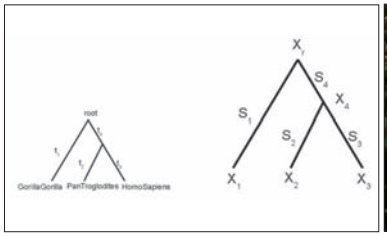
# NEWSLETTER

## OF THE EUROPEAN MATHEMATICAL SOCIETY






December 2012
Issue 86
ISSN 1027-488X


European Mathematical Society

# Editorial Team



# European Mathematical Society


## Newsletter No. 86, December 2012







ISSN 1027-488X



Published by the
EMS Publishing House
ETH-Zentrum SEW A27
CH-8092 Zürich, Switzerland.
homepage: www.ems-ph.org

For advertisements and reprint permission requests contact: newsletter@ems-ph.org

# EMS Executive Committee



# EMS Agenda

2013

**8 January**
Applied Mathematics Committee meeting, Paris
Maria Esteban: esteban@ceremade.dauphine.fr

**14–15 March**
"Friends of Mathematics Education", Berlin, Germany
Günter Törner: guenter.toerner@uni-due.de

**15–16 March**
Meeting of the Committee of Education, Berlin, Germany
Günter Törner: guenter.toerner@uni-due.de

**22–23 March**
ERCOM meeting, Luminy, France
Gert-Martin Greuel: greuel@mfo.de

**22–23 March**
Ethics Committee meeting, London, UK
Arne Jensen: matarne@math.aau.dk

**5–7 April**
Joint EMS-DMF Mathematical Weekend, Aarhus, Denmark
projects.au.dk/emsweekend/

**6 April**
Meeting of Presidents, Aarhus, Denmark
http://projects.au.dk/presidents-ems/
Stephen Huggett: s.huggett@plymouth.ac.uk

**19–20 April**
Committee for Developing Countries meeting, Linköping, Sweden
Tsou Sheung Tsun: tsou@maths.ox.ac.uk

**25–26 May**
Raising Public Awareness Committee meeting, Tycho Brahe's Island Hven, Sweden
Ehrhard Behrends: behrends@mi.fu-berlin.de

**10–14 June**
26th Nordic-EMS Conference of Mathematicians, Lund, Sweden
Lectures by the EMS lecturer for 2013 Tamar Ziegler (Technion, Israel).

**20–25 July**
29th European Meeting of Statisticians, Budapest, Hungary
www.ems2013.eu

**2–6 September**
16th Conference of Women in Mathematics, Bonn, Germany
Lectures by the EMS lecturer for 2013 Tamar Ziegler (Technion, Israel)

**12–13 October**
EMS-PTM Joint Meeting "A. Mostowski Centenary", Warsaw, Poland

**23–24 November**
Raising Public Awareness Committee meeting, Newcastle, UK
Ehrhard Behrends: behrends@mi.fu-berlin.de

# Editorial

Vicente Muñoz (Universidad Complutense de Madrid, Spain)

Dear Newsletter readers,

It has already been four and a half years since I took responsibility of the EMS Newsletter as Editor-in-Chief, and four years more since I joined the Editorial Board of the Newsletter as an editor. Now the time has come to hand over to my successor Lucia Di Vizio from Versailles, France. She and I are jointly working on the preparation of the previous and current issues of the Newsletter and she will take over responsibility after that.

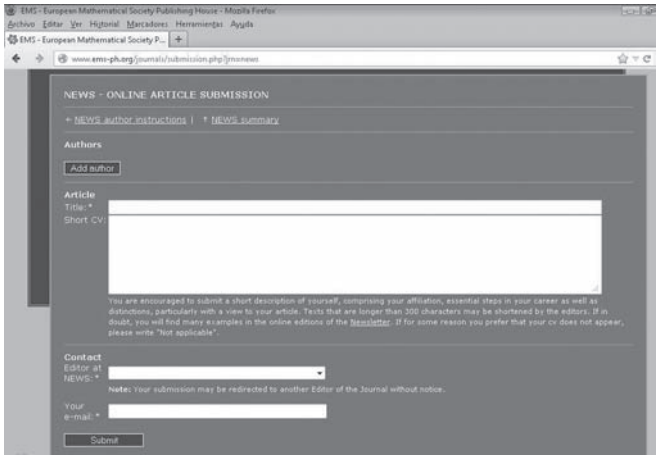
I want to use these lines to thank all the people who have supported this enterprise. The editors on the Editorial Board (whose names can be found on page 1 of every issue of the Newsletter) have the key role, searching for articles, convincing colleagues to write them and even writing articles themselves sometimes. The staff at the EMS Publishing House have always been very collaborative: the director Thomas Hintermann and his production team, the copy editor Chris Nunn who revises all articles for proper British grammar and spelling, and Christoph Eyrich who deals with LaTeX files. I also want to mention explicitly the former Editor-in-Chief Martin Raussen who helped me a lot in the early stages of my job, teaching me the non-trivial technicalities of the editorial process. He stayed on the Editorial Board of the Newsletter and also acted as liaison, being simultaneously a member of the Executive Committee of the EMS.

Also, I have had the opportunity to attend the meetings of the Executive Committee, which are held two or three times a year at different locations in Europe. At these meetings I have seen the huge amount of work that the colleagues involved in the EMS are doing to promote and support the mathematical community around Europe. The members of the Executive Committees of the EMS appear on page 2 of every issue of the Newsletter. During these years I have met many people at these meetings and keep good memories of many of them. Special mention is due to the two presidents of the EMS whose term has overlapped with mine: Ari Laptev and Marta Sanz-Solé. They have always been very comprehensive and supportive with the Newsletter.

Some changes have happened in the Newsletter over these years. In its basic structure, the Newsletter has stayed in the same format, which has been used since 2005 when the EMS Publishing House took charge of printing and distributing it to the EMS individual members. In 2009, the new webpage of the EMS, http://www.euro-math-soc.eu, began functioning. This made it more sensible that the material concerning announcements of conferences and recently published books, appearing up to that point in the EMS Newsletter, would appear on the webpage. The consequent liberation of space had the effect of allowing for new sections like the Zentralblatt Column, the Letters to the Editor, the Societies section and the Solid Findings in Mathematical Education, apart from enlarging the Book Review section.

But the main improvement in the Newsletter has not been visible to the reader, although it is the one that I am more proud of contributing to. The Newsletter has changed the submission system to have a much more professional production process. Now, authors submit their articles by uploading them to the webpage http://www.ems-ph.org/journals/submission.php?jrn=news (previously, they had to be sent by email to one of the editors). In this way all the information necessary about authors (e.g. to send proofs later, to send them complimentary copies, etc.) is collected automatically. Moreover, the editors of the Newsletter have an internal webpage to have access to all submitted articles, being able to see in which state of the process (e.g. submitted, accepted, copy-edited, to appear) each article is at any moment.

Anyone willing to contribute an article to the Newsletter (say a survey article, a letter to the editor or any other type of article that fits into the scope of the EMS Newsletter or any of its sections), please do so by submitting it through the webpage. If you want more specific information on whether an article is suitable, what is the appropriate length or what perspective to take before preparing it, it would be a wise idea to contact an editor of the Editorial Board beforehand. All editors will gratefully answer any queries in this direction.




