Spain)
Artamonov, Dmitry (Russian Federation)
Artamonov, Nikita (Russian Federation)
Arteaga Clemente, Cristian (Spain)
Arteaga Cristino, Maria (Spain)
Artemov, Anatoli (Russian Federation)
Artigue, Michèle (France)
Arvanitoyeorgos, Andreas (Greece)
Arvesú Carballo, Jorge (Spain)
Aryampillymana Vishnu, Jayanthan (India)
Asada, Akira (Japan)

Asadollahi Dehaghi, Javad (Iran)
Asaoka, Masayuki (France)
Ash, J Marshall (USA)
Ashino, Ryuichi (Japan)
Ashiq, Muhammad (Pakistan)
Asiain, Maria José (Spain)
Askari Hemmat, Ataollah (Iran)
Aslaksen, Helmer (Singapore)
Assaf, Sami (USA)
Assal, Miloud (Tunisia)
Asumendi Esteban, Francisco Javier (Spain)
Atserias, Albert (Spain)
Atxitia Macizo, Unai (Spain)
Auroux, Denis (USA)
Ausejo, Elena (Spain)
Avdispahic, Muharem
(Bosnia & Herzegovina)
Avramidi, Ivan (USA)
Avramidou, Parthena (USA)
Ayse, Kara (Turkey)
Azarpanah, Fariborz (Iran)

Baader, Sebastián (Switzerland)
Bäärnhielm, Henrik (United Kingdom)
Babenko, Vladyslav (Ukraine)
Babson, Eric (USA)
Bachiller Basols, José Antonio (Spain)
Badenes Ayestarán, Emilia (Spain)
Badenes Vericat, Núria (Spain)
Badillo, Edelmira (Spain)
Baeza Alba, Miguel Ángel (Spain)
Baeza Manzanares, Antonio (Spain)
Bagayogo, Bass (Canada)
Bagchi, Somesh Chandra (India)
Bagdasaryan, Armen (Russian Federation)
Bailey Mathae, Katherine (USA)
Bainbridge, Mathew (USA)
Bak, Anthony (Germany)
Bakalov, Bojko (USA)
Baker, Matthew (USA)
Baker, Roger (USA)
Bakshi, Gurmeet Kaur (India)
Bakuradze, Malkhaz (Georgia)
Balakrishnan, Ramakrishnan (India)
Baldoni, Maria Welleda (Italy)
Ball, John (United Kingdom)
Balodis, Pedro (Spain)
Banasiak, Jacek (South Africa)
Banchoff, Thomas (USA)
Bandini, Andrea (Italy)
Banulescu, Martha (Romania)
Baños Abascal, Abelardo (Spain)
Bao, Ying (P.R. China)
Baouendi, Salah (USA)
Baran, Michal (Poland)
Barbazo, Eric (France)
Barberis, Laura (Argentina)
Barceló, Bartolomé (Spain)
Barcenilla Torres, María (Spain)
Bardina Simorra, Xavier (Spain)
Barmeier, Till (Germany)
Barón, Miguel Ángel (Spain)
Barquero Salavert, Pedro B. (United Kingdom)
Barrallo, Javier (Spain)
Barreiro-Pereira, Fernando (Spain)
Barrett, David (USA)
Barriento Cervantes, Rolando (Spain)
Barrio, Ismael (Spain)
Barthe, Franck (France)
Bartoll Arnau, Salud (Spain)
Bartoszynski, Tomek (USA)
Barvinok, Alexander (USA)
Basilla, Julius Magalona (Phillippines)
Bass, Hyman (USA)
Bastero, Jesús (Spain)
Bastos, Amélia (Portugal)
Batalla Mateos, Manuel (Spain)
Batat, Wafa (Algeria)
Bayer, Pilar (Spain)
Bazaikin, Yaroslav (Russian Federation)
Becker, Jochen (Germany)
Behforooz, Hossein (USA)
Behrends, Ehrhard (Germany)
Behrstock, Jason (USA)
Belda García, Ana María (Spain)
Belenkiy, Ari (Israel)
Belkhirat, Abdelhadi (Algeria)
Bellaïche, André (France)
Bellaïche, Catherine (France)
Bellido Guerrero, Jose Carlos (Spain)
Bellmunt Giralt, Andratx (Spain)
Bello Bustos, Francisca (Spain)
Bellogin Kouki, Alejandro (Spain)
Belmonte Beitia, Juan (Spain)
Belousov, Evgeny (Russian Federation)
Beltrán Álvarez, Carlos (Spain)
Beltrán Felip, Antonio (Spain)
Beltrán, Johel (Peru)

Ben Amara, Jamel (Tunisia)
Ben Taher, Rajae (Morocco)
Benanti, Francesca (Italy)
Benbourenane, Djamal (United Arab Emirates)
Bendito, Enrique (Spain)
Benítez Lozano, Miguel Ángel (Spain)
Benítez Suárez, Rafael (Spain)
Benito Clavijo, Pilar (Spain)
Benito Peral, Alberto (Spain)
Benito Prieto, Roberto (Spain)
Benito Sualdea, Angélica (Spain)
Berciano-Alcaraz, Ainoa (Spain)
Berezina, Miryam (Israel)
Berg, Christian (Denmark)
Bergelson, Vitaly (USA)
Bergqvist, Göran (Sweden)
Berkani, Mohammed (Morocco)
Bermejillo Ibañez, Francisco (Spain)
Bermejo Abati, Iago (Spain)
Bernatska, Julia (Ukraine)
Bernues Pardo, Julio (Spain)
Berradre Moreno, Txomin (Spain)
Bes, Juan (USA)
Besalú, Mireia (Spain)
Beziau, Jean-Yves (Switzerland)
Bezrukavnikov, Roman V. (USA)
Bhandari, Ashwani (India)
Bhargava, Banjul (USA)
Bhat, B V Rajarama (India)
Bhatia, Rajendra (India)
Bhatt, Abhay (India)
Bhatta, Chetraj (Nepal)
Bhattacharya, Tirthankar (India)
Bhattacharyya, Rabindra Kumar (India)
Bianchini, Stefano (Italy)
Biegler-Koenig, Friedrich (Germany)
Bigatti, Anna Maria (Italy)
Bijan-Zadeh, Mohammad (Iran)
Birgelis, Karlis (Latvia)
Bismut, Jean-Michel (France)
Blackwood, Carol-Ann (USA)
Blanco Cejalvo, Luis (Spain)
Blanco Martín, Mª Francisca (Spain)
Blanco Muñoz, Guillermo (Spain)
Blanco, Rocío (Spain)
Blasco Torrejón, Mª Mercedes (Spain)
Blasco, Fernando (Spain)
Blumen, Sacha (Australia)
Bochi, Jairo (Brazil)
Bocklandt, Raf (Belgium)
Bodnarescu, M.V. (Germany)
Bogart, Tristram (USA)
Bogatov, Egor (Russian Federation)
Bogatyrev, Andrei (Russian Federation)
Bohlender, Gerd (Germany)
Bolanos, Gilda (Mexico)
Boldrini, José (Brazil)
Bollobas, Bela (USA)
Bolos Lacave, Vicente J. (Spain)
Bolt, Michael (USA)
Bombal, Fernando (Spain)
Bonforte, Matteo (France)
Bongiorno, Benedetto (Italy)
Bongiorno, Donatella (Italy)
Bonk, Mario (USA)
Booss-Bavnbek, Bernhelm (Denmark)
Borbely, Albert (Kuwait)
Borcea, Julius (Sweden)
Borges Hernández, Cruz Enrique (Spain)
Borges Quintana, Mijail (Cuba)
Borgs, Christian (USA)
Borkar, Vivek (India)
Borrelli, Giuseppe (Brazil)
Bosch Camós, Anna (Spain)
Bosch, José (Spain)
Bose, Arup (India)
Bosnjalovska, Jelena (Spain)
Bost, Jean-Benoît (France)
Bottacin, Francesco (Italy)
Böttcher, Roger (Germany)
Boukricha, Abderrahman (Tunisia)
Boumazgour, Mohamed (Morocco)
Bourchtein, Andrei (Brazil)
Bourchtein, Ludmila (Brazil)
Bourguignon, Jean Pierre (France)
Bousquet-Melou, Mireille (France)
Bouzahir, Hassane (Morocco)
Bovier, Anton (Germany)
Boxall, John (France)
Boya, Luis J. (Spain)
Boyallian, Carina (Argentina)
Boyd, Stephen (USA)
Boza, Santiago (Spain)
Bozicevic, Mladen (Croatia)
Bradley, David (USA)
Braga Barros, Carlos (Brazil)
Bragdi, Mabrouk (Algeria)
Brändle, Cristina (Spain)

Brauer, Uwe (Spain)
Braverman, A. (USA)
Bravo de La Parra, Rafael (Spain)
Bravo Serrano, Maria (Spain)
Braz e Silva, Pablo (Brazil)
Brendle, Simon A. (USA)
Brendle, Tara (USA)
Breuer, Florian (South Africa)
Brezzi, Franco (Italy)
Bridgeland, Tom (United Kingdom)
Bridson, Martin (United Kingdom)
Brinzanescu, Vasile (Romania)
Brinzei, Nicoleta (Romania)
Briseño Aguirre, Luis (Mexico)
Broaddus, Nathan (USA)
Brochero Martínez, Fabio Enrique (Brazil)
Broto, Carles (Spain)
Broughan, Kevin (New Zealand)
Brox López, José Ramón (Spain)
Bruna Floris, Joaquim (Spain)
Brunelli, Sara (Italy)
Bruscher, Clemens (Spain)
Bryant, Robert (USA)
Bshouty, Daoud (Israel)
Buchanan, Thomas (Germany)
Budur, Nero (USA)
Bueno Orovio, Alfonso (Spain)
Bujalance Fernández-Quero, Laura (Spain)
Bujalance García, Emilio (Spain)
Bujalance Rodríguez, Carla (Spain)
Bujalance, José Antonio (Spain)
Buneci, Madalina (Romania)
Burdick, Bruce (USA)
Burguet Castell, Jordi (Spain)
Burillo Puig, José (Spain)
Bursztyn, Henrique (Brazil)
Busquier Sáez, Sonia (Spain)
Bustillo Saiz, Paula (Spain)
Bustinduy Candelas, Álvaro (Spain)
Butkovic, Davor (Croatia)
Butler, Michael C.R. (United Kingdom)
Button, Jack (United Kingdom)

Cabada, Alberto (Spain)
Cabanillas Zannini, Víctor Rafael (Peru)
Cabaña, Enrique (Uruguay)
Cabañas Polo, Iván (Spain)
Cabezas Rivas, Esther (Spain)
Cabrerizo, José Luis (Spain)
Cachafeiro López, Alicia (Spain)
Cadarso Rebolledo, Andrea (Spain)
Caflish, Russel (USA)
Cagigas Lago, Manuel (Spain)
Cagliari, Francesca (Italy)
Cagliero, Leandro (Argentina)
Caicedo, Xavier (Colombia)
Caine, Arlo (USA)
Calahorrano, Marco (Ecuador)
Calderer, Carme (USA)
Calderón Moreno, Francisco Javier (Spain)
Calderón, Catalina (Spain)
Calero, Mayra (Nicaragua)
Calle, María (USA)
Callejo Ortega, Iratxe (Spain)
Calsamiglia Mendlewicz, Gabriel (Brazil)
Calvaruso, Giovanni (Italy)
Calvete, Herminia I. (Spain)
Calvo García-maroto, Elena (Spain)
Calvo García-Maroto, Marta (Spain)
Calvo Jurado, Carmen (Spain)
Calvo López, Clara (Spain)
Calvo Resino, Laura (Spain)
Camacho Santana, Luisa M. (Spain)
Cámara López, Alberto (Spain)
Cámara Santamaría, Mª Cruz (Spain)
Camarero Coterillo, Cristóbal (Spain)
Camarero Coterillo, Rodrigo (Spain)
Campillo, Antonio (Spain)
Campión Arrastia, Maria Jesús (Spain)
Campo Paredes, Laura (Spain)
Canales Chacón, Mónica del Pilar (Chile)
Canary, Richard (USA)
Candeal Haro, Juan C. (Spain)
Candel, Alberto (USA)
Candela Pokorna, Pablo (United Kingdom)
Candela Pomares, Vicente (Spain)
Candes, Emmanuel (USA)
Caniego Monreal, Javier (Spain)
Canogar, Roberto (Spain)
Cantero, Federico (Spain)
Cantero Piñeiro, Mario (Spain)
Cantón Pire, Alicia (Spain)
Cañadas-Pinedo, María A. (Spain)
Cañas Escamilla, Juan (Spain)
Cañete Martín, Antonio Jesús (Spain)
Cañete Molero, Elisa (Spain)
Cañizo Rincón, José Alfredo (Spain)
Cao Rial, María Teresa (Spain)

Cao, Huai-Dong (USA)
Çapar, Uluð (Turkey)
Caprino, Silvia (Italy)
Caraus, Iurie (Moldova)
Carbery, Anthony (United Kingdom)
Carcaud, Pierre (France)
Cardoso, Fernando (Brazil)
Cariñena Marzo, José F. (Spain)
Carlavilla, José Luis (Spain)
Carleson, Lennart (Sweden)
Carlson, James (USA)
Carmona Ruber, Jorge (Spain)
Carmona, Ángeles (Spain)
Carnahan, Scott (USA)
Carnicer Arribas, Manuel Mariano (Spain)
Carnovale, Giovanna (Italy)
Carrasco, Pilar (Spain)
Carrero Torres, Noé (Spain)
Carrero Yubero, Eduardo (Spain)
Carriazo, Alfonso (Spain)
Carriegos Vieira, Miguel (Spain)
Carrillo de Albornoz Torres, Agustín (Spain)
Carrillo de la Plata, José Antonio (Spain)
Carrillo Menéndez, Santiago (Spain)
Carrio Gaspar, Pau (Spain)
Carro, María J. (Spain)
Casacuberta, Carles (Spain)
Casado Barrio, Mª Jesús (Spain)
Casal Piga, Alfonso Carlos (Spain)
Casal Segade, Ana María (Spain)
Casaravilla Gil, Julia Ana (Spain)
Casas Mirás, José Manuel (Spain)
Casas Rentería, Eduardo (Spain)
Cascudo Pueyo, Ignacio (Spain)
Case, Bettye (USA)
Caselles, Vicent (Spain)
Cassou-Nogues, Philippe (France)
Cassou-Nogues, Pierrette (France)
Cassy, Bhangy (Mozambique)
Castejón Solanas, Ángeles (Spain)
Casteleiro Villalba, José Manuel (Spain)
Castellá, Francesc (Spain)
Castellet, Manuel (Spain)
Castilla de Nova, María (Spain)
Castillo Aranguren, Francisco (Mexico)
Castizo Mantas, María (Spain)
Castrillón López, Marco (Spain)
Castro Esteban, David (Spain)
Castro Jiménez, Francisco-Jesús (Spain)
Castro Smirnova, Mirta María (Spain)
Castro, Ildefonso (Spain)
Castro, Sofia (Portugal)
Catinas, Emil (Romania)
Catinas, Teodora (Romania)
Cattaneo, Alberto S. (Switzerland)
Cavicchioli, Alberto (Italy)
Cayford, Afton (Canada)
Cea, Miguel (Spain)
Ceballos Cañón, Johan Armando (Spain)
Ceballos González, Manuel (Spain)
Cebrián de Barrio, Elena (Spain)
Cembellín Santos, Mari Paz (Spain)
Cerda Tena, Emilio (Spain)
Cerf, Rafael (France)
Cernea, Aurelian (Romania)
Cerone, Pietro (Australia)
Chacon, Pablo Miguel (Spain)
Chai, Ching-Li (USA)
Chaichi, Mohamad (Iran)
Chaisi, Mosa (Lesotho)
Chakraborty, Partha Sarathi (India)
Chaleyat-Maurel, Mireille (France)
Chalishajar, Dimplekumar (India)
Chan, Tony (USA)
Chang, Chih-Chung (Taiwan)
Chang, Gerard Jennhwa (Taiwan)
Chapron, Michel (France)
Charles Kearn, Gene (United Kingdom)
Charney, Ruth (USA)
Charro Caballero, Fernando (Spain)
Chasco, María Jesús (Spain)
Chatterji, Srishti D. (Switzerland)
Chaudhary, Sanjay (India)
Chaudhry, Muhammad (Saudi Arabia)
Chayes, Jennifer (USA)
Cheban, David (Moldova)
Checa Camacho, Isabel (Spain)
Chen, Chin-Yun (Taiwan)
Chen, Linda (USA)
Chen, Louis (Singapore)
Chen, Shaohua (Canada)
Chen, Zhen-Qing (USA)
Chen, Zhiming (P.R. China)
Cheng, Jian (P.R. China)
Cheng, Jih-Hsin (Taiwan)
Cheng, Shiu-Yuen (P.R. China)
Cheng, Wei (P.R. China)
Chern, Tien-Yu (Taiwan)