**New webpage of the EMS Newsletter for submission of articles**

Let me finish by encouraging you to consider becoming an individual member of the EMS, in case you are reading these lines and are not yet a member of the EMS, and to tell any colleagues who may want to join the EMS. The EMS promotes initiatives to strengthen math-

ematics in Europe, maintaining an important presence at the European political level. To support these actions, the EMS needs to have a large number of members. Moreover, members of national societies have a reduced subscription fee, and you may easily become a member through the webpage http://www.euro-math-soc.eu. And last, but not least, all members receive a printed copy[1] of the EMS Newsletter!

[1] Although the Newsletter is generously offered by the EMS Publishing House free of charge online at www.ems-ph.org/journals/journal.php?jrn=news to anyone who wants to read it.

# Farewells within the Editorial Board of the EMS Newsletter

In December 2012, the terms of office are ending for the following editors of the Newsletter of the EMS:

Vasile Berinde (Universitatea de Nord Baia Mare, Romania), Chris Budd (University of Bath, UK), Krzysztof Ciesielski (Jagiellonian University, Kraków, Poland), Vicente Muñoz (Universidad Complutense de Madrid, Spain), Frédéric Paugam (Insitut de Mathématiques de Jussieu, Paris, France), Martin Raussen (Aalborg University, Denmark) and Robin Wilson (Pembroke College, Oxford, UK).

We express our deep gratitude for all the work they carried out during their time on the Editorial Board of the Newsletter. Among those leaving are three former Editors-in-Chief:
Robin Wilson (1999–2003), Martin Raussen (2003–2008) and Vicente Muñoz (2008–2012).

# New Editor of the EMS Newsletter appointed

Jaap Top graduated in 1989 from Utrecht University. After a year at Queen's University in Canada, he spent two years at the Erasmus University in Rotterdam. In 1992, he moved to the University of Groningen where he became a professor in 2005. Between 2003 and 2008 he was Editor-in-Chief of the Dutch mathematics journal "Nieuw Archief voor Wiskunde".
His research interests include arithmetic geometry, in particular curves over finite fields, elliptic surfaces, (history of) geometrical models and recently also geometric aspects of Painlevé differential equations.

# EMS Council Meeting in Kraków on 30 June and 1 July 2012

Stephen Huggett (University of Plymouth, UK)

The president welcomed all the delegates to the council, accepted a shortlist of invited guests and gave a vote of thanks to the Polish Mathematical Society, the Jagiellonian University and the AGH University of Science and Technology for their generosity and hospitality in hosting the meeting.

The agenda was approved and so were the minutes of the last council meeting in Sofia in 2010. The president asked for nominations from the floor of candidates for election to the Executive Committee. There were none. Miguel Abreu, Betul Tanbay and Jan Wiegerinck were then elected scrutineers.

### Reports, Finance and Membership

The president presented her report, noting actions taken to increase membership (such as that it is now free for one year for PhD students), actions taken to improve communication with members (such as the e-news) and new member benefits (such as free online access to *JEMS*). She summarised the scientific activities of the society and focused on publications. Highlights included the news of the Encyclopedia of Mathematics wiki and the availability online of proceedings of all past ECMs. Finally, to mark its 10th anniversary, the publishing house has established a monograph prize.

The secretary gave a short report on the meetings of the Executive Committee since the last council. Then vice-president Martin Raussen gave a report on the EMS website. He drew particular attention to the pages on News, Conferences, Jobs, Book reviews, Membership and Governance. He asked for help in identifying a second team of reviewers for books and he also asked for help in finding people willing to moderate blogs. He ended his report by pointing out that the further development of the website really needed a small working party; it had grown beyond what one person could do alone.

The treasurer gave a very brief report on the overall state of the society's finances, which he described as stable. However, the society would like to increase its activities, for which it needs more money, and for this and other reasons it is important to increase the number of individual members. He pointed out that the membership fee of 23 euros is low. He also noted that it is now very easy to make donations to the society online. This report was approved by the council.

The treasurer then presented the financial statements and auditors' reports for 2010 and 2011. A typographical error was pointed out in the notes on the 2011 Financial Statements but with this correction the statements and reports were approved by council. Finally, the treasurer presented the budget and membership fees for 2013 and 2014, which were also approved by the council.

Vice-president Mireille Martin-Deschamps presented membership statistics, such as the number of members by country and by member society. In reply to a question she said that there were very few individual members who had not joined through a society. The council approved the change of class of the German Mathematical Society from 3 to 4, and the president invited other societies to consider this for the next council.

The president briefly described the process by which the preparations are made for the election of corporate members and then invited the President of the Kosovar Mathematical Society (KMS) to address the council. In response to a question, he replied that the KMS was a non-governmental organisation. Then, in a secret ballot, the council voted to elect the KMS to membership of the EMS.

### By-laws and Elections

After a discussion, the council approved a new by-law, which reads:

**One of the sessions of the Council meeting in Kraków. Photo by Dmitry Feichtner-Kozlov.**

*RULE 15: No Council delegate can represent more than one of the groups referred to in the Statutes ARTICLE 5 number 3. As soon as a person is elected as a Council delegate representing any group, he or she is ineligible as a Council delegate for any other group.*

The council elected unopposed Franco Brezzi and Martin Raussen as Vice-presidents.

In a strongly contested ballot, the council elected Alice Fialowski, Gert-Martin Greuel, Laurence Halpern and Armen Sergeev as new members of the Executive Committee.

The council re-elected Rolf Jeltsch and Gregory Makrides as lay auditors, and PricewaterhouseCoopers as professional auditors, for the years 2013 and 2014.

### Review of Activities

Vicente Muñoz gave his report as Editor-in-Chief of the Newsletter, which the council approved by acclaim. The president presented the report of the Director of the EMS Publishing House, Thomas Hintermann, who could not be present.

Gert-Martin Greuel gave a report on Zentralblatt, emphasising that it was crucially important to dispel misconceptions of its size, range and functionality: it was in fact the largest and oldest (continuous from 1868) such database. Current work includes author identification. He finished by drawing attention to the fact that access is free to EMS members.

The following society committees gave poster presentations:

- Applied Mathematics
- Developing Countries
- Eastern Europe
- Education
- Electronic Publishing
- ERCOM
- Raising Public Awareness
- Women and Mathematics
- Meetings Committee
- Ethics Committee

### European Congresses of Mathematics

Vice-president Martin Raussen presented the report by the Executive Committee on 7ECM 2016.

Volker Mehrmann presented the Berlin bid for hosting the 7ECM 2016. In a show of hands, the council voted overwhelmingly in favour of accepting the bid from Berlin.

### Discussion on Publications

The president introduced the panel discussion on publications. She said that its eventual goal was that the council should have an opportunity to comment on the Code of Practice, before the Executive Committee approved a final version later this year.