Chertock, Alina (USA)
Chien, Mao-Ting (Taiwan)
Chillingworth, David (United Kingdom)
Cho, Jinseok (South Corea)
Cho, Yong Seung (South Corea)
Choda, Marie (Japan)
Choe, Boo Rim (South Corea)
Choi, Q-Heung (South Corea)
Choi, Seul Hee (South Corea)
Choi, Youn-Seo (South Corea)
Chong, Chi Tat (Singapore)
Choquet-Bruhat, Yvonne (France)
Chorwadwala, Anisa Mohmad Husen (India)
Chowdhury Chandra, Khanindra (India)
Chraibi, Lotfi (Morocco)
Chtioui, Hichem (Tunisia)
Chu, Eric (Australia)
Chu, Hahng-Yun (South Corea)
Chuang, Zheng (Spain)
Chung, Eric (USA)
Ciaurri, Oscar (Spain)
Cibils, Claude (France)
Cifuentes, Patricio (Spain)
Cilia, Raffaella (Italy)
Cilleruelo Mateo, Javier (Spain)
Cipriano, Marcelo José (Argentina)
Cirre, Javier (Spain)
Cisneros-Molina, José Luis (Mexico)
Clancey, Kevin (USA)
Clarke, Nancy (Canada)
Clemens, Herbert (USA)
Clement, Rosario (Spain)
Cobo Pablos, Helena (Spain)
Cobos, Fernando (Spain)
Coelho, Flavio (Brazil)
Cogolludo Agustín, José Ignacio (Spain)
Cohen, Albert (France)
Cohn, Henry (USA)
Coifman, Ronald (USA)
Collantes, Jaime (Peru)
Colorado Heras, Eduardo (Spain)
Comellas, Jordi (Spain)
Comman, Henri (Chile)
Conde Calero, Juan Manuel (Spain)
Conejo Pérez, Inmaculada (Spain)
Contreras, Gonzalo (Mexico)
Contreras, Lucia (Spain)
Coonce, Harry B. (USA)
Cooper, Peter (United Kingdom)
Copadó Sánchez, Antonio (Spain)
Copitsas, George (United Kingdom)
Corbacho Rosas, Eusebio (Spain)
Corberán, Ana (Spain)
Córcoles Briongos, César (Spain)
Cordero Fuertes, Juan Antonio (Spain)
Cordero Zamorano, Pablo Martín (Spain)
Cordero-Epperson, Minerva (USA)
Córdoba Hita, Beatriz (Spain)
Córdoba, Diego (Spain)
Corentin, Boissy (France)
Cornea, Octavian (Canada)
Corona, Carlos M. (Spain)
Coronado Barrientos, Edoardo Emilio (Spain)
Corral Pérez, Nuria (Spain)
Corral Rojas, Jesús Alberto (Spain)
Corrales Rodrigañez, Capi (Spain)
Corrales, Antón (Spain)
Corry, Leo (Israel)
Cortadellas Izquierdo, Óscar Alfonso (Spain)
Cortés Gracia, Teresa (Spain)
Cortés Rodríguez, Patricia (Spain)
Cortés, Jorge (USA)
Cortés, Vanesa (Spain)
Costa González, Antonio F. (Spain)
Costoya, Cristina (Spain)
Cowen, Carl (USA)
Cowling, Michael (Australia)
Cramer, Ronald (The Netherlands)
Crapo, Henry (France)
Crawley-Boevey, William (United Kingdom)
Crepi Alemany, Martín (Spain)
Crespo García, Rafael (Spain)
Crespo Rodríguez, Raquel (Spain)
Crespo Vicente, Teresa (Spain)
Criado Cornejo, Alberto (Spain)
Criado, Carlos (Spain)
Crisan, Dan (United Kingdom)
Cristóbal Centenera, Samuel (Spain)
Cristóbal Rodríguez, María Elena (Spain)
Crivei, Septimiu (Romania)
Crmaric, Tonci (USA)
Crowdy, Darren (United Kingdom)
Crowley, Katherine (USA)
Cruz Mercado, Lorena (Spain)
Cuadra Díaz, Juan (Spain)
Cucuzza, Roberta Anna I. (Singapore)
Cuello, Eva (Spain)
Cuenca Escudero, Josefa (Spain)

Cuenca Mira, José Antonio (Spain)
Cuesta Yustas, Gema (Spain)
Cuevas, Antonio (Spain)
Cujó Arenas, Jorge (Spain)
Curbera, Guillermo (Spain)
Cvetkovic, Dragos (Serbia & Montenegro)
Cwiszewski, Aleksander (Poland)
Czernous, Wojciech (Poland)

Daboussi, Hedi (France)
Dafni, Galia (Canada)
Dai, Xianzhe (USA)
Daigle, Daniel (Canada)
Dalang, Robert (Switzerland)
Dale, Knut Theodor (Norway)
Damle, Vaishali (USA)
Dani, Shrikrishna Gopalrao (India)
Danielyan, Arthur (USA)
Darkhovsky, Boris (Russian Federation)
Darmon, Henri (Canada)
Darwish, Mohamed (Egypt)
Das, Manav (USA)
Das, Pratulananda (India)
Dasgupta, Samit (USA)
Datta, Mahuya (India)
Daverman, Robert (USA)
Dávila Díaz, Marta (Spain)
Dawson, Donald (Canada)
Dcruz, Clare (India)
de Blasi, Francesco Saverio (Italy)
de Francisco Iribarren, Araceli (Spain)
de Frutos Escobar, Noemí (Spain)
de Frutos Palomino, José María (Spain)
de Iscar, Jorge (Spain)
de Ita Luna, Guillermo (Mexico)
de Knock, Bram (Belgium)
de la Barrera Mayoral, Daniel (Spain)
de la Cal, Jesús (Spain)
de la Calle Ysern, Bernardo (Spain)
de la Fuente Pérez, José Abraham (Spain)
de la Haz Gan, María Cristina (Spain)
de la Herrán de Blas, Carla (Spain)
de la Higuera Rodríguez, Beatriz (Spain)
de la Hoz Méndez, Francisco (Spain)
de la Iglesia, Eduardo (Spain)
de la Llave, Rafael (USA)
de la Rubia Hernández, Valentín (Spain)
de la Torre, Alberto (Spain)
de Lange, Jan (The Netherlands)
de León, Manuel (Spain)
de Melo, Welington (Brazil)
de Mier Torrecila, Mónica (Spain)
de Mier, Anna (Czech Republic)
de Nápoli, Pablo Luis (Argentina)
de Natividade, María (Spain)
de Pablo Martínez, Arturo (Spain)
de Paz Reina, Carmen María (Spain)
de Prada, Paz (Spain)
de Retes, Fernando (Spain)
de Shalit, Ehud (Israel)
de Vicente Majúa, Julio Iñigo (Spain)
De, Pijus Kanti (India)
Deaño Cabrera, Alfredo (Spain)
Debnath, Lokenath (USA)
Debnath, Ujjal (India)
Deift, Percy (USA)
del Bosque Muñoz, Jorge (Spain)
del Magno, Gianluigi (Italy)
del Riego, Lilia (Mexico)
del Río Mateos, Ángel (Spain)
Delgado de la Mata, Félix (Spain)
Delgado Garrido, Olvido (Spain)
Delgado Pineda, Miguel (Spain)
Delgado Tellez de Cepeda, Marina (Spain)
Deligero, Eveyth (Phillippines)
Dell'Antonio, Gianfausto (Italy)
Delso Foronda, Carlos (Spain)
Demailly, Jean-Pierre (France)
Dembo, Amir (USA)
Demchenko, Oleg (Russian Federation)
Dencker, Nils (Sweden)
Deo, Satya (India)
Derrida, Bernard (France)
Desquith, Etienne (Ivory Coast)
Dessai, Anand (Germany)
DeVore, Ronald (USA)
Devoto, Jorge (Argentina)
Dexeus, Josefina (Spain)
Deyoung, Gregg (Egypt)
Dhakne, Machindra (India)
Diacu, Florin (Canada)
Díaz y Díaz, Francisco (France)
Díaz, Jesús Ildefonso (Spain)
Díaz, Pilar (Spain)
Díaz-Cano Ocaña, Antonio (Spain)
Díaz-Ramos, José Carlos (Spain)
Díez Machío, Héctor (Spain)
Díez Serrano, Carolina (Spain)

Díez-López, Nerea (Spain)
Djokovic, Dragomir (Canada)
Djoric, Mirjana (Serbia & Montenegro)
do Carmo Boratto, Murilo (Spain)
Dobado, Antonio (Spain)
Docampo Álvarez, Roi (USA)
Dodig, Marija (Portugal)
Dodounekova, Rossitza (Sweden)
Dolgopyat, Dmitry (USA)
Domingo-Juan, Mª Carmen (Spain)
Domínguez Benavides, María del Carmen (Spain)
Domínguez de la Iglesia, Manuel (Spain)
Domínguez Gómez, Jesús (Spain)
Donat Beneito, Rosa (Spain)
Donatelli, Marco (Italy)
Dong, Hongjie (USA)
Donnelly, Peter (United Kingdom)
Dony, Julia (Belgium)
Doñamayor Alonso, Silvia (Spain)
Doob, Michael (Canada)
Dorfmeister, Josef Friedrich (Germany)
Dorn, Britta (Germany)
Dotti, Isabel (Argentina)
Doty, Stephen (USA)
Dowla, Arif (Bangladesh)
Downey, Rod (New Zealand)
Draisma, Jan (The Netherlands)
Draper Fontanals, Cristina (Spain)
Driver, Kathy (South Africa)
Drubi Vega, Fátima (Spain)
Druetta, María Josefina (Argentina)
du Sautoy, Marcus (United Kingdom)
Du, Bau-Sen (Taiwan)
Dumitrache, Alexandru (Romania)
Dumortier, Freddy (Belgium)
Dunne, Edward (USA)
Duoandikoetxea, Javier (Spain)
Durán, Antonio J. (Spain)
Durán, Ricardo (Argentina)
Durand Cartagena, Estibalitz (Spain)
Durany, José (Spain)
Durfee, Alan (USA)
Dvornicich, Roberto (Italy)
Dwek, Albert (Israel)
Dwivedi, Shivanand (Germany)
Dyn, Nira (Israel)
Dzhuraev, Abubakir (Kyrgyzstan)
Ebrahimi, Touradj (Switzerland)
Echarri Hernández, José (Spain)
Echevarría Líbano, Rosa (Spain)
Eden, Alp (Turkey)
Edwards, Robert (USA)
Efremov, Roman (Spain)
Ein, Lawrence (USA)
Eixarch Ferrer, Ramón (Spain)
Eklof, Paul (USA)
El Baghdadi, Said (Morocco)
El Bekkaye, Mermri (Morocco)
El Khadiri, Abdelhafed (Morocco)
El Yacoubi, Nouzha (Morocco)
Elbaz-Vincent, Philippe (France)
El-Doma, Mohamed (Sudan)
Elduque, Alberto (Spain)
Elekes, Márton (Hungary)
El-Ghamry, Ramadán (Palestine)
El-Guindy, Ahmad (USA)
Eliashberg, Yakov (USA)
Elizalde, Emilio (Spain)
Elizalde, Sergi (USA)
Ellis Raggio, María Eugenia (Spain)
Eloranta, Kari (Finland)
El-Sabaa, Fawzy (Egypt)
Eltekov, Vitaly (Russian Federation)
Elworthy, Kenneth (United Kingdom)
Emanouilov, Oleg Yu. (USA)
Emerson, Annette W. (USA)
Emmer, Michele (Italy)
Encinas Bachiller, Andrés Marcos (Spain)
Encinas Carrión, Santiago (Spain)
Enciso, Alberto (Spain)
Engoulatov, Alexandre (France)
Engquist, Björn (USA)
Enock, Michel (France)
Enomoto, Kazuyuki (Japan)
Eppelbaum, Lev (Israel)
Epperson, James (USA)
Erbay, Husnu Ata (Turkey)
Erbay, Saadet (Turkey)
Erez, Boas (France)
Erusalimskiy, Iakov (Russian Federation)
Ervedoza, Sylvain (France)
Escauriaza Zubiria, Luis (Spain)
Escribano Iglesias, Carmen (Spain)
Escribano Martínez, Jesús (Spain)
Escribano Ródenas, Mª Carmen (Spain)
Escudero Liébana, Carlos (United Kingdom)

Español González, Luis (Spain)
Espínola García, Rafael (Spain)
Esslamzadeh, Gholam Hossein (Iran)
Esteban Romero, Ramón (Spain)
Estela Carbonell, María Rosa (Spain)
Estelle Burgess, Kim (Australia)
Estévez Domínguez, Carmen (Spain)
Estevez, José Luis (Spain)
Estrada López, Beatriz (Spain)
Etayo Gordejuela, Fernando (Spain)
Eudave Muñoz, Mario (Mexico)
Ewing, John (USA)
Exner, Pavel (Czech Republic)
Extremiana Aldana, José Ignacio (Spain)

Fabre, Bruno (France)
Faddeev, Lyudvig (Russian Federation)
Fakharzadeh Jahromi, Alireza (Iran)
Falcón Ganfornina, Raúl Manuel (Spain)
Faminskii, Andrei (Russia Federation)
Fan, Jianqing (USA)
Faraco, Daniel (Spain)
Farahi, Mohammad Hadi (Iran)
Farber, Michael (United Kingdom)
Farkas, Balint (Germany)
Fathi, Albert (France)
Fattorusso, Luisa (Italy)
Fedeli, Alessandro (Italy)
Fefferman, Charles (USA)
Felder, Giovanni (Switzerland)
Feldman, Konstantin (United Kingdom)
Felikson, Anna (Russian Federation)
Felipe Román, María José (Spain)
Felipe, Raúl (Cuba)
Femic, Bojana (Spain)
Fernandes, Rui Loja (Portugal)
Fernández Álvarez, Luis (United Kingdom)
Fernández Corroto, Alberto (Spain)
Fernández de Bobadilla de Olazabal, Javier (Spain)
Fernández de Córdoba Castella, Pedro (Spain)
Fernández de los Ríos, Lia (Spain)
Fernández Fernández, Francisco Javier (Spain)
Fernández Fernández, María Cruz (Spain)
Fernández Fernández-Arroyo, Fidel José (Spain)
Fernández Gallardo, Pablo (Spain)
Fernández García-Hierro, Manuel (Spain)
Fernández Grado, Inmaculada (Spain)
Fernández Hernández, José Luis (Spain)
Fernández Herrera, Natalia (Spain)
Fernández Jiménez, Antonio José (Spain)
Fernández Jiménez, Teresa (Spain)
Fernández Magadán, María José (Puerto Rico)
Fernández Mariño, Beltrán (Spain)
Fernández Martínez, Pedro (Spain)
Fernández Mateos, Víctor (Spain)
Fernández Muñoz de Morales, Alberto (Spain)
Fernández Parga, Elena (Spain)
Fernández Pérez, José Luis (Spain)
Fernández Polo, Francisco José (Spain)
Fernández Raya, Edurne (Spain)
Fernández Rúa, Ignacio (Spain)
Fernández Sánchez, Casimiro (Mexico)
Fernández Viz, Antonio (Spain)
Fernández, Antonio (Spain)
Fernández, Carlos (Spain)
Fernández, Luis Alberto (Spain)
Fernández, Mercedes (Spain)
Fernández-Blanco, Severino (Spain)
Fernández-Cabrera Marín, Luz M. (Spain)
Fernández-Cara, Enrique (Spain)
Fernández-Suárez, Lucia (Portugal)
Fernando Galván, José Francisco (Spain)
Ferrández Izquierdo, Ángel (Spain)
Ferreira de Pablo, Raúl (Spain)
Ferreira, Ana Cristina (Portugal)
Ferreira, Fernanda A. (Portugal)
Ferreira, Flávio (Portugal)
Ferreira, Luis (Portugal)
Ferreiro Ferreiro, Ana María (Spain)
Ferrer, Walter (Uruguay)
Ferrero, Miguel (Brazil)
Ferreyra, Guillermo (USA)
Field, Timothy (Canada)
Figueiras, Lourdes (Spain)
Finashin, Sergey (Turkey)
Finicias, Mariló (Spain)
Fintushel, Ronald (USA)
Fioravanti, Mario (Spain)
Fischbacher-Weitz, Helena (United Kingdom)
Fischler, Stéphane (France)
Fisher, David (USA)
Fisk, Steve (USA)
Fiz Pontiveros, Gonzalo (United Kingdom)
Fleischner, Herbert (Austria)
Flores Dorado, José Luis (Spain)
Flores Lasa, Irene (Spain)