Jean-Pierre Bourguignon spoke of the dramatically new world of information in which we find ourselves and of the consequent necessity, as a learned society, for us to stand back and take a global view. It is still not clear what the economic implications of these changes will be, or indeed whether paper copies of publications will survive at all. Nor is it clear what the effect on mathematics will be, especially because our patterns of use of the medium are different from other subjects. It is startling how the language has been crafted to serve political ends: "gold open access" means that we have to pay to publish! We will have to watch the legislative struggle in the USA and we will have to consider carefully what it is that we want for the future.

Rolf Jeltsch gave a presentation on the foundation of the EMS Publishing House, describing its principles and its subsequent growth and consolidation. It is part of the story of excessive prices causing editors to resign and move journals to learned society publishers. The EMS Publishing House is now 10 years old, has 2.4 employees and publishes 13 journals and more than 100 books. It is not for profit and has low prices and high quality (both in content and in production).

Ari Laptev noted that the author pays model excludes researchers from poorer countries, which may be regarded as an ethical question. He commented on the problem that bundling of journals forces libraries to subscribe to journals which they do not want. On the other hand, there is now intense pressure on researchers to publish their work in the best journals. This has led to a huge increase in poor quality research being submitted to these journals and therefore a big increase in their workload. It was pressures such as these which led to the formation of the EMS Ethics Committee, as a service to mathematics in Europe. He noted that plagiarism would probably be the thing which took most of the committee's time.

Arne Jensen described the various sorts of unethical behaviour in mathematical publications, such as plagiarism, duplicate publication, inadequate or dishonest citations, inflated self citation, and inadequate or dishonest refereeing.

He said that the remit of the Ethics Committee was to raise the awareness of the problem by preparing a Code of Practice, to encourage journals and publishers to respond to allegations of unethical behaviour in a conscientious way, and to provide a mechanism whereby researchers can ask the committee to help them pursue claims of unethical behaviour.

He presented the Code of Practice, noting first that although the Ethics Committee had spent a great deal of time on it, arguing over almost every word, they were now unanimous in recommending it. The president thanked the Ethics Committee for their hard work and invited comments and discussion from the floor on any of the topics raised by the panel.

In discussion, it was noted that under the gold open access model, there may be pressure to compromise quality, and that there are different types of open access, one of which involves specific funding for authors.

### Mathematics in Europe

The president gave a report on the considerable efforts of the EMS to influence the development of Horizon 2020, which led to considerable discussion. Mario Primicerio suggested that the amendments made to two documents on Horizon 2020 by Ciro Ciliberto on behalf of the EMS could be circulated and Jean-Pierre Bourguignon emphasised that our real deadline for having any further influence is around September (2012). Towards the end of 2013 the legislation will be enacted and Horizon 2020 begins on 1 January 2014.

Pavel Exner gave a report on the European Research Council. He said that 90% of the budget was spent on the starting and advanced grants but that from next year the starting grants would be split into two – starting and consolidation – because of the very high demand. The quality of peer review was crucial and so the ERC reviewers are separate from the wider pool of reviewers in the DG. He proposed a vote of thanks to all the reviewers and panel chairs, which the council approved by acclaim. There is a new grant scheme, providing seed money for commercial exploitation of research, and there are also synergy grants, in which small groups of individually excellent researchers would work together on a project. Finally, he expressed concern that even if the proposed increase in the budget is maintained, the increasing demand for grants may cause the current 12% or 13% success rate to fall. He asked all present to help to defend the success, and the budget, of the ERC.

### Closing

Vagn Lundsgaard Hansen, President of the Danish Mathematical Society, offered to host the next Meeting of Presidents in Aarhus University in April 2013. The council showed its gratitude by acclaim.

The president announced that the next council meeting would take place in 2014 and called for invitations to host the event, which would probably be held in conjunction with a scientific meeting of some sort.

Jean-Pierre Bourguignon spoke briefly in memory of Friedrich Hirzebruch, recalling how crucial he was to the founding of the European Mathematical Society.

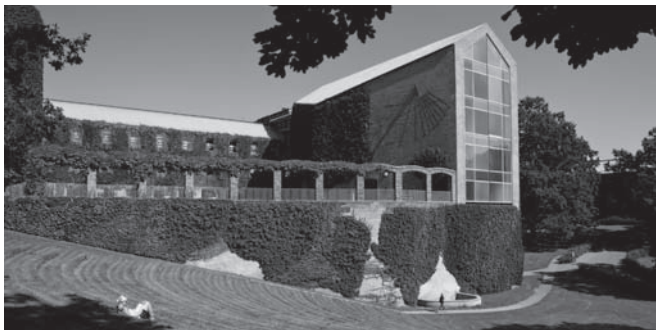
The president again thanked the Jagiellonian University and the Polish Mathematical Society for hosting the council. She also proposed a vote of thanks to the departing members of the Executive Committee, and to the Editor-in-Chief of the Newsletter, for all their work.

# Aarhus (Denmark) invites: Joint Mathematical Weekend and Meeting of Presidents

The Danish Mathematical Society (DMF) was founded in 1873 and will thus be 140 years old in 2013. During this year's council meeting in Kraków, to celebrate the occasion, the society's president (at the time) Vagn Lundsgaard Hansen (DTU Lyngby) invited the presidents of the European mathematical societies represented in the EMS to have their annual meeting in Denmark next year. Shortly afterwards, the society realised that it would be a good idea to combine this event with a scientific workshop in the form of a Joint Mathematical Weekend co-organised with the EMS. Such a weekend was held with success in Copenhagen in 2008; this time the venue will be Denmark's second largest city Aarhus in Jutland (the peninsula), on the premises of the Department of Mathematics at Aarhus University.

While the presidents will meet each other for a day-long meeting on Saturday 6 April, the Joint Mathematical Weekend will, as is customary, start on Friday 5 April at noon and last until Sunday 7 April at noon. This will allow the participants to listen to four plenary talks given by well-known mathematicians still to be chosen by the scientific committee. Moreover, participants will be involved in six parallel sessions with up to eight talks each under the following headings:

Algebra and Number Theory.
Algebraic Topology.
History of Mathematics.
Quantum and Riemannian Geometry.



Partial Differential Equations and Applications.
Stochastics and Free Probability.

Participants are also invited to display their research interests in poster format. In addition, it is planned to show the interactive travelling exhibition IMAGINARY alongside the two events. A conference dinner will be organised on Saturday evening in downtown Aarhus.

The Danish Mathematical Society, the European Mathematical Society and the Centre for Quantum Geometry of Moduli Forms at Aarhus University have already committed to helping fund the events; further sponsors will be approached.

For detailed information, including programme and travel information, please consult http://projects.au.dk/presidents-ems/ and http://projects.au.dk/emsweekend.

The organisers hope to welcome many European mathematicians to Aarhus in April 2013.

# Some History and Reminiscences of the Committee for Developing Countries

Tsou Sheung Tsun (Oxford University, UK)

I was asked to join the Committee for Developing Countries (CDC) by Bodil Branner, then a Vice-president of the EMS. That was the start of a very long association, which has been a joy and for which I am really grateful to Bodil. CDC turned out to be the nicest committee I have ever known, in spite of, or because of, many changes over the years.