Flores Peña, Edurne (Spain)
Flores, Ramón J. (Spain)
Flores-Bazán, Fabián (Chile)
Flores-Espinoza, Rubén (Mexico)
Flytzanis, Elias (Greece)
Foellmer, Hans (Germany)
Font, Sarita (Puerto Rico)
Fontelos López, Marco Antonio (Spain)
Fontich, Ernest (Spain)
Formaggia, Luca (Italy)
Förster, Markus (Germany)
Forti, Marco (Italy)
Fox, Daniel (Spain)
Fraguela Collar, Andrés (Mexico)
Francaviglia, Stefano (Spain)
Franco Lázaro, Elena (Spain)
Franco, Camilo (Spain)
Frangos, Nicolaos (Greece)
Franjou, Vincent (France)
Frank, Vallentin (The Netherlands)
Franks, John (USA)
Freniche, Francisco (Spain)
Fresán Leal, Javier (Spain)
Freyn, Walter (Germany)
Frías Armenta, Martín Eduardo (Mexico)
Friedlander, John (Canada)
Friedlander, Susan (USA)
Friedman, Eduardo (Chile)
Friger, Michael (Israel)
Frolkin, Alexander (United Kingdom)
Fuentes Fernández-Vegue, Beatriz (Spain)
Fuentes García-Arévalo, Marta (Spain)
Fuertes Fraile, Mª Concepción (Spain)
Fujiwara, Kazuhiro (Japan)
Fukaya, Kenji (Japan)
Fukshansky, Lenny (USA)
Fukumoto, Yoshihiro (Japan)
Furati, Khaled (Saudi Arabia)
Futaki, Akito (Japan)
Futorny, Vyacheslav (Brazil)

Gadjiev, Tahir (Azerbaijan)
Gago Couso, Felipe (Spain)
Gago Vargas, Manuel Jesús (Spain)
Galanis, George (Greece)
Galatius, Soren (USA)
Galdón, José Mª (Spain)
Galeana Sánchez, Hortensia (Spain)
Galguera García, Lucía (Spain)
Galina, Esther (Argentina)
Galindo Guil, Francisco J. (Spain)
Galindo Pastor, Carlos (Spain)
Gallardo, Luis H. (France)
Gallego Alonso-Colmenares, José María (Spain)
Gallego Ortiz, Leticia (Spain)
Galluzzi, Federica (Italy)
Galo Sánchez, José R. (Spain)
Gálvez Carrillo, María Inmaculada (United Kingdom)
Gamboa Mutuberria, José Manuel (Spain)
Gamero Martínez, Natalia (Spain)
Gamkrelidze, Nikolay (Russian Federation)
Gancedo, Francisco (Spain)
Gann, Sebastián (Austria)
Gao, Mingzhe (P.R. China)
Garay, József (Hungary)
García Alonso, Andoni (Spain)
García Barroso, Evelia Rosa (Spain)
García Bouso, Ana (Spain)
García Cabrera, Ana Rus (Spain)
García Cuesta, Serapio (Spain)
García Díaz, Pedro Ruymán (Spain)
García Duarte Júnior, Geraldo (Brazil)
García Escamilla, María Luz (Spain)
García Escudero, Juan (Spain)
García Fernández, Belén (Spain)
García Fernández, Mario (Spain)
García Fernández, Roberto (Spain)
García Ferrández, Pedro (Spain)
García García, Antonio (Spain)
García García, Concepción (Spain)
García Garrido, Víctor José (Spain)
García Guerrero, Oscar (Spain)
García Hernández, Josefa María (Spain)
García Herrero, Sara (Spain)
García Lechuga, Claudia (Spain)
García López, Sara (Spain)
García Marco, Ignacio (Spain)
García Martín, Montserrat Andrea (Spain)
García Martínez, Luis E. (Spain)
García Nieto, Marina (Spain)
García Pineda, Mª Pilar (Spain)
García Planas, María Isabel (Spain)
García Rodríguez, José Antonio (Spain)
García Rubira, José María (Spain)
García Sánchez, Mª Asun (Spain)
García Santos, Florentino (Spain)

García Seco de Herrera, Alba (Spain)
García Soriano, David (Spain)
García Stranz, David (Spain)
García Valldecabres, Marta (Venezuela)
García Vallinas, José Manuel (Spain)
García Zamora, Alexis (Mexico)
García, Esther (Spain)
García, Juan Luis (Spain)
García-Cuerva, José (Spain)
García-Gutiérrez Báez, Carlos (Spain)
García-Jurado, Ignacio (Spain)
García-López, Jesús (Spain)
García-Pardo Alonso, Jimena (Spain)
García-Pelayo Novo, Ricardo (Spain)
Garcia-Prada, Oscar (Spain)
García-Río, Eduardo (Spain)
Garma Pons, Santiago (Spain)
Garrido, Ángel (Spain)
Garrido, Isabel (Spain)
Garrigós, Gustavo (Spain)
Garza Merino, Sergio (Spain)
Garzón, Antonio R. (Spain)
Garzon, Martin Ezequiel (Spain)
Gaspar, Maria (Spain)
Gassiat, Elisabeth (France)
Gatto, A. Eduardo (USA)
Gaudry, Garth (Australia)
Gavioli, Andrea (Italy)
Gea García, Clara (Spain)
Geer, Nathan (USA)
Gejji, Varsha (India)
Gelfand, Sergei (USA)
Gelfreich, Vassili (United Kingdom)
Geraci, Linda (USA)
Gérard, Patrick (France)
Gerards, Bert (The Netherlands)
Gerhard Dorfmeister, Josef (USA)
Gerhard, Wanner (Switzerland)
German, Oleg (Russian Federation)
Gesto, José Manuel (Spain)
Geyn, Sergey (Germany)
Ghaffari, Ali (Iran)
Ghahramani, Saeed (USA)
Ghenciu, Ioana (USA)
Ghenciu, Petre (USA)
Ghita, Constantine (Romania)
Ghorbani, Ebrahim (Iran)
Ghoussoub, Nassif (Canada)
Ghrist, Robert (USA)
Ghys, Étienne (France)
Giacardi, Livia (Italy)
Giannoulis, Johannes (Germany)
Giaquinto, Anthony (USA)
Giardina, Federica (Spain)
Gibson, Paul F. (USA)
Gil Álvarez, Pedro (Spain)
Gil Clemente, Elena (Spain)
Gil Gutiérrez, Mauricio (Mexico)
Gil Medrano, Olga (Spain)
Gilligan, Bruce (Canada)
Gilmer, Patrick (USA)
Gilsanz Mayor, M. Ángeles (Spain)
Giménez de Ory, Elena (Spain)
Giménez Palomares, Fernando (Spain)
Giner Bosch, Vicent (Spain)
Ginoux, Jean-Marc (France)
Ginovart, Marta (Spain)
Gioev, Dimitri (USA)
Giovine, Pasquale (Italy)
Giraldo Carbajo, Antonio (Spain)
Giraldo Suárez, Luis (Spain)
Girela, Daniel (Spain)
Girondo, Ernesto (Spain)
Gloeckner, Helge (Germany)
Godoy, Eduardo (Spain)
Goetze, Friedrich (Germany)
Goffa, Isabel (Belgium)
Golchin, Akbar (Iran)
Golse, François (France)
Goltser, Yakov (Israel)
Golubitsky, Martin (USA)
Gómez Aparicio, María Paula (France)
Gómez Aroca, José María (Spain)
Gómez Ayala, Eugenio Jesús (Spain)
Gómez Gandarillas, Delfina (Spain)
Gómez Gil, Javier (Spain)
Gómez Lozano, Miguel (Spain)
Gómez Martín, José R. (Spain)
Gómez Martín, Verónica (Spain)
Gómez Pasquali, Gabriela (Paraguay)
Gómez Pérez, Javier (Spain)
Gómez Repollés, Carlos (Spain)
Gómez Ruiz, Francisco (Spain)
Gómez Ruiz, Paloma (Spain)
Gómez Serrano, Javier (Spain)
Gómez Sierra, César Augusto (Colombia)
Gómez Villegas, Miguel A. (Spain)
Gómez, Bernardo (Spain)

Gómez, Tomas l. (Spain)
Gómez-Cabrero López, David (Spain)
Gómez-Larrañaga, José Carlos (Mexico)
Gómez-Mourelo, Pablo (Spain)
Gómez-Ullate Oteiza, David (Spain)
Gong, Fuzhou (P.R. China)
Gongopadhyay, Krishnendu (India)
González Acuña, Francisco (Mexico)
González Álvarez, José Luis (Spain)
González de La Cruz, Ana (Spain)
González Díaz, Celia (Spain)
González Díaz, Julio (Spain)
González Díez, Gabino (Spain)
González Fernández, Cesareo (Spain)
González Gómez, Antonia (Spain)
González Gutiérrez, Pablo (Spain)
González Jiménez, Enrique (Spain)
González Jiménez, Santos (Spain)
González Llavona, José (Spain)
González Manchón, Pedro María (Spain)
González Manteiga, María Teresa (Spain)
González Moya, Oscar (Spain)
González Nogueras, Maria del Mar (USA)
González Núñez, Jorge (Spain)
González Pérez, Pedro (Spain)
González Regaña, Alfonso J. (Spain)
González Rojo, Elena (Spain)
González Rovira, Joseph (Spain)
González Salcedo, Alejandro (Spain)
González Salcedo, Carlos (Spain)
González Sánchez, Luis (Spain)
González Sarabia, Manuel (Mexico)
González Sotos, León (Spain)
González Vasco, María Isabel (Spain)
González Vega, Laureano (Spain)
González Vida, José Manuel (Spain)
González Villa, Manuel (Spain)
González Viña, Pablo (Spain)
González, Elena (Spain)
González-Aguilar, Hernán (Mexico)
González-Berenguer, Aranzazu (Spain)
González-Manteiga, Wenceslao (Spain)
González-Pérez, Beatriz (Spain)
Gonzalo Pérez, Jesús (Spain)
Gonzalvo Ballano, Raquel (Spain)
Gopalakrishnan, Santhanam (India)
Gordon, Cameron (USA)
Górka, Przemyslaw (Poland)
Gorkavyy, Vasyl (Ukraine)
Gorodski, Claudio (Brazil)
Gorrochategui Gregorio, Leire (Spain)
Goswami, Debashish (India)
Gothen, Peter (Portugal)
Goto, Midori (Japan)
Gouveia, Paulo (Portugal)
Gowers, Timothy (United Kingdom)
Graber, Tom (USA)
Gracia, Juan Miguel (Spain)
Gracia-Saz, Alfonso (USA)
Graf, Gian Michèle (Switzerland)
Grafe Arias, Fritz Hans (Spain)
Granados Pérez, Ana Belén (Spain)
Granero Belinchón, Rafael (Spain)
Granja Barón, Ángel (Spain)
Grantcharov, Dimitar (USA)
Graña, Matías (Argentina)
Grasselli, Luigi (Italy)
Grasso, Thomas (USA)
Grau de la Herrán, Ana (Spain)
Gray, Mary (USA)
Grebenyuk, Marina (Ukraine)
Green, Ben J. (United Kingdom)
Greuel, Gert-Martin (Germany)
Griebel, Michael (Germany)
Griffiths, Phillip A. (USA)
Griffiths, Simon (United Kingdom)
Grinblat, Leonid (Israel)
Grinevich, Petr (Russian Federation)
Grobstich, Peter (Germany)
Groeschel, Michael (Germany)
Groisman, Pablo (Argentina)
Grojnowski, I. (United Kingdom)
Gromov, Nikolay (Russian Federation)
Grötschel, Martin (Germany)
Groves Groves, Daniel (USA)
Gruber, Peter M. (Austria)
Grundman, Helen (USA)
Grunewald, Fritz (Germany)
Guaraldo, Rosalind (USA)
Guàrdia, Jordi (Spain)
Guccione, Jorge Alberto (Argentina)
Guccione, Juan José (Argentina)
Guenther, Christine (USA)
Guerra Guaza, Ana Mª (Spain)
Guerrero Meléndez, Iván (Spain)
Guerrero Villanueva, Víctor (Spain)
Guerrero, Manuel (Spain)
Guerrero-García, Pablo (Spain)

Guevara-Jordan, Juan (Venezuela)
Guezane-Lakoud, Assia (Algeria)
Guicciardini, Niccolo (Italy)
Guijarro Santamaría, Luis (Spain)
Guil Asensio, Pedro Antonio (Spain)
Guillamón Grabolosa, Antoni (Spain)
Guillén González, Francisco (Spain)
Guillén Martín, Antonio (Spain)
Guillera Goyanes, Jesús (Spain)
Guionnet, Alice (France)
Guirado Granados, Juan Francisco (Spain)
Gun, Sanoli (India)
Gunzburger, Max (USA)
Guo, Wei (P.R. China)
Gupta, Shiv (USA)
Gurevich, Pavel (Russian Federation)
Gurney, Susan (USA)
Gursky, Matthew (USA)
Gurtu, Vishnu Kumar (India)
Gusevskii, Nikolay (Brazil)
Guseyn-Sade, Sabir (Russian Federation)
Gusinde, Ellinor (Germany)
Guterman, Alexander (Russian Federation)
Gutiérrez del Álamo, Joaquín M. (Spain)
Gutiérrez Jiménez, José Manuel (Spain)
Gutiérrez León, Ignacio (Spain)
Gutiérrez Mejía, Darwin (Spain)
Gutiérrez Moya, Ester (Spain)
Gutiérrez, Elena Olga (Spain)
Gutiérrez, Javier José (Spain)
Gutiérrez, Manuel (Spain)
Gutu, Olivia (Mexico)
Guzmán Arias, Fernando (Spain)
Guzmán Estepa, Violeta (Spain)
Gwena, Tawanda (USA)

Ha Binh, Minh (the Netherlands)
Ha Tien, Ngoan (Vietnam)
Ha, Huy Khoai (Vietnam)
Hagelstein, Paul (USA)
Hagen, Thomas (USA)
Haglund, Jim (USA)
Haiman, Mark (USA)
Haime Pastore, Dayse (Brazil)
Hajto, Zbigniew (Poland)
Hales, Thomas C. (USA)
Hamada, Tatsuyoshi (Japan)
Hamilton, Richard (USA)
Hansen, Vagn Lundsgaard (Denmark)
Hans-Gill, Rajinder (India)
Harris, Michael (France)
Hartmann W, Frederick (USA)
Hartmann, Robert (Germany)
Hartwig, Jonas (Sweden)
Hasegawa, Keizo (Japan)
Hashmi, Viquar (United Kingdom)
Hassairi, Abdelhamid (Tunisia)
Hästö, Peter (Finland)
Hasumi, Morisuke (Japan)
Hauser, Herwig (Austria)
Hayrapetyan, Hrachik (Armenia)
Hbid, Moulay Lhassan (Morocco)
Hearst, William (USA)
Hebert, Michel (Egypt)
Heinig, Hans (Canada)
Heinze, Joachim (Germany)
Helemskii, Alexander (Russian Federation)
Hempfling, Thomas (Switzerland)
Hencl, Stanislav (Czech Republic)
Henniart, Guy (France)
Henriques G., Andre (Germany)
Henry, Philippe (Switzerland)
Heo, Jaeseong (South Corea)
Herencia González, J.A. (Spain)
Hermida Alonso, José Ángel (Spain)
Hernández Arteaga, Jonay (Spain)
Hernández Corbato, Luis (Spain)
Hernández Jiménez, Mª Beatriz (Spain)
Hernández Paricio, Luis Javier (Spain)
Hernández Peñalver, Gregorio (Spain)
Hernández Pérez, Begoña (Spain)
Hernández Rodríguez, Francisco l. (Spain)
Hernández, Eugenio (Spain)
Hernández, Francisco Javier (Spain)
Hernando Boto, Beatriz Isabel (Spain)
Hernando Carrillo, Fernando (Spain)
Herrera García, Fátima (Spain)
Herrero Sanz, Henar (Spain)
Hershberger, Mark (Germany)
Herzig, Florian (France)
Hessami Pilehrood, Khodabakhsh (Iran)
Hessami Pilehrood, Tatiana (Iran)
Hezlet, Susan (United Kingdom)
Hidaka, Fumio (Japan)
Hidalgo Ortega, Rubén (Chile)
Himadri Kumar, Mukerjee (India)
Hinojosa, Gabriela (Mexico)
Hintermann, Thomas (Switzerland)

Hinz, Andreas (Germany)
Hiriart-Urruty, Jean-Baptiste (France)
Hitchin, Nigel (United Kingdom)
Hjelle, Geir Arne (USA)
Hoang Nguyen, Tuan Khanh (Germany)
Hodgson, Bernard R. (Canada)
Hofmann, Steven (USA)
Hollanti, Camilla (Finland)
Holme, Anne Berit Lunde (Norway)
Holme, Audun (Norway)
Holte, John (USA)
Honda, Ko (USA)
Hong, Feng (P.R. China)
Hoover Kearn, Vickie (United Kingdom)
Hopcroft, John (USA)
Hopkins, Michael (USA)
Horadam, Kathy (Australia)
Horiuchi, Kiyomitsu (Japan)
Horiuchi, Toshio (Japan)
Horváth, Miklós (Hungary)
Houdayer, Cyril France)
Houpa Danga, Duplex Elvis (Cameroon)
Hoyos, José Jaime (Spain)
Hric, Roman (France)
Hryn, Aliaksandr (Belarus)
Hsiang, Wu-Chung (USA)
Hsu, Jyh-Ping (Taiwan)
Huang, Chu-ching (Taiwan)
Huerta Herrera, Carlos (Spain)
Huertas Sánchez, Maria Antonia (Spain)
Huggett, Stephen (United Kingdom)
Hughes, Kenneth (South Africa)
Huguet Casades, Gemma (Spain)
Hunt, John H. V. (South Africa)
Hurtado Cortegana, Ana (Spain)
Hwang, Jun-Muk (South Corea)
Hwang, Tea-Yuan (Taiwan)

Ibáñez Mateos, Álvaro (Spain)
Ibáñez Mesa, Santiago (Spain)
Ibáñez Torres, Raúl (Spain)
Ibort, Alberto (Spain)
Ibragimov, Zair (USA)
Ichihara, Kazuhiro (Japan)
Iglesias Martínez, José Alberto (Spain)
Iglesias Ponte, David (Spain)
Ignat, Ioan Liviu (Spain)
Ignat, Ioan Liviu (Spain)
Iitaka, Shigeru (Japan)
Ilie, Monica (Canada)
Illusie, Luc (France)
Ilmanen, Tom (Switzerland)
Im, Bokhee (South Corea)
Incinillas Vicario, Alba (Spain)
Indurain-Eraso, Esteban (Spain)
Infante del Río, Juan Antonio (Spain)
Inglada Pérez, Lucia (Spain)
Iniotakis, Jan-Mark (Germany)
Insua Hermo, Manuel Avelino (Spain)
Inugay Rojas, Sandra (Spain)
Iommi Amunategui, Godofredo (Portugal)
Ion, Patrick (USA)
Ionel, Marianty (USA)
Iranmanesh, Ali (Iran)
Irastorza, Luis (Spain)
Isábal de Marta, Tresa Myriam (Spain)
Isaev, Alexander (Australia)
Isakovic Ilic, Mirjana (Serbia & Montenegro)
Ishii, Hitoshi (Japan)
Isselkou Ould, Ahmed Izid Bih (Mauritania)
Istad, Roy Martin (Norway)
Itô, Junko (Japan)
Itoh, Jin-Ichi (Japan)
Ivic, Aleksandar (Serbia & Montenegro)
Iwaniec, Henryk (USA)
Iyama, Osamu (Japan)
Izquierdo Barrios, Milagros (Sweden)
Jacobsson, Karl Magnus (Italy)
Jaeyoo, Choy (South Corea)
Jaffe, Arthur (USA)
Jaikin Zapirain, Andrei (Spain)
Jamardo Ventoso, Diego (Spain)
Jambu, Michel (France)
Jane, James (United Kingdom)
Jang, Sun-Young (South Corea)
Janno, Jaan (Estonia)
Jara Martínez, Pascual (Spain)
Jaramillo Aguado, Jesús Ángel (Spain)
Jaramillo, Diana (Colombia)
Jardim, Marcos (Brazil)
Jedrzejak, Tomasz (Poland)
Jeltsch, Rolf (Switzerland)
Jen, Yuan-Jen Chiang (USA)
Jeong, Ja A (South Corea)
Jeong, Moonja (South Corea)
Jeremías López, Ana (Spain)
Jerónimo, Gabriela (Argentina)
Ji, Lizhen (USA)

Ji, Yongmao (Spain)
Jiang, Erxiong (P.R. China)
Jiménez Alcalá, Elena (Spain)
Jiménez Canencia, Francisco Javier (Spain)
Jiménez Carretero, Daniel (Spain)
Jiménez del Toro, Ana (Spain)
Jiménez Gómez, David (Spain)
Jiménez Urroz, Jorge (Spain)
Jiménez, Bienvenido (Spain)
Jiménez, Clara (Spain)
Jin, Yafen (P.R. China)
Jing, Naihuan (USA)
Joe, Dosang (South Corea)
Joglar, Nuria (Spain)
Johnsen, Trygve (Norway)
Johnson, David (USA)
Johnstone, Iain (USA)
Joita, María (Romania)
Jones, Damien Michael (USA)
Jones, Keith (The Netherlands)
Jones, Vaughan (USA)
Jong, Jaebu (North Corea)
Joshi, Uttank (India)
Jover, Francisco (Spain)
Jovero, Edgardo (Spain)
Jozefiak, Tadeusz (USA)
Juano Ayllón, Antonio (Spain)
Juárez, Adriana (Mexico)
Juhl-Jöricke, Burglind (Sweden)
Juliá Obrador, Mª Sebastiana (Spain)
Jung, Tacksun (South Corea)
Jurisich, Elizabeth (USA)
Just, Andrzej (Poland)

Kaabachi, Saida (France)
Kaarli, Kalle (Estonia)
Kacinskaite, Roma (Lithuania)
Kadaoui Abbassi, Mohamed Tahar (Morocco)
Kaijser, Sten (Sweden)
Kaimakamis, Georgios (Greece)
Kakiuchi, Nobuhiko (Japan)
Kalajdzievski, Sasho (Canada)
Kalimeris, Konstantinos (United Kingdom)
Kalita, Jiten (India)
Kalmenov, Tynysbek (Kazakhstan)
Kaloshin, Vadim (USA)
Kamiya, Noriaki (Japan)
Kamotski, Vladimir (United Kingdom)
Kamran, Niky (Canada)
Kanbay, Filiz (Turkey)
Kanduru, Venkata Krishna (India)
Kane, Richard (Canada)
Kaneko, Makoto (Japan)
Kang, Seok-Jin (South Corea)
Kang, Soon-Yi (South Corea)
Kangro, Urve (Estonia)
Kania-Bartoszynska, Joanna (USA)
Kapelou, Aikaterini (Greece)
Kapovich, Michael (USA)
Kappos, Efthimios (Greece)
Kapshayev, Iskander (Kazakhstan)
Kaptanoglu, H. Turgay (Turkey)
Karaliolios, Nikolaos (Greece)
Karamzadeh, Omid Ali (Iran)
Karbe, Manfred (Germany)
Karimov, Umed (Tadjikistan)
Karmanova, Maria (Russian Federation)
Karoubi, Max (France)
Karuppuchamy, Paramasamy (India)
Kashif, Abdul Rehman (Pakistan)
Kashiwara, Masaki (Japan)
Kassara, Khalid (Morocco)
Kasyanov, Victor (Russian Federation)
Katavolos, Aristides (Greece)
Kato, Kazuya (Japan)
Katona, Gyula O.H. (Hungary)
Katrin, Gelfert (Germany)
Katsap, Ada (Israel)
Kawamura, Minaru (Japan)
Kayvanfar, Saeed (Iran)
Kazakov, Vladimir (Mexico)
Kazarian, Kazaros (Spain)
Kazuhiro, Sakue (Japan)
Keith, Jonathan (Australia)
Keller, Bernard (France)
Kenderov, Petar (Bulgary)
Kenmotsu, Katsuei (Japan)
Kepczynska, Anna (Poland)
Kerchy, Laszlo (Hungary)
Keum, Jonghae (South Corea)
Keyfitz, Barbara (Canada)
Khaldi, Rabah (Algeria)
Khalil, Zohel (Canada)
Khalique, Chaudry Masood (South Africa)
Kharaghani, Hadi (Canada)
Kharchenko, Vladislav (Mexico)
Kharin, Yuriy (Belarus)
Khatskevich, Victor (Israel)

Khazaie, Behzad (France)
Khokhlov, Vladimir (Russian Federation)
Khön Luque, Álvaro (Spain)
Khosravi, Behrooz (Iran)
Khosrovshahi, Gholamreza B. (Iran)
Khots, Boris (USA)
Khovanov, Mikhail (USA)
Kida, Masanari (Japan)
Kida, Yoshikata (Germany)
Kientega, Gerard (Burkina Faso)
Kierlanczyk, Mark (USA)
Kilp, Mati (Estonia)
Kim, Chang-Wan (South Corea)
Kim, Daehong (South Corea)
Kim, Dohan (South Corea)
Kim, Hoil (South Corea)
Kim, Inkang (South Corea)
Kim, Innsun (South Corea)
Kim, Jeong Han (USA)
Kim, Jongsu (South Corea)
Kim, Joonhyung (South Corea)
Kim, Seongtag (South Corea)
Kim, Tujin (North Corea)
Kim, Yoon Hee (South Corea)
Kimura, Shun-Ichi (Japan)
Kimura, Takashi (USA)
Kirillov, Oleg (Germany)
Kirschenhofer, Peter (Austria)
Kisaka, Masashi (Japan)
Kiss, György (Hungary)
Kitano, Teruaki (Japan)
Kiwi, Jan (Chile)
Kiyohara, Kazuyoshi (Japan)
Klartag, Boáz (USA)
Klatte, Rudi (Germany)
Klazar, Martin (Czech Republic)
Klein, Moshe (Israel)
Kleinberg, Jon M. (USA)
Kleiner, Bruce (USA)
Kloeckner, Benoit (France)
Knezevic Miljanovic, Julka
(Serbia & Montenegro)
Knoebel, Arthur (USA)
Ko, Ki Hyoung (South Corea)
Kobayashi, Keiko (Japan)
Kodama, Hiroki (France)
Koenig, Steffen (Germany)
Koh, Sung-Eun (South Corea)
Kohn, Robert V. (USA)
Kojima, Sadayoshi (Japan)
Kokubu, Hiroshi (Japan)
Kolodziejczyk, Danuta (Poland)
Kondic, Lou (USA)
König, Hannah (Germany)
Konijeti, Sreenadh (India)
Konopelchenko, Boris (Italy)
Konstantin, Lutskiy (Russian Federation)
Konyagin, Sergey (Russian Federation)
Koo, Hyung Woon (South Corea)
Koo, Nam Jip (South Corea)
Kornilowicz, Artur (Poland)
Korobkov, Mikhail (Russian Federation)
Korotiaev, Mikhail (USA)
Korte, Riikka (Finland)
Koryakin, Pavel (Russian Federation)
Koshiba, Yoichi (Japan)
Kostant, Ann (USA)
Kotschick, Dieter (Germany)
Kotyada, Srinivas (India)
Koua, Konin (Ivory Coast)
Kourki I, Farid (Morocco)
Kozdron, Michael (Canada)
Kozlovskiy, Oleg (United Kingdom)
Kozlowski, Wojciech (Poland)
Kra, Bryna (USA)
Kral, Daniel (Czech Republic)
Kraljevic, Hrvoje (Croatia)
Kranz, Przemo (USA)
Kremer, Darla (USA)
Kreussler, Bernd (Ireland)
Kribs Zaleta, Christopher (USA)
Kröger, Heinz (Germany)
Kropielnicka, Karolina (Poland)
Kruglikov, Boris (Norway)
Kujawa, Jonathan (USA)
Kukreja, Vijay Kumar (India)
Kuku, Aderemi (USA)
Kulkarni, Rekha (India)
Kumar, Abhinav (USA)
Kumar, Romesh (India)
Kumar, Sanjeev (India)
Kumlin, Peter (Sweden)
Kunnath, Sandeep (India)
Kuo, Tsang-Hai (Taiwan)
Kuperberg, Greg (USA)
Kurdachenko, Leonid (Ukraine)
Kurganov, Alexander (USA)
Kurlin, Vitaliy (United Kingdom)

Kuzichev, Alexander (Russian Federation)
Kwak, Sijong (South Corea)
Kwon, Ohin (South Corea)

Laburta, M. Pilar (Spain)
Lacomba, Ernesto (Mexico)
Ladra González, Manuel (Spain)
Laffey, Thomas (Ireland)
Lahcène, Mezrag (Algeria)
Lahoz Beltra, Rafael (Spain)
Lajara López, Sebastián (Spain)
Laliena, Jesús (Spain)
Lalley, Steven (USA)
Lalonde, François (Canada)
Lam, Thomas (USA)
Lampe, Philipp (Germany)
Lance, Christopher (United Kingdom)
Lanchon, Pierre (France)
Lang, Jens (Germany)
Lange, Herbert (Germany)
Langer, Marina (Germany)
Langford, William (Canada)
Lap, James T. (USA)
Laptev, Ari (Sweden)
Larkine, Nikolai (Brazil)
Lastra Díaz, Juan José (Spain)
Laumon, Gérard (France)
Laurenti, Sharon (Italy)
Lauret, Jorge (Argentina)
Lawler, Gregory (USA)
Lawrence, Snezana (United Kingdom)
Le Bris, Claude (France)
Le Calvez, Patrice (France)
Le Gall, Jean-Francois (France)
Le Jan, Yves (France)
Leary, Ian (USA)
Lebrija Trejos, Analinnette (Spain)
Lee, Donghi (South Corea)
Lee, Eunjeong (South Corea)
Lee, Hyang-Sook (South Corea)
Lee, Jaewoo (USA)
Lee, Jyh-Hao (Taiwan)
Lee, Keonhee (South Corea)
Lee, Kyu-Hwan (USA)
Lee, Mi Kyung (South Corea)
Lee, Nam-Hoon (South Corea)
Lee, Pengyee (Singapore)
Lee, Seok-Min (South Corea)
Lee, Yng-Ing (Taiwan)
Lee, Young Joo (South Corea)
Lee, Yuan-Pin (USA)
Lee, Yuh-Jia (Taiwan)
Leganés Combarro, Jesús (Spain)
Lehnert, Jörg (Germany)
Lekuona Amiano, Alberto (Spain)
Lelievre, Samuel (United Kingdom)
Lemahieu, Ann (Belgium)
Lemaire, Luc (Belgium)
Lempert, Laszlo (USA)
Lenzi, Domenico (Italy)
Lenzing, Helmut (Germany)
Leok, Melvin (USA)
León Fernández, Aurora (Spain)
Lequain, Yves (Brazil)
Lequeu, Emmanuel (United Kingdom)
Lesmono, Dharma (Indonesia)
Leuschke, Graham (USA)
LeVeque, Randall J. (USA)
Levermore, David (USA)
Levin, Alexander (USA)
Levstein, Fernando (Argentina)
Lewis, Robert (USA)
Leykin, Anton (USA)
Lezaun, Mikel (Spain)
Li, Chi (P.R. China)
Li, Dong (P.R. China)
Li, Fucai (P.R. China)
Li, Miao (P.R. China)
Li, Yuxiang (P.R. China)
Liang, Song (Japan)
Libbrecht, Paul (Germany)
Libedinsky, Nicolas (France)
Liberatii, José (Argentina)
Libine, Matvei (USA)
Lih, Ko-Wei (Taiwan)
Lin, Ling (P.R. China)
Linares Bravo, Daniel (Spain)
Linares Briones, Pablo (Spain)
Linares, Felipe (Brazil)
Lind, Andreas (Sweden)
Lindenstrauss, Elon (USA)
Lindenstrauss, Joram (Israel)
Linton, Fred E.J. (USA)
Lipponen, Marjo (Finland)
Liu, Fengshan (USA)
Liu, Xiaobo (USA)
Liverpool, Lennox (Nigeria)
Lizárraga, David A. (Mexico)

Llado, Anna (Spain)
Lledó, Fernando (Germany)
Llerena Aguilar, Estrella (Spain)
Llerena Rodríguez, Irene (Spain)
Llorente Comí, Marta (Spain)
Lloveras Aulet, Angelina (Spain)
Lockhart, Deborah (USA)
Lodares González, Dolores (Spain)
Loftin, John (USA)
Logares Jiménez, Marina (Spain)
Longás, Concepción (Spain)
Longhi, Ignazio (Italy)
Lopes-Dias, Joao (Portugal)
López Arena, José Antonio (Spain)
López Cabeceira, Montserrat (Spain)
López Cerdá, Marco Antonio (Spain)
López Clazada, Juan Pedro (Spain)
López de Silanes Busto, María Cruz (Spain)
López Díaz, María Concepción (Spain)
López Fidalgo, Jesús (Spain)
López García, Juan Antonio (Spain)
López Garza, Gabriel (Mexico)
López Hernández, Sergio (Spain)
López López, Victoria (Spain)
López Martialay, Francisco (Spain)
López Martín, Alberto (Germany)
López Martín, Ana Cristina (Spain)
López Meléndez, José María (Spain)
López Palacios, Iris (Venezuela)
López Pellicer, Manuel (Spain)
López Peña, Javier (Spain)
López Prieto, Manuel (Spain)
López Quijorna, María (Spain)
López Rodríguez, Mª Teresa (Spain)
López Serna, Juan Daniel (Spain)
López Valdes, María (Spain)
López, Guillermo (Spain)
López, Luis (USA)
López, Rafael (Spain)
Lorente Morata, Ana Cecilia (Spain)
Lorenzo García, Elisa (Spain)
Lott, John (USA)
Loureiro Galán, Gonzalo (Spain)
Lovas, Rezso Laszlo (Hungary)
Lovasz, Laszlo (USA)
Lozano Rivas, Mª José (Spain)
Lozano Rojo, Álvaro (Spain)
Lozano Soneira, María Rosa (Spain)
Lozano, María Teresa (Spain)
Lozano-Robledo, Álvaro (USA)
Lu, Guofu (P.R. China)
Lu, Yunguang (P.R. China)
Luca, Florian (Mexico)
Lucas Rodríguez, Fernando (Spain)
Luciano, Erika (Italy)
Luczak, Tomasz (Poland)
Luengo Velasco, Ignacio (Spain)
Lukkari, Teemu (Finland)
Luo, Wenzhi (USA)
Luoto, Kurt (USA)
Lupiáñez, F.G. (Spain)
Luque, Javier (USA)
Luzón Cordero, Ana María (Spain)