CDC was in a sense revived by the then EMS President Rolf Jeltsch who invited Herbert Fleischner to take up the chair. We had our first meeting in 2002, in Zurich, and there were five of us: Georg Bock (Heidelberg), Herbert Fleischner (Vienna), M. S. Narasimhan (ICTP Trieste), Andrzej Pelczar (Krakow) and myself (Oxford). Herbert suggested me as the Vice-chair and I think I have never looked back since! Other than Narasimhan, I was meeting the others for the first time. When I discovered that Herbert knew more about the Chinese revolutionary heroes than I did, I was sure we would get on well, and we did!

One of the first practical things we did was to initiate what we called the Book Donation Scheme. Through various channels, including the EMS Newsletter, we at-

tracted donations from individual mathematicians and mathematical libraries to send to institutions in developing countries, with the stipulation that they be made available to all members of that institution. So far we have moved some 18 tonnes of books and journals, at a very rough estimate. These include libraries who want to go digital and get rid of their paper copies, and also personal libraries of retired colleagues. This has remained our most popular activity, so much so that we are now restricting ourselves to books most of the time to save on the high postage costs, since many journals are available online. This has been supported through grants first from ICTP and then later from the IMU and the LMS, and some others. It is really heart-warming that some donors, institutions and individuals are willing to pay, at least partly, for the shipping costs. I foresee that we shall be running this scheme for many years to come.

Another practical step was suggested by Herbert at that first meeting. He said we should have a separate bank account, under the wing of the EMS main account of course. I was very polite and did not laugh out loud because at that point we had zero euros, or pounds or whatever monetary unit you care to think of! But as it turns out, it was a wise move on Herbert's part. It turns out that we do have a regular (but small) income, thanks to the generosity of many reviewers for Zentralblatt Math, who donate their honorariums to us. This is still going on and we are forever grateful to them. From time to time I hear from Barbara Strazzabosco that in addition to the usual donations, some reviewer happens not to have collected their honorariums for many years and has decided to give it all to us! It is so heart-warming to know that people do care.

Then some time in 2006 another heart-warming donation came our way. I had heard from our member Michel Jambu, the Director of CIMPA (Centre International de Mathematiques Pures et Appliquees), that they had started an MSc programme in Cambodia, which had then just one mathematician with a PhD in the whole country! One promising student was accepted to do a PhD in China but there was no funding. The amount needed was not at all large and I was fretting that for want of such a small sum we would have one less mathematician in the developing world and, what was worse, fail to double the number of Cambodian PhDs! I remember walking round and round a circular carpet at home not knowing what to do. Then suddenly I remembered that the Encyclopaedia of Mathematical Physics I was co-editing was just about to be published (in five volumes) and each contributor would be paid 300 pounds. With about 500 authors that amounted to quite a large sum, but 300 pounds to each author would not be a great deal, especially noting that it would involve filling in tax forms. So I wrote to them, with willing help from my co-editors and the copy editor. And we collected over 20,000 pounds! We felt so rich! To me this money is really sweet because it is donated by mathematicians themselves to help other mathematicians. And yes, we did give CIMPA the requested sum.

As the years went by, our committee was gradually enlarged. At the moment we have 14 members but we are looking for new members to fill spaces vacated by retiring members. We have a good reason to enlarge the committee: our members travel a lot and at any one time only a portion of them are within easy communication. This is particularly important for our annual meetings. We have also created a new category of members – associated members – who work with us in an informal manner. They contribute greatly to our work, especially because by this method we have contacts in most European countries.

Every year we hold our annual meeting around April. This is at the invitation of one of our members, who usually pays our local expenses. In recent years we have also invited other colleagues who are interested in our work. We have had two presidents attending our meetings: Ari Laptev and Marta Sanz-Sole. It is very good, as then members can talk directly to the president and new schemes are often thus discussed and formed.

We thought up many schemes: some worked, some flopped. Notable among the latter were what we called "Twinning" and "Seed grants". In Sweden they have a successful scheme of "twinning", whereby one Swedish department commits itself to helping a chosen department in a developing country; so we thought we could expand this Europe-wide. There was absolutely no response from either side. So then we invented a "seed grant" to try to entice participants – still to no avail. I don't think we have yet quite understood why these ventures failed.

Apart from our book donation scheme, one project which did work was the Emerging Regional Centres of Excellence. For this we received support from the Executive Committee, particularly the president Marta Sanz-Solé, after a lot of liaison work by member Michel Waldschmidt and others. There are actually several other schemes which work well but it would be tedious to count one's successes.

Among our members there is one non-mathematician. He is a librarian in a well-known Swedish medical school and recruiting him was one of the best things we did. Anders Wandahl is not only enthusiastic about helping the developing world; he also has immense experience and vast knowledge about the internet. He has been running some electronic access workshops on our behalf, which young mathematicians, and the not-so-young ones too, find tremendously helpful. This is an area of activity we want to expand.

But what makes the committee so exceptionally good to work in is not really the successes or failures; it is the fact that we all have the same objective and it is a selfless objective with no personal gain or advancement as a prize dangling at the end of it.

I shall retire at the end of this year. We hope that Michel Waldschmidt will succeed me and in him CDC will have an exceptionally motivated and excellent chair. There are just two regrets: we lost both Andrzej Pelczar and Mikael Passare. Other than that, it has been for me 12 years of unalloyed comradeship and satisfying work.

*Tsou Sheung Tsun*
*Chair, Committee for Developing Countries*

# Second Call for Applications/ Expression of Interest

## Emerging Regional Centres of Excellence (EMS-ERCE)

## European Mathematical Society


With the success of our pilot scheme in electing the Abdus Salam School of Mathematical Sciences[1] (ASSMS) in Lahore, Pakistan, as the first EMS-ERCE, we are now seeking more applications from developing countries worldwide.

With the proliferation of emerging economies worldwide there are, among developing countries, varying degrees of development, just as among the developed world. In order to benefit from this situation our strategy of cooperation and help has to be adapted to the different levels of development.

Very good centres exist in emerging economies, where students from the least developed regions can be trained to a Master's level or higher; after the Master's degree, such a student could be given the option of coming to Europe to do a PhD. This is much more cost-effective than sending such a student directly to Europe.

It is in this spirit that the Committee for Developing Countries of the European Mathematical Society (EMS-CDC) wishes to propose a scheme of Emerging Regional Centres of Excellence (EMS-ERCE). The idea is for the EMS to select, endorse and help a number of such centres to offer training to MSc level to students from less developed countries in their region. With experience gained with the ASSMS, we know that such a scheme can work well, with the backing of the EMS and provided there are institutions in the emerging economies who are interested in participating.

We have spoken of this idea to a number of mathematicians and the reaction has been really positive, from Europe, South America, South Africa and Asia.

The advantages of such a procedure are threefold:

- It is cheaper in general to send a student to a nearby country or region.
- The student will be less disoriented and, in some cases, they may not need a higher European degree.
- The educating institution will gain experience and prestige.

As we know, there are already a number of prestigious institutions in emerging regions of international renown. They are of course welcome to apply, if the scheme interests them. In that case, they would add lustre to the scheme.

The criteria for eligibility are:

1. The centre is of good scientific standing in the region and neighbouring regions.
2. It has a good track record both in research and in pedagogy.
3. The centre has a fairly international outlook.
4. The centre has a long-term potential with reasonable guarantee for such.
5. The centre is willing to admit and educate graduate students from less developed regions. It should have the infrastructure to do so, e.g. the language of instruction should preferably be in one of the main European languages (English, French or Spanish).
6. The degree aimed at is MSc, or PhD in exceptional cases.
7. The centre is willing to welcome well-established foreign visiting mathematicians for collaboration in research and for teaching graduate courses.

If selected, the centre will be labelled an EMS-ERCE, initially for four years but renewable thereafter subject to mutual agreement.

The advantages for the centre are:

1. The label can add prestige and visibility to the centre, which will most probably attract more and better students.
2. Often this will in turn attract funding from local and regional sources.
3. The members of the CDC will be there to give support and advice whenever needed. Since this will be considered part of the CDC direct mission, the centre will get priority of CDC time and resources.
4. The CDC will be on hand to help those of the students who might wish to and who are capable of continuing their studies after their MSc.
5. The CDC will try to send experienced lecturers to give short or medium courses, e.g. by involving the Voluntary Lecturers Scheme, run by the IMU.
6. The CDC will seek European hosts for researchers from these centres for visits or collaborations, or both.
7. The CDC will make available small grants for members of the centres to attend conferences, where appropriate.

[1] In EMS Newsletter Issue 81 (September 2011) there are two articles about the centre.

If this scheme succeeds, these EMS-ERCEs will provide education to other, less developed, regions and get in exchange help to further develop themselves. We think it will be an advantageous scheme for all. At the same time, with much less expenditure, a larger number of students can receive their first graduate education, in a culture not too removed from their own. This will be a practical and efficient way for mathematicians to help other mathematicians.

The members of the ERCE subcommittee of EMS-CDC are:

Georg Bock (Heidelberg)
Giulia Di Nunno (Oslo)
Anna Fino (Torino)
Michel Jambu (Nice)
Michel Thera (Limoges)
Ramadas Ramakrishnan Trivandrum (ICTP)
Tsou Sheung Tsun (Oxford)
Begona Victoriano (Madrid)
Paul Vaderlind (Stockholm)
Michel Waldschmidt (Paris)

# Application or Expression of Interest European Mathematical Society Emerging Regional Centres of Excellence

Each interested institute is asked to send us a brief description of its activities and its suitability, together with a covering letter and supporting material, if any, to:

Michel Waldschmidt: miw@math.jussieu.fr or
Giulia Di Nunno: g.d.nunno@cma.uio.no or
Tsou Sheung Tsun: tsou@maths.ox.ac.uk

Institutes are welcome to discuss informally with any member of the ERCE subcommittee (named above) before sending their applications.

The preliminary deadline for application or expression of interest is 28 February 2013, which is expected to be extended if there is sufficient interest.

http://www.euro-math-soc.eu/comm-develop.html

# MSC/SKOS – The New Implementation of the MSC as a Linked Open Dataset

Graeme Fairweather (Executive Editor, Mathematical Reviews) and Gert-Martin Greuel (Editor-in-Chief, Zentralblatt MATH)

*Mathematical Reviews* and *Zentralblatt MATH* collaborate in developing and maintaining the Mathematics Subject Classification (MSC). The MSC is used by their services and generally in the mathematics profession and related fields to organise the mathematics literature. The current version, MSC2010, is the result of a careful public revision process culminating in its public release in January 2010. Now we are pleased to announce MSC2010 availability as a Linked Open Dataset, a modernised form following the standard called SKOS (Simple Knowledge Organization System) of the World Wide Web Consortium (W3C). SKOS is one of the newer standards set out for the developing Semantic Web and is based on RDF (Resource Description Framework). The new MSC/SKOS version results from the effort to make the MSC more available to the Semantic Web movement and on the internet.

It will be maintained as the authoritative source of the MSC, from which other forms may be derived, and will be available as linked data at http://msc2010.org/resources/MSC/2010/MSC2010. This is a large authority file in XML form. For other forms of the data perhaps more

suitable for special applications, see http://msc2010.org/resources/MSC/2010/info/.

The MSC/SKOS preserves the contents of MSC2010. It offers a new format better suited to the Semantic Web and adds authoritative translations into Chinese, Russian and Italian. In addition, there are cross-references to earlier MSC versions and to some other mathematics classification systems, such as the Dewey system. It is expected that similar information will be added in ways made possible by the new format, as a result of ongoing efforts to improve the MSC.

Comments about the MSC in general can be submitted through a Web form at http://msc2010.org/feedback or by email to feedback@msc2010.org. All information concerning MSC is shared fully by Mathematical Reviews and Zentralblatt MATH.

# André Lichnerowicz Prize in Poisson Geometry 2012

The André Lichnerowicz Prize in Poisson geometry was established in 2008. It is awarded for notable contributions to Poisson geometry, every two years at the "International Conference on Poisson Geometry in Mathematics and Physics", to researchers who completed their doctorates at most eight years before the year of the conference.

The prize is named in memory of André Lichnerowicz (1915–1998) whose work was fundamental in establishing Poisson geometry as a branch of mathematics. It is awarded by a jury composed of the members of the scientific and advisory committees of the conference.

The 2012 André Lichnerowicz Prize in Poisson geometry was awarded on 30 July to Thomas Willwacher (Harvard University) at the opening ceremony of the Poisson 2012 conference held at Utrecht University, the Netherlands. The 2012 edition of the prize was sponsored by the KWG (the Royal Dutch Mathematical Society) through the mathematics journal of the KNAW (Royal Netherlands Academy of Arts and Sciences) *Indagationes Mathematicae*.

Thomas Willwacher completed his PhD in 2009 at the ETH Zürich under the supervision of Giovanni Felder. His thesis, entitled "Cyclic formality", earned him the 2010 ETH Medal for outstanding dissertation. He subsequently took on a position at Harvard University as a Junior Fellow of the Society of Fellows. Willwacher has made

**Thomas Willwacher receives the prize from Ieke Moerdijk (representing the KWG). Photo by Gil Cavalcanti.**

deep and fundamental contributions to Poisson geometry, combining techniques from quantum field theory, homological algebra and graph complexes. His results include proofs of Kontsevich's cyclic formality conjecture for cochains and Tsygan's cyclic formality conjecture for chains. Together with Severa, he established the homotopy equivalence between Kontsevich's and Tamarkin's formalities of the little disk operad. More recently, he proved that the cohomology of the Kontsevich graph complex is isomorphic to the Grothendieck–Teichmueller Lie algebra.

# BSHM Neumann Book Prize

The British Society for the History of Mathematics is pleased to announce the biennial Neumann Prize for 2013. The prize is awarded for a book in English (including books in translation) dealing with the history of mathematics, aimed at a broad audience and published in 2011 or later. The prize is named in honour of Peter M. Neumann OBE, a former President and longstanding contributor to the Society. The value of the prize is £600.