Ma, Li (P.R. China)
Ma, Xiaonan (France)
Ma, Zhi-Ming (P.R. China)
Mabuchi, Toshiki (Japan)
Macarini, Leonardo (Brazil)
Machaca, Marina (Spain)
Macho Stadler, Marta (Spain)
Macias Virgós, Enrique (Spain)
Macintyre, Angus (United Kingdom)
Mackaay, Marco (Portugal)
Madan, Shobha (India)
Madanshekaf, Ali (Iran)
Maday, Yvon (France)
Madkhali, Abdossalam (Saudi Arabia)
Madsen, Ib (Denmark)
Maeda, Hidetoshi (Japan)
Maehara, Kazuhisa (Japan)
Maestre Caballero, Faustino (Spain)
Magnanini, Rolando (Italy)
Magnin, Louis (France)
Magnitskii, Nikolai (Russian Federation)
Mahdavi-Hezavehi, Mohammad (Iran)
Mahyar, Hakimeh (Iran)
Maillet, Jean-Michel (France)
Maín Yaque, Paloma (Spain)
Maingi, Damian (Kenya)
Mainkar, Meera (India)
Maitra Kumar, Jitendra (India)
Makky, Sadia M. (USA)
Malamud, Mark (Ukraine)
Malcolmson, Peter (USA)
Maldonado, Mercedes (Spain)
Malek, Alaeddin (Iran)
Maleknejad, Khosrow (Iran)

Malheiro, Maria Teresa (Portugal)
Maliki, Youssef (Algeria)
Mallavibarrena Martínez de Castro, Raquel (Spain)
Malliaris, Maryanthe (USA)
Malliavin, Paul (France)
Mallor Holla, Silvana (Spain)
Maltsev, Arkady (Russian Federation)
Mamadou Makhtar, Diop (Senegal)
Mampassi, Benjamin (Senegal)
Manchanda, Pammy (India)
Mancho, Ana María (Spain)
Mandai, Takeshi (Japan)
Mandelbrot, Benoit (USA)
Manders, Kenneth (USA)
Mandrescu, Eugen (Israel)
Manfredi, Juan (USA)
Mango Magero, John (Uganda)
Manickam, Murugesan (India)
Manin, Yuri (USA)
Manjarín, Mónica (Spain)
Mann, Elizabeth (USA)
Mantegazza, Carlo (Italy)
Mantilla Nuñez, Irla Doraliza (Peru)
Manturov, Vassily Olegovich (Russian Federation)
Manubens Ferriol, Montserrat (Spain)
Manuilov, Vladimir (Russian Federation)
Manzano, Antonio (Spain)
Maqsood, Tariq (Pakistan)
Marcati, Pierangelo (Italy)
Marcellan, Francisco (Spain)
March, Peter (USA)
Marchetti, Riccardo (Italy)
Marco Buzunariz, Miguel Ángel (Spain)
Marco, Ana (Spain)
Marco, José Manuel (Spain)
Marcum, Howard Junior (USA)
Marcus, Andrei (Romania)
Margulis, Gregory (USA)
Mariano, Paolo María (Italy)
Marica, Aurora-Mihaela (Spain)
Marie France, Vigneras (France)
Marijuán López, Carlos (Spain)
Marín, David (Spain)
Marino, Marcos (Switzerland)
Marín-Rubio, Pedro (Spain)
Markarian, Roberto (Uruguay)
Markku, Ekonen (Finland)
Markwardt, Sylwia (Germany)
Marmon, Oscar (Sweden)
Marola, Niko (Finland)
Maróti, Miklós (Hungary)
Marquès Solé, Daniel (Spain)
Márquez, Bernardo (Phillippines)
Marrero, Isabel (Spain)
Marrero, Juan Carlos (Spain)
Marrero, Osvaldo (USA)
Marriero Hermida, Eva Mary (Spain)
Martell, José María (Spain)
Marti, Christoph (Switzerland)
Martín Alustiza, José Antonio (Spain)
Martín Brualla, Ricardo (Spain)
Martín Cabrera, Francisco (Spain)
Martín de Blas Sánchez, Pablo (Spain)
Martín de Diego, David (Spain)
Martín de la Sierra, Raúl (Spain)
Martín del Rey, Ángel (Spain)
Martín Domínguez, Ana (Spain)
Martín García, Luís (Spain)
Martín Gómez, María José (Spain)
Martín Herce, Fabián (Spain)
Martín Márquez, Victoria (Spain)
Martín Martín, Enrique (Spain)
Martín Mateos, José Carlos (Spain)
Martín Molina, Verónica (Spain)
Martín Morales, Jorge (Spain)
Martín Ruiz, Sebastián (Spain)
Martín Stickle, Miguel (Spain)
Martín Suárez, Miguel (Spain)
Martín Vázquez, Noa (Spain)
Martin, Gaven (New Zealand)
Martín, Miguel Ángel (Spain)
Martín, Pape (Germany)
Martínez Anoz, Luis (Spain)
Martínez Aparicio, Pedro Jesús (Spain)
Martínez Belda, Mª Carmen (Spain)
Martínez Calvo, Mª Cristina (Spain)
Martínez Campos, Cédric (Spain)
Martínez Díaz, Sonia (USA)
Martínez Fernández, Eduardo (Spain)
Martínez García, Ernesto (Spain)
Martínez García, Eva (Spain)
Martínez García, Jesús (Spain)
Martínez García, Mª Ángeles (Spain)
Martínez Gavara, Anna (Spain)
Martínez González, Alicia (Spain)
Martínez González, Gustavo (Spain)

Martínez Juste, Sergio (Spain)
Martínez López, Consuelo (Spain)
Martínez Marín, Alberto (Spain)
Martínez Martínez, Antonio (Spain)
Martínez Martínez, Mª Carmen (Spain)
Martínez Moro, Edgar (Spain)
Martínez Naveira, Antonio (Spain)
Martínez Pastor, Ana (Spain)
Martínez Pérez, Álvaro (Spain)
Martínez Prado, Lidia (Spain)
Martínez Ramírez, Cristina (Spain)
Martínez Rodríguez, Erick Osvaldo (Spain)
Martínez Salmerón, José (Spain)
Martínez, José Javier (Spain)
Martínez, Miqueas (Spain)
Martínez-Varela, Aurea (Spain)
Martinón, Antonio (Spain)
Martio, Olli (Finland)
Marusic, Sanja (Croatia)
Marusic-Paloka, Eduard (Croatia)
Maruyama, Fumitsuna (Japan)
Marzougui, Habib (Tunisia)
Masa Noceda, Mª Concepción (Spain)
Mata Hernández, Águeda (Spain)
Mata Lorenzo, Luis E. (Venezuela)
Mateos del Pino, Maider (Spain)
Mateos Guilarte, Juan (Spain)
Matheus, Carlos (Brazil)
Mathieu, Martin (United Kingdom)
Matías, Fernanda (Portugal)
Matolcsi, Mate (Hungary)
Matsuda, Osamu (Japan)
Matsumoto, Shigenori (Japan)
Matsuyama, Yoshio (Japan)
Matthes, Roland (Germany)
Mattila, Pertti (Finland)
Matuszewski, Roman (Poland)
Matveev, Sergey (Russian Federation)
Mauceri, Silvana (Italy)
Mautner, Carl (USA)
Maxim, Laurentiu (USA)
Maycock, Ellen (USA)
Mayeli, Azita (Germany)
Maylybaeva, Gulnara (Russian Federation)
Mayor Forteza, Gaspar (Spain)
Mazón Jareño, Diego (Spain)
Mazuelas Franco, Santiago (Spain)
McCammond, Jon (USA)
McCullagh, Peter (USA)
McDermott, Moira (USA)
McDonough, Thomas (United Kingdom)
McGettrick, Michael (Ireland)
McKay, John (Canada)
Mdzinarishvili, Leonard (Georgia)
Mebkhout, Zoghman (France)
Meessen, Patrick (Spain)
Mehta, Ghanshyam (Australia)
Mehta, Vikram (India)
Meier, David (Switzerland)
Melero Salvador, David (Spain)
Melián Pérez, María Victoria (Spain)
Melle Hernández, Alejandro (Spain)
Melnikov, Nikolai (Russian Federation)
Menal, Pere (Spain)
Menarguez Palanca, Mª Trinidad (Spain)
Mendes de Jesús, Catarina (Brazil)
Mendes Gonçalves, Suzana (Portugal)
Méndez Pérez, José Manuel (Spain)
Mendoza, Berta (Spain)
Mera Rivas, María Eugenia (Spain)
Merí de la Maza, Javier (Spain)
Merillas, Iván (Spain)
Merino Castro, Glicina (Mexico)
Mester, Armin (USA)
Mette, Ina (Germany)
Meyer, Johan (South Africa)
Miana, Pedro J. (Spain)
Michel, Philippe (France)
Michor, Peter (Austria)
Mihai Emilian, Popescu (Romania)
Mikhalkin, Grigory (USA)
Miklos, Dezso (Hungary)
Miller, Andrea (Germany)
Millionshchikov, Dmitry (Russian Federation)
Milson, Robert (Canada)
Mimouni, Abdeslam (Saudi Arabia)
Min, Kyung Chan (South Corea)
Mingarelli, Angelo B. (Spain)
Mínguez Ceniceros, Judit (Spain)
Minicozzi, William P. (USA)
Minsky, Yair (USA)
Miquel Miralles, Cristina (Spain)
Mira Anzola, Carolina (Spain)
Miranda Suárez, David (Spain)
Miranda, Anna Maria (Italy)
Mirás Calvo, Miguel Ángel (Spain)
Miret, Josep M. (Spain)
Mironov, Andrey (Russian Federation)

Misra, Gadadhar (India)
Misso, Paola (Italy)
Mitsumatsu, Yoshihiko (Japan)
Miyazaki, Yoichi (Japan)
Mladenovic, Pavle (Serbia & Montenegro)
Moazzami, Dara (Iran)
Mohammad, Abdullah (Saudi Arabia)
Mohri, Hiroaki (Japan)
Mokrane, Abdelhafid (Algeria)
Molati, Motlatsi (Lesotho)
Molchanov, Vladimir (Russian Federation)
Molina Castellano, Antonio (Spain)
Molina Madrid, Estela (Spain)
Molina Prieto, Abel (Spain)
Molinero López, Mª Celeste (Spain)
Moll Cebolla, Salvador (Spain)
Moll López, Santiago (Spain)
Monastyrsky, Michael (Russian Federation)
Moncayo, María (Spain)
Monod, Nicolas (Switzerland)
Monreal, Llúcia (Spain)
Monson, Barry (Canada)
Montaldo Montaldo, Stefano (Italy)
Montans, Fernando (Uruguay)
Montero Sánchez, Juan Aurelio (Spain)
Montes Rodríguez, Alfonso (Spain)
Montes, Antonio (Spain)
Montijano Torcal, Juan Ignacio (Spain)
Montoya Delgadillo, Elizabeth (France)
Montserrat Delpalillo, Francisco José (Spain)
Moon, Myoungho (South Corea)
Moori, Jamshid (South Africa)
Mora Cordero, Manuel José (Spain)
Morais, José Enrique (Spain)
Morales Campoy, Antonio (Spain)
Morales, Borja (Spain)
Morales, Domingo (Spain)
Morán, Manuel (Spain)
Moree, Pieter (Germany)
Morel, Fabien (Germany)
Moreno Briceño, Juan Carlos (Venezuela)
Moreno Damas, Jesús Pascual (Spain)
Moreno Gálvez, Elena (Spain)
Moreno Ventas, Javier (Spain)
Moreno, Ismael (Spain)
Moreta Santos, Mª Jesús (Spain)
Morgan, Frank (USA)
Morgan, John (USA)
Morimoto, Kanji (Japan)
Morita, Yasuo (Japan)
Moro Moyano, Rubén (Spain)
Morton, Hugh (United Kingdom)
Mosquera Mercader, Jennifer (Spain)
Mostaghim, Zohreh (Iran)
Mostovoy, Jacob (Mexico)
Moura Santos, Ana (Portugal)
Moyano Fernández, Julio-José (Spain)
Moyano Pérez, Patricia (Spain)
Moyua, Adela (Spain)
Mozo Fernández, Jorge (Spain)
Mrozowicz, Roman (Spain)
Muguruza Epelde, Eneritz (Spain)
Mukherjee, Goutam (India)
Mukherjee, Manabendra Nath (India)
Mukhopadhyay, Parthasarathi (India)
Mulase, Motohico (USA)
Mulazzani, Michele (Italy)
Mulero González, Julio (Spain)
Müller, Franz X. (Switzerland)
Munch, Arnaud (France)
Mundet i Riera, Ingasi (Spain)
Muneta, Koichi (Japan)
Munkholm, Hans J. (Denmark)
Muñoz Bouzo, María José (Spain)
Muñoz Casado, José Luis (Spain)
Muñoz Escolano, José María (Spain)
Muñoz Guillén, María del Pilar (Spain)
Muñoz López, Susana (Spain)
Muñoz Rubio, Mª José (Spain)
Muñoz Velázquez, Vicente (Spain)
Muñoz Villarragut, Víctor (Spain)
Muñoz, Roberto (Spain)
Muñoz-Lecanda, Miguel C. (Spain)
Murasugi, Kunio (Canada)
Murillo Hernández, José Alberto (Spain)
Muro, Fernando (Germany)
Murphy, Noel (Ireland)
Mushtari, Daniar (Russian Federation)
Myung, Hyo Chul (South Corea)
Myung, Sung (South Corea)

Nabarro, Ana Claudia (Brazil)
Nagai, Yasunari (South Corea)
Nagórko, Andrzej (Poland)
Nagy, Bela (Hungary)
Naidoo, Inderasan (South Africa)
Nakajima, Toru (Japan)
Nakamura, Gou (Japan)

Näkki, Raimo (Finland)
Nam, Ki-Bong (USA)
Namdari, Mehrdad (Iran)
Napp Avelli, Diego (The Netherlands)
Narayanaswami, Pallasena (Canada)
Narbona Reina, Gladys (Spain)
Nardmann, Marc (Germany)
Nart Viñals, Enric (Spain)
Narváez Macarro, Luis (Spain)
Natarajan, Saradha (India)
Natroshvili, David (Georgia)
Navada, Kodi Gowri (India)
Navarra-Madsen, Junalyn (USA)
Navarro Ajo, Antonio (Spain)
Navarro Garmendia, Alberto (Spain)
Navarro Garmendia, José (Spain)
Navarro Garulo, Gabriel (Spain)
Navarro Lérida, Maria Cruz (Spain)
Navarro Llinares, Juan F. (Spain)
Navarro Loidi, Juan (Spain)
Navas Flores, Andrés (Chile)
Navas Ureña, Juan (Spain)
Naya Fernández, Salvador (Spain)
Nebres, Father Ben (Phillippines)
Neeman, Amnon (Australia)
Neeman, Itay (USA)
Negreiros, Caio José Colletti (Brazil)
Nemenzo, Fidel (Phillippines)
Nemivroski, Arkadi (Israel)
Nerirosa, Otero (Puerto Rico)
Nesetril, Jaroslav (Czech Republic)
Neuberger, Barbara (USA)
Neuberger, John (USA)
Neunzert, Helmut (Germany)
Nevai, Andrew (USA)
Nevanlinna, Olavi (Finland)
Newman, Charles (USA)
Nezakati Rezazadeh, Ahmad (Iran)
Ng, Chi-Keung (P.R. China)
Ngo, Bao-Chau (France)
Nguyen An, Khuong (The Netherlands)
Nguyen, Dinh Cong (Vietnam)
Ngwa, Gideon Akumah (Cameroon)
Nicolau, Marcel (Spain)
Niederman, Laurent (France)
Nier, Francis (France)
Nieto Monje, Elena Sofia (Spain)
Nieto Roig, Juan José (Spain)
Nikolic, Aleksandar (Serbia & Montenegro)
Ninnemann, Olaf (Germany)
Nishimura, Jun-Ichi (Japan)
Niziol, Wieslawa (USA)
Nkemzi, Boniface (Cameroon)
Nobre, Sergio (Brazil)
Noda, Tomonori (Japan)
Noel, Alfred (USA)
Noel, Justin (USA)
Nolla de Celis, Álvaro (United Kingdom)
Noomene, Rouhia (Spain)
Novo, Vicente (Spain)
Nowak, Marian (Poland)
Nowroozi Larki, Farzaneh (Iran)
Noy, Marc (Spain)
Nualart, David (Spain)
Nualart, Joan (Spain)
Nunes, Guilherme (Brazil)
Núñez del Prado, José Antonio (Spain)
Núñez Rodríguez, Matías (France)
Núñez Valdés, Juan (Spain)
Núñez, Carmen (Spain)
Nuño Ballesteros, Juan José (Spain)