Nominations for the prize are invited from individuals and publishers. Nominations should be sent to the chair of the judging panel, Norman Biggs, at n.l.biggs@lse.ac.uk. Publishers should send three copies of their nominated book(s) to Professor Norman Biggs, Chair: BSHM Neumann Prize, Department of Mathematics, London School of Economics, Houghton Street, London WC2A 2AE, United Kingdom.

# Algebraic Tools for Evolutionary Biology

Marta Casanellas (Universitat Politècnica de Catalunya, Barcelona, Spain)

*Algebraic statistics is a new discipline which, among other applications, is being used to study the evolution of species. Here we present the problems evolutionary biologists deal with, and explain how to address them from the algebraic statistics point of view and using tools from algebraic geometry. At the same time, we present new mathematical challenges that have resulted from this interdisciplinary interaction.*

## 1 Introduction

Based on Darwin's theory of natural selection, the evolution of species is usually modelled on a *phylogenetic tree*: the contemporary species are represented by its leaves, the root represents the common ancestor to all the species and each split into branches represents a speciation process (see Figure 1). Nowadays, due to the genome sequencing of a huge number of species (publicly available at www.ensembl.org, for example), the study of the evolutionary history of a group of species is carried out via the relationship of DNA molecules attached to them (normally corresponding to genes). Thanks to the double helix structure, each DNA molecule can be thought of as a sequence of nucleotides (adenine `A`, cytosine `C`, guanine `G` and thymine `T`), and thus as a sequence of the characters `A`, `C`, `G`, `T`. The aim of computational evolutionary biology or *phylogenetics* is to reconstruct the ancestral relations among species, i.e., the phylogenetic tree, from the given DNA sequences. The reconstruction of the phylogenetic tree is not only relevant to the evolutionary history but also to the genetics and physiology of the species.

Mathematically speaking, a phylogenetic tree is an acyclic connected graph whose leaves are labelled with the contemporary species names and (possibly) with a given interior node called the *root*. The length of an edge on a phylogenetic tree represents the *evolutionary distance* between both ends and is called the *branch length*. The *topology* of a phylogenetic tree means the topology of the labelled graph (without taking into account the branch lengths). It specifies the species groups that are created at each step of the evolutionary process (for instance, the trees in Figure 1 have the same topology as graphs but distinct topology in terms of phylogenetics, i.e., as labelled graphs). A phylogenetic tree of a set of species is specified by its topology and the corresponding branch lengths.

In order to reconstruct the phylogenetic tree of a group of contemporary species (both the tree topology and the branch lengths), one usually models evolution by mathematical models of nucleotide substitution (see next section). Then, the goal is to answer the following questions:

– What is the evolutionary model that best fits the given DNA sequences?
– What is the tree topology that best fits the data? What are the corresponding branch lengths?
– Is it actually possible to identify the phylogenetic tree from the DNA sequences? That is, are the parameters of the chosen evolutionary model *identifiable*?

Although one tends to think that biologists would consider only evolutionary models with an affirmative answer to the last question, this is not true in practice: biologists create more and more complex models of evolution without knowing whether its parameters can be recovered. For example, it is now well known that the root of a phylogenetic tree is not identifiable. Indeed, one cannot place the root having only information of the DNA sequences at the leaves, and an extra species acting as an outgroup is needed to determine its position. In other words, the common ancestral species cannot be placed in time only from the information of the contemporary species. This explains why phylogenetic trees are unrooted, although we will use a root for clarity in exposition. Once unrooted trees are considered, the model parameters of the most commonly used evolutionary models are identifiable. However, for more complex models, identifiability is an important issue. Biologists do not know whether the parameters are identifiable or not and base their decisions on tests performed on simulated data, but mathematicians have tools which could solve this problem.

As far as the first question is concerned, biologists often make an heuristic choice of the evolutionary model depending on the group of species under consideration and, even more often, they just use the model set by default in phylogenetic software. However, inaccurate model selection completely conditions the phylogenetic tree inferred (see for example [28]). Therefore, the problem of selecting the most suitable model for the given data is also crucial.

Several mathematical areas, such as combinatorics, dynamical systems, computer sciences and statistics, play a role in phylogenetics nowadays. In the last decade, the new discipline of *algebraic statistics* (coined by Riccomagno, Pistone and Wynn in [26]) has emerged and is becoming more and more used in computational biology [25]. In algebraic statistics one uses tools from algebraic geometry and commutative algebra on algebraic statistical models (that is, parametric statistical models where the distributions can be writ-


**Figure 1. Two phylogenetic trees on the set of species *Homo Sapiens* (human), *Pan Troglodytes* (chimpanzee), *Gorilla Gorilla* (gorilla) and *Macaca Mulatta* (macaque) with distinct topology.**

ten as polynomials in the parameters). In 1987, the biologists Cavender, Felsenstein and Lake were the first to realise that certain polynomials can play an important role in phylogenetic reconstruction. But it has not been until the new century that mathematicians have turned their attention to this application of algebraic geometry and have started studying the varieties involved to give a better understanding of phylogenetic reconstruction. These tools have now been applied to model selection (see [21]) to solve identifiability issues (see discussion below and [2]) and to deduce ancestral divisions among groups of species [29]. The reader interested in a deeper explanation on the applications of algebraic geometry in phylogenetics is referred to the book chapter [1].

In this paper we introduce the reader to the usage of algebraic statistics in phylogenetics, while proposing new mathematical challenges. In the next section we present evolutionary models as discrete-time hidden Markov processes on trees. In Section 3, we introduce the tools needed to handle these models as algebraic varieties and we discuss how to use these varieties in different phylogenetic problems. In Section 4 we present the most used phylogenetic reconstruction methods and we compare them to methods using algebraic geometry. Finally, we end the report with several conclusions.

## 2 Evolutionary models

Due to several processes of mutation, insertion and deletion of nucleotides along evolution, the DNA sequences of the same gene in different species are not identical: they contain similar parts but also parts that cannot be compared. Even more, as the genomes of different species contain different numbers of chromosomes and nucleotides, it is difficult to find these similar regions of the same gene. However, it is important to know which parts of the genomes of contemporary species come from the same part of the genome of their common ancestor. This information is collected in a multiple sequence *alignment*, i.e., a table whose rows are the species DNA sequences and whose columns correspond, theoretically, to nucleotides that have evolved from the same nucleotide of the common ancestor to all sequences (see Table 1). The problem is to obtain a "good" alignment for the given DNA sequences, i.e., an alignment where the majority of columns do indeed come from the same nucleotide of the common ancestor (without having a priori any other knowledge than the DNA sequences of the species, given separately). In this paper, as most biologists working in phylogenetics do, we will not deal with this problem, as we will assume that the alignment is already given. To simplify, we shall only consider mutation events (as most biologists do), that is, we avoid considering deletion and suppression of nucleotides.

In order to model evolutionary processes one usually gives a statistical model under the following hypotheses:

(i) Mutations in a DNA sequence occur randomly.