O´Farrell, Anthony (Ireland)
Oakes, Susan (United Kingdom)
Obada, Abdel-Shafy (Egypt)
Oberbroeckling, Lisa (USA)
Obitsu, Kunio (Japan)
Oda, Hiroshi (Japan)
Odai, Yoshitaka (Japan)
O'Donovan, Donal (Ireland)
Ogana, Wandera (Kenya)
Ogata, Shoetsu (Japan)
Oger, Francois (South Africa)
Oguiso, Keiji (Japan)
Oh, Yong-Geun (USA)
Oh, Young-Tak (South Corea)
Ohba, Kiyoshi (Japan)
Ohta, Shin-Ichi (Japan)
Oikkonen, Juha (Finland)
Ojeda Aciego, Manuel (Spain)
Ojeda Martínez de Castilla, Ignacio (Spain)
Okada, Masami (Japan)
Okada, Susumu (Spain)
Okada, Tatsuya (Japan)
Okayasu, Rui (Japan)
Okazaki, Ryotaro (Japan)
Okounkov, Andrei (USA)
Olajos, Peter (Hungary)

Oleaga, Gerardo (Spain)
Oliveira, Bruno M.P.M. (Portugal)
Oliverio, Paolo Antonio (Italy)
Olivieri Palmas, Aurora Alejandra (Venezuela)
Oller Marcén, Antonio (Spain)
Olmedo Zazo, Manuel (Spain)
Olteanu, Gabriela (Spain)
Ombrosi, Sheldy (Argentina)
Omolofe, Babatope (Nigeria)
Oniciuc, Cezar (Romania)
Ono, Kaoru (Japan)
Onshuus, Alf (Colombia)
Opdam, E.M. (The Netherlands)
Opozda, Barbara (Poland)
Oprisan, Alexandra (Romania)
Orden, David (Spain)
Orive, Rafael (Spain)
Orman V., Gabriel (Romania)
O'Rourke, Francesca (United Kingdom)
Ortega Martínez, Rafael (Spain)
Ortega, Rafael (Spain)
Ortigas Galindo, Jorge (Spain)
Ortiz, Eduardo (Spain)
Oruetxebarria, Osane (Spain)
Oset Sinha, Rául (Spain)
O'Shea, Donal (USA)
Osterwalder, Konrad (Switzerland)
Otal Germán, Antonio (Spain)
Otero Pardo, Ricardo (Spain)
Otero, Margarita (Spain)
Otrocol, Diana Ioana (Romania)
Otsuka, Kenichi (Japan)
Ouafi, Rachid (Algeria)
Ovando, Gabriela Paola (Argentina)
Owens, Brendan (USA)
Oyelami Oyediran, Benjamin (Nigeria)
Ozawa, Narutaka (Japan)
Ozeki, Michio (Japan)
Ozsváth, Peter (USA)
Öztop, Serap (Turkey)

Pablos Romo, Fernando (Spain)
Pacharoni, María Inés (Argentina)
Padrón, Edith (Spain)
Pae, Sung-Il (South Corea)
Paeng, Seong-Hun (South Corea)
Páez Jiménez, Alfredo (Spain)
Pais, Enno (Estonia)
Pal, Arup Kumar (India)
Palacios, Francisco (Spain)
Palis, Jacob (Brazil)
Palka, Karol (Poland)
Palmer, Jeffrey (Spain)
Panazzolo, Daniel (Brazil)
Pansuwan, Adoon (Thailand)
Parada Maroto, Oscar (Spain)
Paranjape, Kapil (India)
Paranjape, Shriram Dattatraya (India)
Paranpye, Avanti (USA)
Parcet, Javier (Spain)
Pardo Martín, Carlos (Spain)
Pardo Milanés, Alberto (Spain)
Pardo Serrano, Mario (Spain)
Pareja Tobes, Eduardo (Spain)
Pareja-Heredia, Diego (Colombia)
Parente Morales, Guadalupe (Spain)
Parés Mariné, Núria (Spain)
Pari, Abdón (Bolivia)
Pariguan, Eddy (Venezuela)
Park Koh, Kyewon (South Corea)
Park, Euisung (South Corea)
Park, Gi Hyun (South Corea)
Park, Hyungju (South Corea)
Park, Jongil (South Corea)
Park, Sung Ho (South Corea)
Parlier, Hugo (Spain)
Parmenter, Michael (Canada)
Parra Guevara, David (Mexico)
Parreño Navarro, José Joaquín (Spain)
Parthasarathi, Rangasamy (India)
Parumasur, Nabendra (South Africa)
Parviainen, Mikko (Finland)
Pascual Fuentes, Fernando (Spain)
Paseman, Gerhard (USA)
Passare, Mikael (Sweden)
Pataridis, Kostas (Spain)
Paternain, Gabriel (United Kingdom)
Patil, Dilip Kumar (India)
Paúl, Pedro J. (Spain)
Paveri-Fontana, Stefano (Italy)
Pavlovic, Natasa (USA)
Paxia, Giuseppe (Italy)
Payá, Rafael (Spain)
Paycha, Sylvie (France)
Paziy, Vadym (Spain)
Pe, María (Spain)
Pedraza Aguilera, Carmen (Spain)
Pedraza Aguilera, Tatiana (Spain)

Pedregal Tercero, Pablo (Spain)
Pedreira Mengotti, Alicia (Spain)
Peetta Kandy, Ratnakumar (India)
Peil, Matthias (Germany)
Peirone, Roberto (Italy)
Pekonen, Osmo (Finland)
Pelczar, Andrzej (Poland)
Peled, Ron (USA)
Peltonen, Kirsi (Finland)
Pender, Paris (USA)
Pensupha, Luddawan (Thailand)
Peña Alcaraz, Maite (Spain)
Peña Ferrández, Juan Manuel (Spain)
Peña Peña, Dixan (Belgium)
Peón Nieto, Ana (Spain)
Peral Alonso, Ireneo (Spain)
Peralta Guacheta, Blanca María (Colombia)
Perea Marco, Carmen (Spain)
Pereira, Jorge Vitorio (Brazil)
Perera, Francesc (Spain)
Pérez Alegre, Aranzazu (Spain)
Pérez Curiel, César (Spain)
Pérez de Pedro, Mª del Carmen (Spain)
Pérez de Vargas Luque, Alberto (Spain)
Pérez del Pozo, Ángel Luis (Spain)
Pérez del Río, Jesús S. (Spain)
Pérez Díaz, Sonia (Spain)
Pérez García, David (Spain)
Pérez García, Víctor Manuel (Spain)
Pérez Garrandés, Carlos (Spain)
Pérez González, Fernando (Spain)
Pérez González, Pilar (Spain)
Pérez Hornedo, Jesús (Spain)
Pérez Jiménez, Juan de Dios (Spain)
Pérez Jiménez, Sara (Spain)
Pérez Julián, Marina (Spain)
Pérez Lázaro, Francisco Javier (Spain)
Pérez Mansilla, Sonia (Spain)
Pérez Pérez, María Teresa (Spain)
Pérez Pla, José Francisco (Spain)
Pérez Quiles, María Jezabel (Spain)
Pérez Ramos, M. Dolores (Spain)
Pérez Riera, Mario (Spain)
Pérez Rodríguez, Daniel (Spain)
Pérez Rodríguez, Marta (Spain)
Pérez Ruiz, Diego Andrés (Mexico)
Pérez Sanz, Antonio (Spain)
Pérez Sinusía, Ester (Spain)
Pérez Velasco, Pedro Pablo (Spain)
Pérez, Carlos (Spain)
Pérez, Joaquín (Spain)
Pérez, Mª Eugenia (Spain)
Pérez, Sonsoles (Spain)
Pérez-Chavela, Ernesto (Mexico)
Pérez-López, Antonio (Spain)
Periago Esparza, Francisco (Spain)
Perisic, Dusanka (Serbia & Montenegro)
Perovic, Miodrag (Serbia & Montenegro)
Persson, Mikael (Sweden)
Persson, Ulf (Sweden)
Pervova, Ekaterina (Russian Federation)
Pestana Galván, Domingo (Spain)
Pete, Gabor (USA)
Petermichl, Stefanie (USA)
Peters, Martin (Germany)
Peterson, Janet (USA)
Petrova, Guergana (USA)
Petrovic, Ljiljana (Serbia & Montenegro)
Pevzner, Michael (France)
Pham-Gia, Thu (Canada)
Pianigiani, Giulio (Italy)
Picard, Dominique (France)
Piccione, Paolo (Brazil)
Piccioni, Mauro (Italy)
Picken, Roger (Portugal)
Pickering, Andrew (Spain)
Piedra, Ramón (Spain)
Piene, Ragni (Norway)
Pier, Jean-Paul (Luxembourg)
Pierantozzi, Teresa (Spain)
Pikovski, Alexander (Germany)
Pilipovic, Stevan (Serbia & Montenegro)
Pino Paulino, Sergi (Spain)
Pintado Jiménez, Fernando (Spain)
Pinto, Alberto Adrego (Portugal)
Pintz, Janos (Hungary)
Pinzón, Sofía (Colombia)
Piñera Nicolás, Alejandro (Spain)
Piñero Molano, Emilio (Spain)
Pirashvili, Teimuraz (United Kingdom)
Pireddu, Marina (Italy)
Pisante, Adriano (Italy)
Pisier, Gilles (France)
Pisonero Pérez, Miriam (Spain)
Pla Martos, Francisco (Spain)
Plato, Robert (Germany)
Plaumann, Daniel (Germany)
Polizzi, Francesco (Italy)

Pollington, Andrew (United Kingdom)
Polo Blanco, Irene (The Netherlands)
Ponosov, Arcady (Norway)
Popa, Sorin (USA)
Popovici, Adriana Florica (Romania)
Popovici, Dan Emanuel (Romania)
Porst, Hans E. (Germany)
Portilla Ferreira, Ana (Spain)
Porto Ferreira da Silva, Ana Mª (Spain)
Potapenko, Stanislav (Canada)
Potapov, Vadim (Russian Federation)
Pozo Coronado, Luis Miguel (Spain)
Pozo Montaño, Miguel (Spain)
Pozo Montero, Francesc (Spain)
Praeger, Cheryl (Australia)
Prajapat, Jyotshana (India)
Pranesachar, Chudamani (India)
Prastaro, Agostino (Italy)
Prats Fernández, Itziar (Spain)
Prestini, Elena (Italy)
Prieto, Ángeles (Spain)
Primo Ramos, Ana (Spain)
Privezentsev, Vladimir (Russian Federation)
Prokhorenkov, Igor (USA)
Prokopchuk, Alexandr (Belarus)
Promislow, David (Canada)
Prusiñska, Agnieszka (Poland)
Przytycki, Feliks (Poland)
Przytycki, Piotr (Poland)
Puel, Jean-Pierre (France)
Pujals, Enrique (Brazil)
Pujol, Gisela (Spain)
Pulvirenti, Mario (Italy)
Puthenpurakal, Tony (India)
Puusemp, Peeter (Estonia)
Py, Pierre (France)

Quarteroni, Alfio (Italy)
Quer Bosor, Jordi (Spain)
Quer, Lluís (France)
Quilez, Iñigo (Spain)
Quine, Jack (USA)
Quintana Portilla, Gema R. (Spain)
Quintana, Yamilet (Venezuela)
Quintero, Antonio (Spain)
Quintero, Roy (Venezuela)
Quirós Gracián, Adolfo (Spain)
Quirós Gracián, Fernando (Spain)

Raczynski, Andrzej (Poland)
Radulescu, Marius (Romania)
Raghunathan, Madabusi S. (India)
Rahimi, Hamidreza (Iran)
Raitums, Uldis (Latvia)
Rajola, Sandro (Italy)
Raka, Madhu (India)
Rakic, Zoran (Serbia & Montenegro)
Rakotondrajao, Fanja (Madagascar)
Ralston, Anthony (USA)
Ramachandran, Balasubramanian (India)
Ramagge, Jacqui (Australia)
Rambla Barreno, Fernando (Spain)
Ramírez González, Victoriano (Spain)
Ramírez Uclés, Rafael (Spain)
Ramos González, Marta (Spain)
Ramos Maravall, Javier (Spain)
Ramos San Millán, Lorena (Spain)
Ramos, Pedro A. (Spain)
Ran, Andre (The Netherlands)
Rangarajan, Govindan (India)
Rangel Oliveros, Yenny (Spain)
Rappoport, Juri M. (Russian Federation)
Rasila, Antti (Finland)
Rasmussen, Jesper (Denmark)
Rassias, Michael (Greece)
Rassias, Themistocles (Greece)
Rathjen, Michael (USA)
Raugel, Geneviève (France)
Raventós, Oriol (Spain)
Ravi, Sreenivasan (India)
Rayskin, Victoria (Germany)
Real, Christophe (France)
Reankittiwat, Paramee (Thailand)
Recamán Santos, Bernardo (Colombia)
Recio, Tomás (Spain)
Redondo Buitrago, Antonia (Spain)
Reed, Jon (Norway)
Rees, Elmer (United Kingdom)
Rees, Mary (United Kingdom)
Rege, Mangesh B. (India)
Regensburger, Georg (Austria)
Regis, Goiffon (France)
Reguero Guerra, Lorena (Spain)
Rehmann, Ulf (Germany)
Reich, Holger (Germany)
Reinfelds, Andrejs (Latvia)
Reingold, Omer (Israel)
Reiten, Idun (Norway)

Reiterer, Michael (Italy)
Remón, Dionís (Spain)
Renchin-Ochiri, Mijiddorjj (Mongolia)
Rendall, Alan (Germany)
Renedo Pedrajas, José Luis (Spain)
Rentsen, Enkhbat (Mongolia)
Resende, Pedro (Portugal)
Restrepo, Guillermo (Colombia)
Reventós Tarrida, Agustí (Spain)
Rey Alcántara, Patricia (Spain)
Rey Ley, Guillermo (Spain)
Rey, José Manuel (Spain)
Reyes Castro, Miguel (Spain)
Reyes Iglesias, María Encarnación (Spain)
Reyes Mata, Rocío (Spain)
Reyes Salguero, Elía (Spain)
Reyes Souto, Guillermo (Spain)
Reynoso Alcántara, Claudia (Mexico)
Rezola, M. Luisa (Spain)
Riaza, Ricardo (Spain)
Ribes, Luis (Canada)
Ríder Moyano, Alfonso (Spain)
Riera Burger, Constanza (Norway)
Riley, Timothy (USA)
Rincón, Luis (Mexico)
Ringel, Claus Michael (Germany)
Riordan, Oliver (United Kingdom)
Ríos Fachal, Matilde (Spain)
Ríos, Cristian (USA)
Risueño Pérez, Carlos (Spain)
Ritoré, Manuel (Spain)
Rittatore, Álvaro (Uruguay)
Rivero García, Luis Felipe (Spain)
Riveros, María Silvina (Argentina)
Roath, Chan (Cambodia)
Robbiano, Luc (France)
Robinson, Ben-Zion (Israel)
Robles Arredondo, Gabriela (Mexico)
Rocchi, Paolo (Italy)
Rocha Martín, Juan (Spain)
Rochon, Frederic (USA)
Roczen, Marko (Germany)
Rodnianski, Igor (USA)
Rodrigues Faustino, Nelson José (Portugal)
Rodrigues, José Francisco (Portugal)
Rodríguez Álvarez, Margarita (Spain)
Rodríguez Arbeo, Sergio (Spain)
Rodríguez Arós, Ángel Daniel (Spain)
Rodríguez Bellido, María Ángeles (Spain)
Rodríguez Blancas, José Luis (Spain)
Rodríguez Blanco, Guillermo (Colombia)
Rodríguez Buitrago, Carlos J. (Spain)
Rodríguez Castaño, David (Spain)
Rodríguez de la Peña, Thalía (Spain)
Rodríguez del Río, Roberto (Spain)
Rodríguez García, José Manuel (Spain)
Rodríguez Guerrero, Marta (Spain)
Rodríguez Hertz, Federico (Uruguay)
Rodríguez Hertz, Mª Alejandra (Spain)
Rodríguez López, Jesús (Spain)
Rodríguez Luján, Irene (Spain)
Rodríguez Méndez, José Ángel (Spain)
Rodríguez Mielgo, César (Spain)
Rodríguez Pérez, M. Magdalena (Spain)
Rodríguez Piazza, Luis (Spain)
Rodríguez Rodríguez, Arturo (Spain)
Rodríguez Salazar, Soledad (Spain)
Rodríguez Sánchez, Cristina (Spain)
Rodríguez Sanjurjo, José Manuel (Spain)
Rodríguez Santamaría, Ana (Spain)
Rodríguez Soler, Javier (Spain)
Rodríguez Uría, Maria Victoria (Spain)
Rodríguez Velázquez, Juan Alberto (Spain)
Rodríguez, Francisco (Spain)
Rodríguez, Gerardo (Spain)
Rodríguez, María Elena (Spain)
Rodríguez, Miguel A. (Spain)
Rodríguez-Moldes Rey, Covadonga (Spain)
Rogers, Keith (Spain)
Roig, Abdo (Spain)
Rojas León, Antonio (USA)
Rojas Matas, Ángela (Spain)
Rojas Monroy, Rocío (Mexico)
Rojas-Medar, Marko (Brazil)
Roldán López de Hierro, Concepción (Spain)
Romance del Río, Miguel (Spain)
Romera Colmenarejo, Elena (Spain)
Romero Álvarez, Natalia (Spain)
Romero Avello, César (Spain)
Romero Fuster, Mª Carmen (Spain)
Romero Ibáñez, Ana (Spain)
Romero Laorden, David (Spain)
Romero Olivares, Esther (Spain)
Romero Sánchez, Natalia (Spain)
Romero Sánchez, Pantaleón David (Spain)
Rondero Guerrero, Carlos (Mexico)
Ronzhin, Alexandr (Russian Federation)
Ropchan, Carmen (Canada)