**Table 1. A multiple sequence alignment of DNA sequences of *Homo Sapiens* (human), *Pan Troglodytes* (chimpanzee) and *Gorilla Gorilla* (gorilla).**

| | |
|---|---|
| *Gorilla Gorilla* | AACTTCGAGGCTTACCGCTG |
| *Homo Sapiens* | AACGTCTATGCTCACCGATG |
| *Pan Troglodytes* | AAGGTCGATGCTCACCGATG |

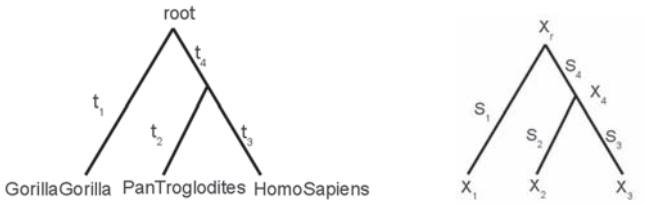



**Figure 2. (a) Phylogenetic tree of *Gorilla Gorilla, Pan troglodytes* and *Homo Sapiens* (magnitudes $t_i$ denote branch lengths). (b) Statistical model on a rooted phylogenetic 3-leaved tree.**

(ii) Evolutionary processes on different lineages only depend on their common node.

(iii) Each nucleotide in a DNA sequence evolves independently of the other nucleotides and all of them evolve according to the same process.

Due to this last hypothesis, it is enough to model the evolution of a single position in the DNA sequences. Assume we are given a tree, for instance the one in Figure 2a. Then we represent the statistical model on the tree as in Figure 2b. We associate a discrete random variable $X_i$ taking values in the set of four nucleotides $\{\mathtt{A}, \mathtt{C}, \mathtt{G}, \mathtt{T}\}$ to each vertex $i$. Random variables on the leaves of the tree represent nucleotides observed in the contemporary species (for example, $X_1$ displays nucleotides in *Gorilla Gorilla* in Figure 2). As each column of an alignment can be thought of as an observation of the random vector $X = (X_1, X_2, X_3)$, the random variables $X_i$ at the leaves are called "observed" variables. On the other hand, as we do not know the genome of the ancestral species, the random variables at the interior nodes of the tree are called "hidden" variables.

Following a Markov process, a *substitution matrix* (or *transition matrix*) $S_e$ is associated to each directed edge $e$. Its entries are the conditional probabilities $P(x|y, e)$ of a nucleotide $y$ at the parent node of $e$ being substituted by a nucleotide $x$ at its child, during the evolutionary process along branch $e$,

$$S_e = \begin{array}{c} \\ \mathtt{A} \\ \mathtt{C} \\ \mathtt{G} \\ \mathtt{T} \end{array} \begin{array}{c} \begin{array}{cccc} \mathtt{A} & \mathtt{C} & \mathtt{G} & \mathtt{T} \end{array} \\ \begin{pmatrix} P(\mathtt{A}|\mathtt{A}, e) & P(\mathtt{C}|\mathtt{A}, e) & P(\mathtt{G}|\mathtt{A}, e) & P(\mathtt{T}|\mathtt{A}, e) \\ P(\mathtt{A}|\mathtt{C}, e) & P(\mathtt{C}|\mathtt{C}, e) & P(\mathtt{G}|\mathtt{C}, e) & P(\mathtt{T}|\mathtt{C}, e) \\ P(\mathtt{A}|\mathtt{G}, e) & P(\mathtt{C}|\mathtt{G}, e) & P(\mathtt{G}|\mathtt{G}, e) & P(\mathtt{T}|\mathtt{G}, e) \\ P(\mathtt{A}|\mathtt{T}, e) & P(\mathtt{C}|\mathtt{T}, e) & P(\mathtt{G}|\mathtt{T}, e) & P(\mathtt{T}|\mathtt{T}, e) \end{pmatrix} \end{array}.$$

The entries of $S_e$ are unknown and, jointly with the distribution of nucleotides $(\pi_{\mathtt{A}}, \pi_{\mathtt{C}}, \pi_{\mathtt{G}}, \pi_{\mathtt{T}})$ at the root of the tree, form the *parameters* of the model. According to the values given to these parameters, there will be more or less substitutions along branch $e$ and therefore its length (measured as evolutionary distance) will vary. Actually, the branch length is usually measured in terms of the number of substitutions per nucleotide occurred along branch $e$ and it can be approximated by $-\frac{1}{4} \log \det S_e$ [4].

Depending on the amount of freedom on these matrices, we have different evolutionary models. For example, if no restriction is given, we have the most *general Markov model GMM* (see [30, 4]):

$$S_e = \begin{pmatrix} a_e & b_e & c_e & d_e \\ e_e & f_e & g_e & h_e \\ j_e & k_e & l_e & m_e \\ n_e & o_e & p_e & q_e \end{pmatrix}$$

If one imposes $\pi_{\mathtt{A}} = \pi_{\mathtt{T}}, \pi_{\mathtt{C}} = \pi_{\mathtt{G}}$ and $j_e = h_e, k_e = g_e, l_e = f_e$, $m_e = e_e, n_e = d_e, o_e = c_e, p_e = b_e, q_e = a_e$ then one obtains the *Strand symmetric model* whose name is attributed to the fact that it reflects the double strand symmetry of a DNA molecule (see [11]). If we impose uniform root distribution $\pi_{\mathtt{A}} = \pi_{\mathtt{C}} = \pi_{\mathtt{G}} = \pi_{\mathtt{T}} = 1/4$ and substitution matrices of type

$$S_e = \begin{pmatrix} a_e & b_e & c_e & d_e \\ b_e & a_e & d_e & c_e \\ c_e & d_e & a_e & b_e \\ d_e & c_e & b_e & a_e \end{pmatrix}$$

then we obtain the algebraic version of the *Kimura 3-parameter model* (see [23]). Also imposing $b_e = d_e$, we obtain the algebraic *Kimura 3-parameter* model (see [22]) and restricting to $b_e = c_e = d_e$, one obtains the algebraic version of the *Jukes-Cantor (JC)* model (see [20]):

$$S_e = \begin{pmatrix} a_e & b_e & b_e & b_e \\ b_e & a_e & b_e & b_e \\ b_e & b_e & a_e & b_e \\ b_e & b_e & b_e & a_e \end{pmatrix}.$$

Therefore, the parameter $a_e$ in these last models stands for the probability that nucleotides remain the same throughout the evolutionary process. All these models are instances of the so-called *equivariant* models (see [14, 9]). Obviously, the root distribution and the row sums of the transition matrices add to 1, so the actual number of free parameters is smaller than the quantity of letters given (for example, for the general Markov model there are three free parameters at the root and 12 free parameters at each substitution matrix).