Rordam, Mikael (Denmark)
Ros, Antonio (Spain)
Rosado Linares, Jesús (Spain)
Rosado, Mª Eugenia (Spain)
Rosales Lombardo, M. César (Spain)
Rosenschon, Andreas (USA)
Rosón Trespalacios, José (Spain)
Rosselló Llompart, Francesc (Spain)
Rossi, Julio D. (Spain)
Rothschild, Linda (USA)
Roughgarden, Tim (USA)
Rouquier, Rápale (France)
Rousseau, Christiane (Canada)
Rovenski Yu, Vladimir (Israel)
Rovira Escofet, Carles (Spain)
Roy, Marie-Francoise (France)
Roy, Rahul (India)
Royo Regueiro, María Pilar (Spain)
Ruan, Qihua (P.R. China)
Ruano Sáinz, Susana (Spain)
Ruano, Diego (Spain)
Rubashkina, Elena (Russian Federation)
Rubinfeld, Ronitt (USA)
Rubio Crespo, María Jesús (Spain)
Rubió Pons, Llorenç (Spain)
Rubio Ruiz, Rafael María (Spain)
Rubio Segovia, Baldomero (Spain)
Rubio, Roberto (Spain)
Rubtsov, Konstantin (Russian Federation)
Ruddy, David (USA)
Rué Perna, Juanjo (Spain)
Rueda, Sonia l. (Spain)
Ruesga, Pilar (Spain)
Ruiz Calvo, Manuel (Spain)
Ruiz del Portal, Francisco R. (Spain)
Ruiz González, Alberto (Spain)
Ruiz Gordoa, Pilar (Spain)
Ruiz López, Natalia (Spain)
Ruiz Morcillo, Víctor Manuel (Spain)
Ruiz, Ceferino (Spain)
Ruiz, Jesús M. (Spain)
Ruiz-Rivas, Carmen (Spain)
Russo, Remigio (Italy)
Rustarazo, Patricia (Spain)
Ruzsa, Imre (Hungary)
Ryabov, Alexey (Germany)
Rybicki, Tomasz (Poland)

Saà, Joel (Spain)
Saadetoglu, Muge (Turkish Cyprus)
Sabatti, Chiara (USA)
Sabina de Lis, José (Spain)
Sablonniere, Paul (France)
Saboya Baquero, Martha (Spain)
Sacchetti, Andrea (Italy)
Sad, Ligia Arantes (Brazil)
Sadallah, Boubaker (Algeria)
Sadornil Renedo, Daniel (Spain)
Saez Beltrán, Moises (Spain)
Sáez Schwedt, Andrés (Spain)
Sagredo Sánchez, Lucía (Spain)
Sahoo, Binod Kumar (India)
Sahraoui, Fatiha (Algeria)
Saifi, Ali (United Arab Emirates)
Saifullah, Khalid (Pakistan)
Saikia, Anupam (India)
Sakai, Fumio (Japan)
Sakakibara, Nobuhisa (Japan)
Sakasai, Takuya (Japan)
Sala Siscar, Josep Vicent (Spain)
Salafranca Laforga, Rafael (Spain)
Salas, Héctor (Puerto Rico)
Saleem, Mohammad (Japan)
Saleri, Fausto (Italy)
Salvador González, Alfredo (Spain)
Salvai, Marcos (Argentina)
Salvarani, Francesco (Italy)
Salvetti, Mario (Italy)
Samadi, Sedki (Spain)
Samian, A. Latif (Malaysia)
Samoylovich, Mikhail (Russian Federation)
Samuel, Joseph (India)
San Antolín, Ángel (Spain)
San Ginés Ruiz, Aranzazu (Spain)
San José Martínez, Fernando (Spain)
San Martín Alarcia, Carmen (Spain)
San Segundo, Fernando (Spain)
Sanabria Codesal, Esther (Spain)
Sánchez Altozano, Sonia (Spain)
Sánchez Ávila, Carmen (Spain)
Sánchez Benito, M. Mercedes (Spain)
Sánchez Caja, Miguel (Spain)
Sánchez del Pozo, Mª del Pilar (Spain)
Sánchez Gabites, Jaime Jorge (Spain)
Sánchez García, Rubén (United Kingdom)
Sánchez García, Sergio (Spain)
Sánchez Gil, Lidia (Spain)
Sánchez Giralda, Tomás (Spain)

Sánchez Gómez, Gema (Spain)
Sánchez Iglesias, Adela (Spain)
Sánchez Lajusticia, Luis (Spain)
Sánchez Martín, Elisa (Spain)
Sánchez Migallón Cano, Mara (Spain)
Sánchez Morgado, Héctor (Mexico)
Sánchez Ortega, Juana (Spain)
Sánchez Palacio, José Luis (Spain)
Sánchez Rodríguez, Estela (Spain)
Sánchez Sánz, Julia (Spain)
Sánchez Sánz, Urko (Spain)
Sánchez Valdés, Ariel (Spain)
Sánchez Villaseñor, Eduardo Jesús (Spain)
Sánchez, Eva (Spain)
Sánchez-Lirola Ortega, María Gracia (Spain)
Sánchez-Ruiz, Jorge (Spain)
Sandberg, Oskar (Sweden)
Sane, Sharad (India)
Sangroniz Gómez, José (Spain)
Sankaran, Parameswaran (India)
Santa-María Megía, Ignacio (Spain)
Santamaría Sánchez, Rafael (Spain)
Santiago del Río, Pedro María (Spain)
Santiago Fernández, Jorge (Spain)
Santonja Gómez, Francisco José (Spain)
Santos Alaez, Evangelina (Spain)
Santos Barradas, Ismael (Spain)
Santos Santiago, Paz (Spain)
Santos, Francisco (Spain)
Sanugi, Bahrom (Malaysia)
Sanz Aguado, Ángel (Spain)
Sanz Alix, Miguel (Spain)
Sánz Alonso, Beatriz (Spain)
Sanz Ferrer, Fernando (Spain)
Sanz Gil, Javier (Spain)
Sanz, Ana María (Spain)
Sanziel, María Cristina (Argentina)
Sanzo Curran, Patrick (Spain)
Sanz-Serna, Jesús María (Spain)
Sanz-Solé, Marta (Spain)
Saorín Castaño, Manuel (Spain)
Sapir, Jenya (USA)
Sapir, Mark (USA)
Saraiva, Luis (Portugal)
Saravanan, Jeya Bharathi (India)
Sarkar, Jaydeb (India)
Sarkar, Rudra Pada (India)
Sarma, Bhaba Kumar (India)
Sarma, Ritumoni (India)
Sarnak, Peter (USA)
Sastre Gómez, Silvia (Spain)
Sastre Rosa, Mª Asunción (Spain)
Sastri, Chelluri C.A. (Canada)
Sasyk, Roman (USA)
Satkurunath, Ramesh (United Kingdom)
Satoh, Takao (Japan)
Sauzin, David (France)
Savin, Anton (Russian Federation)
Savin, Ovidiu (USA)
Savo, Alessandro (Italy)
Sawae, Ryuichi (Japan)
Sawano, Yoshihiro (Japan)
Sawon, Justin (USA)
Sbordone, Carlo (Italy)
Scanlon, Thomas (USA)
Schappacher, Norbert (France)
Schaps, Mary (Israel)
Scherbakov, Eugeniy Aleksandrovich (Russian Federation)
Scherr, Constantin (Germany)
Schleicher, Dierk (Germany)
Schmickler-Hirzebruch, Ulrike (Germany)
Schmid, Wilfried (USA)
Schmidt, William (USA)
Schmitt, Peter (Austria)
Schneider, Peter (Germany)
Schönlieb, Carola-Bibiane (Austria)
Schramm, Oded (USA)
Schreiber, Bertram (USA)
Schultens, Jennifer (USA)
Schulze-Halberg, Axel (Mexico)
Schwartz, Fernando (USA)
Schweigert, Christoph (Germany)
Schweitzer, Pascal (Germany)
Scriven, Neil (United Kingdom)
Sebastián Benito, Alberto Ricardo (Spain)
Sebastián Gómez, Alberto (Spain)
Seco Forsnacke, Daniel (Spain)
Seco Revilla, Luis Ángel (Canada)
Sedó Torres, Leonor (Spain)
Seiler, Ruedi (Germany)
Seiler, Wolfgang K. (Germany)
Selinger, Nikita (Germany)
Semenov, Vasyl (Ukraine)
Semenovich Holevo, Alexander (Russian Federation)
Semião, Paulo (Portugal)
Sempere Montero, Lourdes (Spain)

Sendra Pons, Juana (Spain)
Sendra, Juan Rafael (Spain)
Sengupta, Indranath (India)
Seok Woo, Kim (South Corea)
Seppälä, Mika (Finland)
Seress, Akos (USA)
Serfaty, Sylvia (USA)
Serna Cabeza, Mª del Pilar (Spain)
Serra Fuster, Rafael (Spain)
Serra, Oriol (Spain)
Serrano, Helia (Spain)
Serrat Piè, Carles (Spain)
Sertoz, Ali Sinan (Turkey)
Sevenster, Arjen (The Netherlands)
Sever Silvestru, Dragomir (Australia)
Sevilla Ramírez, Juan Manuel (Spain)
Shadmi, Doron (Israel)
Shalom, Yehuda (Israel)
Shamarova, Evelina (Germany)
Sharaffedin, Ahmad (Iran)
Sharma, Anuradha (India)
Shatz, Stephen (USA)
Shaw, Sen-Yen (Taiwan)
Shawagfeh, Nabil (Jordan)
Shen, Jian (Spain)
Shi, Xiquan (USA)
Shibano, Hiroki (Japan)
Shiga, Hironori (Japan)
Shikare, Maruti (India)
Shin, Sugwoo (USA)
Shiraiwa, Kenichi (Japan)
Shishikura, Mitsuhiro (Japan)
Shmarev, Sergey (Spain)
Sholapurkar, Vinayak (India)
Shorey, Tarlok Nath (India)
Shorikov, Andrey (Russian Federation)
Shoytov, Alexander (Russian Federation)
Shrivastava, Manjulata (India)
Shub, Michael (Canada)
Shubin, Mikhail (USA)
Shubladze, Mamuka (Georgia)
Shutyaev, Victor (Russian Federation)
Sic García, Ángel Roberto (Guatemala)
Siddiqi, Abul Hasan (Saudi Arabia)
Sidi Ammi, Moulay Rchid (Portugal)
Siegel, Alan (USA)
Sierra Vázquez, Vicente (Spain)
Sierra, Germán (Spain)
Sigarreta Almira, José María (Spain)
Sigmund, Karl (Austria)
Signes, Teresa (Spain)
Siguero Chinchilla, Ana Isabel (Spain)
Sikorav, Jean-Claude (France)
Siles Molina, Mercedes (Spain)
Simic, Slavko (Serbia & Montenegro)
Simon, László (Hungary)
Simon, Peter (Hungary)
Simons, Gord (Canada)
Singerman, David (United Kingdom)
Singh Laishram, Shanta (India)
Singh, Anupam Kumar (India)
Singh, Mansa (Canada)
Singh, S.V. (India)
Siqveland, Arvid (Norway)
Siu, Man Keung (P.R. China)
Sivak-Fischler, Jimena (France)
Skopina, Maria (Russian Federation)
Skvortsov, Valentin (Russian Federation)
Slavova, Angela (Bulgary)
Sletsjøe, Arne B. (Norway)
Sloan, Ian (Australia)
Slominska, Jolanta (Poland)
Smajlovic, Lejla (Bosnia & Herzegovina)
Smania Brandao, Daniel (Brazil)
Smirnov, Eugeny (Russian Federation)
Smirnov, Stanislav (Switzerland)
Smith, Stuart (USA)
Smoktunowicz , Agata (United Kingdom)
Snoussi, Jawad (Mexico)
Soblechero, Ana (Spain)
Soffer, Abraham (USA)
Sofi, Mohammad Amin (India)
Soheili, Ali Reza (Iran)
Sohn, Sung Ik (South Corea)
Sokolov, Maksim (Uzbekistán)
Sola Ortiz, Cristina (Spain)
Solà-Morales Rubió, Juan (Spain)
Solbes Castro, Lucía (Spain)
Solla, Antonio (Spain)
Sols Lucia, Ignacio (Spain)
Somaskandan, Kumaresan (India)
Son, Nguyen Khoa (Vietnam)
Sonn, Jack (Israel)
Soria de Diego, F. Javier (Spain)
Soria, Fernando (Spain)
Soriano García, Yolanda (Spain)
Sorli, Ronald (Australia)
Sós, Vera T.(Hungary)

Sosa Martín, Diana de las Nieves (Spain)
Sossinsky, Alexei (Russian Federation)
Soto Bajo, Moisés (Spain)
Soto Monge, Beatriz (Spain)
Soto Uruñuela, Marta Parrales (Spain)
Soto-Andrade, Jorge (Chile)
Soudry, David (Israel)
Soydan, Gôkhan (Turkey)
Spaggiari, Fulvia (Italy)
Speh, Birgit (USA)
Spence, Stephen (Spain)
Spencer, Mark (USA)
Spencer, Thomas (USA)
Sprekels, Jürgen (Germany)
Srinivas, Vasudevan (India)
Srinivasan, Anitha (India)
Srinivasan, Kesavan (India)
Srinivasan, Natesan (India)
Srivastava, Sashi Mohan (India)
Staffans, Olof (Finland)
Stahl, Herbert (Germany)
Stana, Nikcevic (Serbia & Montenegro)
Stancu, Alina (Canada)
Staniszewski, Michal (Poland)
Stanley, Richard P. (USA)
Starita, Giulio (Italy)
Stauch, Marika (Germany)
Steinby, Paula (Finland)
Steinhorn, Charles (USA)
Stekolshchik, Rafael (Israel)
Stern, Ronald (USA)
Sternheimer, Daniel (France)
Steuding, Joern (Germany)
Steuding, Rasa (Spain)
Stoll, Carina (Germany)
Storozhuk, Konstantin (Russian Federation)
Stosic, Marko (Portugal)
Straube, Emil (USA)
Stray, Arne (Norway)
Strazzabosco, Barbara (Germany)
Strooker, Jan R. (The Netherlands)
Strunkov, Sergey (Russian Federation)
Stukow, Michal (Poland)
Suárez Granero, Antonio (Spain)
Suárez Serrato, Pablo (United Kingdom)
Sudbery, Anthony (United Kingdom)
Sugahara, Kunio (Japan)
Suh, Dong Youp (South Corea)
Suli, Endre (United Kingdom)
Sullivan, John (Germany)
Sumi, Hiroki (Japan)
Sushch, Volodymyr (Poland)
Susi García, Rosario (Spain)
Susperregui Lesaca, Julián (Spain)
Suzuki, Noriaki (Japan)
Svrtan, Dragutin (Croatia)
Szabó, Zoltán (USA)
Szaniszlo, Zsuzsanna (USA)
Szarek, Stanislaw (France)
Szepessy, Anders (Sweden)
Sznitman, Alain-Sol (Switzerland)
Ta, Thi Hoai An (Vietnam)
Tabarintseva, Elena Vladimirovna (Russian Federation)
Tabera, Luis (Spain)
Tabernero Guzmán, Hugo (Spain)
Tachizawa, Kazuya (Japan)
Tadmor, Eitan (USA)
Taduri Rao, Srinivasa Siva Rama Krishna (India)
Taft, Earl (USA)
Tajvidi, Nader (Sweden)
Takahashi, Atsushi (Japan)
Takahashi, Takéo (France)
Takakura, Tatsuru (Japan)
Takayama, Manabu (Japan)
Takayama, Nobuki (Japan)
Takenouchi, Yoshifumi (Phillippines)
Takesaki, Masamichi (Japan)
Tamaru, Hiroshi (Japan)
Tamburini, Maria Clara (Italy)
Tamm de Araujo Moreira, Carlos Gustavo (Brazil)
Tanaka, Kokoro (Japan)
Tanbay, Betül (Turkey)
Tandon, Rajat (India)
Tandra, Haryono (Indonesia)
Tanoglu, Gamze (Turkey)
Tao, Jing (USA)
Tao, Terence (USA)
Tareghian, Hamed Reza (Iran)
Tarieladze, Vaja (Spain)
Tarrío Quintela, José Carlos (Spain)
Tasaki, Hiroyuki (Japan)
Tatjer, Joan Carles (Spain)
Tauste Campo, Adria (Spain)
Taya, Hisao (Japan)
Taylor, Dewey (USA)

Taylor, Richard (United Kingdom)
Tchantcho, Bertrand (Cameroon)
Tchuenche, Jean Michel (Tanzania)
Te Riele, Herman (The Netherlands)
Teicher, Mina (Israel)
Tejada, Juan (Spain)
Tejero Prieto, Carlos (Spain)
Tellechea Armenta, Eduardo (Mexico)
Temirgaliyev, Nurlan (Kazakhstan)
Temlyakov, Vladimir (USA)
Tena Ayuso, Juan (Spain)
Tengely, Szabolcs (Hungary)
Tent i Jorques, Joan Francesc (Spain)
Teo, Lee-Peng (Malaysia)
Terai, Nobuhiro (Japan)
Terakawa, Hiroyuki (Japan)
Terasawa, Yutaka (Japan)
Terasoma, Tomohide (Japan)
Terman, David (USA)
Terng, Chuu-Lian (USA)
Terrés, Raquel (Spain)
Tetjana, Eisner (Germany)
Thas A., Joseph (Belgium)
The Long, Pham (Vietnam)
Theobald, Thorsten (Germany)
Thiele, Christoph (USA)
Thilikos, Dimitrios (Greece)
Thomas, Janet (Australia)
Thomas, Robin (USA)
Thomas, Simon (USA)
Thomé, Michel (France)
Thomsen, Momme Johs (Germany)
Tikhonov, Sergey (Spain)
Tillmann, Ulrike (United Kingdom)
Timofte, Aida-Mirela (Germany)
Timoney, Richard (Ireland)
Tindel, Samy (France)
Tiraboschi, Alejandro (Argentina)
Tirumalasetty, Amaranath (India)
Tisseyre, François (France)
Tocón Barroso, Maribel (Canada)
Toda, Yukinobu (Japan)
Todd, Michael (United Kingdom)
Todjihounde, Léonard (Benin)
Todorov, Ivan (United Kingdom)
Toerner, Guenter (Germany)
Tojeiro, Ruy (Brazil)
Toland, John (United Kingdom)
Toledo Romero, Jesús (Spain)
Tolsa, Xavier (Spain)
Tomás Estevan, Virtudes (Spain)
Tomazella, João Nivaldo (Brazil)
Tondeur, Philippe (USA)
Tonegawa, Yoshihiro (Japan)
Tong, Anna Sea-Lin (Singapore)
Tonks, Andrew Peter (United Kingdom)
Ton-That, Tuong (USA)
Topping, Peter (United Kingdom)
Topsøe, Flemming (Denmark)
Torisu, Ichiro (Japan)
Tornaría, Gonzalo (Uruguay)
Torrea, José Luis (Spain)
Torrecilla-Tarantino, Iván (Spain)
Torres Gutiérrez, Nuria (Spain)
Torres Martín, Eugenia (Spain)
Torres Pérez, Marta (Spain)
Torres Téigell, David (Spain)
Torres-Hernández, Roberto (Mexico)
Tosatti, Valentino (USA)
Totaro, Burt (United Kingdom)
Toure, Saliou (Ivory Coast)
Touris Lojo, Eva (Spain)
Toussaint, Godfried (Canada)
Tovar Sánchez, Luis Manuel (Mexico)
Tovio Ciercoles, Víctor (Spain)
Tradacete Pérez, Pedro (Spain)
Travesa, Artur (Spain)
Tretiakov, Alexey (Poland)
Trevisan, Luca (USA)
Trillo Moya, Juan Carlos (Spain)
Trivisa, Constantina (USA)
Trobajo de las Matas, Mª Teresa (Spain)
Tronel, Gerard (France)
Trudinger, Neil (Australia)
Trujillo Jacinto del Castillo, Juan J. (Spain)
Truong, May (Australia)
Tschinkel, Yuri (Germany)
Tseng, Shiojenn (Taiwan)
Tsigoni, Anastasia (Greece)
Tsou, Sheung Tsun (United Kingdom)
Tsuboi, Takashi (Japan)
Tsuchiya, Nobuo (Japan)
Tsuda, Ei (Japan)
Tsugawa, Kotaro (Japan)
Tsushima, Ryuji (Japan)
Tumarkin, Pavel (Russian Federation)
Tunc, Cemil (Turkey)
Turiel, Francisco Javier (Spain)

Turner, Edward (USA)
Tuset, Lars (Norway)
Tuzhilin, Mikhail (Russian Federation)
Tylli, Hans-Olav (Finland)

Úbeda García, José I. (Spain)
Úbeda Rives, José P. (Spain)
Ubis Martínez, Adrián (Spain)
Uchiyama, Atsushi (Japan)
Uchiyama, Mitsuru (Japan)
Udaya Kovilakath, Anandavardhanan (India)
Udomene, Aniefiok (Italy)
Udriste, Constantin (Romania)
Ueno Jacue, Carlos (Spain)
Ueno, Kenji (Japan)
Uesu, Hiroaki (Japan)
Ulecia García, Mª Teresa (Spain)
Umemura, Hiroshi (Japan)
Ungureanu, Viorica (Romania)
Upadhye, Chandraprabha (India)
Urban, Eric (USA)
Urbano, Francisco (Spain)
Urbina, Wilfredo (Venezuela)
Ures, Raúl (Uruguay)
Ushio, Keizo (Japan)
Usnich, Alexandr (France)
Uteshev, Alexei (Russian Federation)
Uusipaikka, Esa (Finland)

Vaccarino, Francesco (Italy)
Valdecantos Dema, Mª Teresa (Spain)
Valdivia Pérez, Fabián (Mexico)
Valencia Vizcaino, Pedro Francisco (Mexico)
Valero, Isaac (Spain)
Valette, Alain (Switzerland)
Vallejo, Ernesto (Mexico)
Van de Weyer, Geert (Belgium)
Van der Hoeven, Joris (France)
Van der Kallen, Wilberd (The Netherlands)
Van der Poorten, Alfred J. (Australia)
Van der Put, Marius (The Netherlands)
Van der Schaft, Arjan (The Netherlands)
Van Frankenhuijsen, Machiel (USA)
Van Steirteghem, Bart (Portugal)
Van Wyk, Leon (South Africa)
Vanninathan, Muthusamy (India)
Varga, Zoltán (Hungary)
Vargas Mendoza, José (Mexico)
Vargas, Ana (Spain)
Vargas, Edson (Brazil)
Vargas, Jorge Antonio (Argentina)
Varju, Peter P. (Hungary)
Varona Malumbres, Juan Luis (Spain)
Varvaruca, Eugen (United Kingdom)
Varvaruca, Lorina (United Kingdom)
Vasilieva, Olga (Colombia)
Vassiliev, Victor A. (Russian Federation)
Vatsal, Vinayak (Canada)
Vaz, Pedro (Portugal)
Vazirani, Mónica (USA)
Vázquez Corral, Javier (Spain)
Vázquez Furelos, Mercedes (Spain)
Vázquez González, Leonor (Spain)
Vázquez Martínez, Luis (Spain)
Vázquez, Juan Luis (Spain)
Vázquez-Abal, María Elena (Spain)
Vecina Jiménez, José María (Spain)
Vega García, Bonifacio (Spain)
Vega Vicente, Pilar (Spain)
Vega, José M. (Spain)
Vega, Luis (Spain)
Vela Hernández, Manuela (Spain)
Vela Pérez, María (Spain)
Vela, Montserrat (Spain)
Velasco Recrían, María Pilar (Spain)
Velázquez, Juan L. (Spain)
Velimirovic, Ljubica (Serbia & Montenegro)
Veloso, José Miguel (Brazil)
Vendrell Simón, Josep Mª (Spain)
Venema, Gerard (USA)
Ventura, Enric (Spain)
Vera de Serio, Virginia Norma (Argentina)
Vera, Daniel (Spain)
Verdera, Joan (Spain)
Verdugo Díaz, Julieta (Mexico)
Verelst, Karin (Belgium)
Vergne, Michèle (France)
Verjovsky, Alberto (Mexico)
Verma, Jugal (India)
Verrill-Schlichting, Helena (USA)
Vershinin, Vladimir (France)
Vesztergombi, Katalin (USA)
Veys, Willem (Belgium)
Viana, Marcelo (Brazil)
Viaño, Juan Manuel (Spain)
Vicente Matilla, Pilar (Spain)
Vicente, Miquel Molina (Spain)
Victoria de la Iglesia Meleiro, Coral (Spain)

Vidal Díez de Ulzurrun, Guillermo (Spain)
Vidal Vázquez, Ricardo (Spain)
Vielhaber, Michael (Chile)
Vigara Benito, Rubén (Spain)
Vigon, Vincent (France)
Vikraman, Balaji (Spain)
Vikraman, Uma (India)
Vilas Prieto, José Luis (Spain)
Vílchez Gómez, María Fátima (Spain)
Villacampa Gutiérrez, Raquel (Spain)
Villamayor, Orlando (Spain)
Villani, Cédric (France)
Villanueva García, José David (Spain)
Villar Santos, Jorge Luis (Spain)
Villatoro Machuca, Francisco R. (Spain)
Villegas, Salvador (Spain)
Villén Pizarro, Antonio (Spain)
Vinuesa del Río, Carlos (Spain)
Viña, Andrés (Spain)
Viola, Carlo (Italy)
Viro, Oleg (Sweden)
Vishne, Uzi (Israel)
Vives, Joseph (Spain)
Vivo Molina, Juana María (Spain)
Vodopyanov, Sergey (Russian Federation)
Vogtmann, Karen (USA)
Voisin, Claire (France)
Vojtechovsky, Petr (USA)
Volic, Ismar (USA)
Volk, Wolfgang (Germany)
Von Mouche, Pierre (Nederlandse Antillen)
Von Renteln, Michael (Germany)
Von Wuthenau, Sebastian (Mexico)
Vorobiev, Yury (Mexico)
Vukotic Jovsic, Dragan (Spain)
Vukovic, Mirjana (Bosnia & Herzegovina)

Wagner, Dominique (Spain)
Walias Cuadrado, Magdalena (Spain)
Walker, James (USA)
Wan Soon, Kim (North Corea)
Wang, Bin (USA)
Wang, Erxiao (USA)
Wang, Hwai-Chiuan (Taiwan)
Wang, Shicheng (P.R. China)
Wang, Shin-Hwa (Taiwan)
Wang, Weichung (Taiwan)
Webster, Benjamin (USA)
Wegner, Bernd (Germany)
Weibel, Charles (USA)
Weiss, Michael (United Kingdom)
Wen, Lan (P.R. China)
Werner, Wendelin (France)
Wibmer, Michael (Austria)
Wiegerinck, Jan (The Netherlands)
Wiegmann, Paul (USA)
Wigderson, Avi (USA)
Wilking, Burhard (Germany)
Will, Cynthia (Argentina)
Williams, Lauren (USA)
Wills Toro, Luis Alberto
(United Arab Emirates)
Wilson, John (United Kingdom)
Winitzky de Spinadel, Vera Martha (Argentina)
Winkel, Matthias (United Kingdom)
Winther, Ragnar (Norway)
Wlodarczyk, Jaroslaw (USA)
Wolf, Julia (United Kingdom)
Wolfart, Jürgen (Germany)
Wood, David (Spain)
Wouts, Marc (Falkland Islands)
Wright, James (United Kingdom)
Wright, Margaret H. (USA)
Wu, de Ting (USA)
Wu, Hansheng (Japan)
Wu, Hung-Hsi (USA)
Wulfsohn, Aubrey (United Kingdom)
Wunderli, Thomas (United Arab Emirates)

Xambó, Sebastiá (Spain)
Xenophontos, Christos (Cyprus)
Xie, Shishen (USA)

Yadav, Rajendra Kumar (India)
Yagasaki, Tatsuhiko (Japan)
Yaguchi, Teruo (Japan)
Yakubov, Yakov (Israel)
Yamada, Kotaro (Japan)
Yamashita, Go (France)
Yan, Baisheng (USA)
Yan, Min (Hong-Kong)
Yanaba, Hiroko (Japan)
Yanai, Kana (Japan)
Yanchevskii, Vyacheslav (Belarus)
Yannacopoulos, Athanasios (Greece)
Yao, Guowu (P.R. China)
Yao, Xin (Germany)
Yasuda, Takehiko (Japan)

Yasutoshi , Nombra (Japan)
Yazdani, Alireza (United Kingdom)
Yeh, Fang-Bo (Taiwan)
Yeh, Lina (Taiwan)
Yeh, Yeong-Nan (Taiwan)
Yera Gracia, Isabel (Spain)
Ying, Daniel (Sweden)
Ylinen, Kari (Finland)
Yoneda, Tsuyoshi (Japan)
Yoshinaga, Masahiko (Italy)
Yu, Chia-Fu (Taiwan)
Yu, Guoliang (USA)
Yu, Jeong Youn (South Corea)
Yu, Josephine (USA)
Yu, Roger (P.R. China)
Yuste Leciñena, Piedad (Spain)

Zacarés González, Mario (Spain)
Zádník, Vojtech (Czech Republic)
Zaharopol, Radu (USA)
Zaitsev, Dmitri (Ireland)
Zalama Hernández, Débora (Spain)
Zaldivar, Felipe (Mexico)
Zamarro de Santos, Mª Carmen (Spain)
Zangeneh, Bijan (Iran)
Zapatero Cabañas, Elena (Spain)
Zarate, María José (Spain)
Zarco García, Ana María (Spain)
Zare Firoozabadi, Sanaz (Iran)
Zarzuela, Santiago (Spain)
Zarzycki, Roland (Poland)
Zavaleta, Andrés (Spain)
Zbigniew, Palka (Poland)
Zdravkovska, Smilka (USA)
Zelenyuk, Yuliya (Ukraine)
Zelmanov, Efim (USA)
Zertuche, Federico (Mexico)
Zhang, Ping (Turkish Cyprus)
Zhang, Qiao (USA)
Zhang, Qiong (Spain)
Zhang, Zhong Fu (P.R. China)
Zharkov, Ilia (USA)
Zheng, Songmu (P.R. China)
Zheng, Yong (P.R. China)
Zhizhchenko, Alexey (Russian Federation)
Zhou, Yong (P.R. China)
Zhu, Zuonong (P.R. China)
Zhuravlev, Sergei (Russian Federation)
Ziegler, Günter M. (Germany)
Ziegler, Martin (Germany)
Zili, Mounir (Tunisia)
Zimmermann, Irene (Germany)
Zinger, Aleksey (USA)
Zitan, Fouad (Morocco)
Zocar Expósito, Concepción (Spain)
Zohouri Zangeneh, Ali (Iran)
Zöller, Stefanie (Germany)
Zoltan, Nemeth (Hungary)
Zorboska, Nina (Canada)
Zorich, Anton (France)
Zouhaïr, Mouayn (Morocco)
Zuazua Iriondo, Enrique (Spain)
Zubelli, Jorge Passamani (Brazil)
Zugadi Reizabal, Amaia (Spain)
Zurro, María-Ángeles (Spain)
Zyskin, Maxim (United Kingdom)

Participants by country*

Algeria 11
Argentina 32
Armenia 1
Australia 23
Austria 11
Azerbaijan 11
Bangladesh 1
Belarus 4
Belgium 12
Benin 1
Bolivia 1
Bosnia & Herzegovina . . 3
Brazil 47
Bulgary 2
Burkina Faso 1
Cambodia 1
Cameroon 4
Canada 53
Chile 9
Colombia 13
Croatia 6
Cuba 2
Cyprus 1
Czech Republic 7
Denmark 9
Ecuador 1
Egypt 6
Estonia 6
Falkland Islands 1
Finland 26
France 122
Georgia 4
Germany 120
Greece 15
Guatemala 1
Hong-Kong 1
Hungary 21
India 111
Indonesia 2
Iran 38
Ireland 8
Israel 34
Italy 81
Ivory Coast 3
Japan 128
Jordan 1
Kazakhstan 4
Kenya 2
Kuwait 1
Kyrgyzstan 1
Latvia 3
Lesotho 2
Lithuania 1
Luxembourg 1
Madagascar 1
Malaysia 3
Mauritania 1
Mexico 57
Moldova 2
Mongolia 2
Morocco 15
Mozambique 2
Nederlandse Antillen 1
Nepal 1
Netherlands 25
New Zealand 3
Nicaragua 1
Nigeria 4
North Corea 3
Norway 16
Pakistan 4
Palestine 1
Panama 1
Paraguay 1
Peru 5
Phillippines 6
Poland 32
Portugal 32
P.R. China 33
Puerto Rico 5
Romania 22
Russian Federation 75
Saudi Arabia 6
Senegal 2
Serbia & Montenegro . . 15
Singapore 6
South Africa 12
South Corea 61
Spain 1330
Sudan 1
Sweden 21
Switzerland 26
Tadjikistan 1
Taiwan 24
Tanzania 1
Thailand 4
Tunisia 7
Turkey 16
Turkish Cyprus 2
Uganda 1
Ukraine 8
United Arab Emirates . . . 4
United Kingdom 103
USA 383
Uruguay 8
Uzbekistan 1
Venezuela 11
Vietnam 6

* According to their mailing addresses.

Author index

(Volumes I, II and III)