Hypothesis (iv) implies that the probability that the alignment in Table 1 had been produced following an evolutionary process on the tree $T$ of Figure 2 equals

$$(p^T_{\mathtt{AAA}})^4 * p^T_{\mathtt{CCG}} * p^T_{\mathtt{TGG}} * (p^T_{\mathtt{TTT}})^3 * (p^T_{\mathtt{CCC}})^4 * p^T_{\mathtt{GTG}} * p^T_{\mathtt{GTT}} * (p^T_{\mathtt{GGG}})^3 * p^T_{\mathtt{TCC}} * p^T_{\mathtt{CAA}},$$

where $p^T_{xyz}$ stands for the probability of observing nucleotides $x, y, z$ at the leaves *Gorilla Gorilla* ($X_1$), *Homo Sapiens* ($X_2$) and *Pan Troglodytes* ($X_3$) of the tree $T$, respectively:

$$p^T_{xyz} = \mathrm{Prob}(X_1 = x, X_2 = y, X_3 = z \mid T).$$

Under the Markov process (hypothesis (ii)) on the tree of Figure 2, the probability $p^T_{xyz}$ can be expressed in terms of the entries of the substitution matrices as follows:

$$p^T_{xyz} = \sum_{x_r, x_4 \in \{\mathtt{A,C,G,T}\}} \pi_{x_r} S_1(x_r, x) S_4(x_r, x_4) S_2(x_4, y) S_3(x_4, x), \tag{1}$$

where $\pi = (\pi_{\mathtt{A}}, \pi_{\mathtt{C}}, \pi_{\mathtt{G}}, \pi_{\mathtt{T}})$ is the distribution of nucleotides at the root.

For example, under the Jukes-Cantor model we obtain

$$p^T_{\mathtt{AAA}} = \frac{1}{4}(a_1a_4a_2a_3 + 3b_1b_4a_2a_3 + 3b_1a_4a_2a_3 + 3a_1b_4a_2a_3 + 6b_1b_4b_2b_3), \quad a_i + 3b_i = 1 \text{ for } i = 1, 2, 3, 4.$$

As a consequence, under the evolutionary models we have described above, the joint distribution of nucleotides at the root of the tree can be expressed as a polynomial function in the parameters (see equation (1)). Models that share this property are called *algebraic statistical models* and are the kind of models algebraic statistics deals with.

## 3 Phylogenetic invariants

From now on $T$ will denote a phylogenetic tree *topology* on a set of $n$ species. Given an evolutionary model $\mathcal{M}$ as above with $d$ free parameters on the tree topology $T$, the following polynomial map sends each set of parameters to the joint distribution $(p^T_{x_1\ldots x_n})_{x_1,\ldots,x_n}$ (see equation (1)) of nucleotides at the leaves:

$$\begin{aligned} \varphi^{\mathcal{M}}_T : \mathbb{R}^d &\longrightarrow \mathbb{R}^{4^n} \\ \theta = (\theta_1, \ldots, \theta_d) &\mapsto p^T = (p^T_{\mathtt{AA\ldots A}}, p^T_{\mathtt{AA\ldots C}}, p^T_{\mathtt{AA\ldots G}}, \ldots, p^T_{\mathtt{TT\ldots T}}). \end{aligned} \tag{2}$$

For instance, the Jukes-Cantor model on the tree topology of Figure 2 corresponds to the following polynomial map:

$$\begin{aligned} \varphi^{JC}_T : \mathbb{R}^4 &\longrightarrow \mathbb{R}^{64} \\ (a_1, a_2, a_3, a_4) &\mapsto p^T = (p^T_{\mathtt{AAA}}, p^T_{\mathtt{AAC}}, p^T_{\mathtt{AAG}}, \ldots, p^T_{\mathtt{TTT}}). \end{aligned}$$

Although the parameters of the model represent probabilities and therefore lie in $[0, 1]$, in order to apply tools from algebraic geometry, one often forgets about this restriction and considers polynomial maps defined over $\mathbb{R}^d$ or $\mathbb{C}^d$.

The image $\mathrm{Im}\,\varphi^{\mathcal{M}}_T$ contains all joint distributions of nucleotides that have been generated by some set of parameters in the model $\mathcal{M}$ on the tree topology $T$. We denote by $V_{\mathcal{M}}(T)$ the smallest *algebraic variety* containing $\mathrm{Im}\,\varphi^{\mathcal{M}}_T$. An algebraic variety is the set of solutions to a system of polynomial equations: $V_{\mathcal{M}}(T) = \{p \in \mathbb{R}^{4^n} \mid f_1(p) = 0, \ldots, f_r(p) = 0\}$ for some polynomials $f_1, \ldots, f_r$. The image set itself $\mathrm{Im}\,\varphi^{\mathcal{M}}_T$ is not in general an algebraic variety but it forms a dense subset in the smallest algebraic variety containing it, $V_{\mathcal{M}}(T)$ when we stick to the complex numbers field.

On the other hand, it is well known that given any subset $S$ in $\mathbb{R}^{4^n}$, the set $I(S)$ of polynomials vanishing on all the points in $S$ forms an ideal (called the *ideal of* $S$). The Hilbert basis theorem implies that this ideal will have a finite set of generators. We are interested in the ideal $I(\mathrm{Im}\,\varphi^{\mathcal{M}}_T)$, which will be denoted $I_{\mathcal{M}}(T)$. If a polynomial $f$ lies in $I_{\mathcal{M}}(T)$ then $f$ is a relation among the theoretical probabilities $p^T_{x_1,\ldots,x_n}$, no matter which set of parameters of the model produced them (so $f$ is somehow "invariant"). In the 80s, biologists Cavender, Felsenstein and Lake proposed the following definition (see [12], [24]):

**Definition 3.1.** Given a tree topology $T$ on $n$ leaves and an evolutionary model $\mathcal{M}$, the polynomials in $I_{\mathcal{M}}(T)$ are called *invariants of* $T$. If $f$ is a polynomial in $I_{\mathcal{M}}(T)$ which does not belong to $I_{\mathcal{M}}(T')$ for another tree topology $T'$ on $n$ leaves, then $f$ is called a *phylogenetic invariant of* $T$.

**Example 3.2.** There are three distinct unrooted tree topologies on the set of leaves $\{1, 2, 3, 4\}$:

Let $T$ be one of these tree topologies and let $p^T = \varphi^{JC}_T(\theta)$ be a point in $V_{JC}(T)$ ($JC$ stands for the Jukes-Cantor model). Then the following equalities, which can be easily deduced from the symmetry of the transition matrices, lead to invari-


**Figure 3. The three different unrooted tree topologies on four leaves are denoted** 12|34**,** 13|24 **and** 14|23 **respectively.**

ants of $T$:

$$p^T_{\mathtt{AAAA}} = p^T_{\mathtt{CCCC}} = p^T_{\mathtt{GGGG}} = p^T_{\mathtt{TTTT}}$$
$$p^T_{\mathtt{AAAC}} = p^T_{\mathtt{AAAG}} = p^T_{\mathtt{AAAT}} = \cdots = p^T_{\mathtt{TTTG}}.$$

However, as they hold for any tree topology on four trees as above, they are not *phylogenetic* invariants. To give phylogenetic invariants, we consider the following $16 \times 16$ matrix:

$$flat_{12|34} = \begin{array}{c} \\ \text{states} \\ \text{leaves} \\ 1,2 \end{array} \begin{array}{c} \text{states at leaves 3 and 4} \\ \begin{pmatrix} p_{\mathtt{AAAA}} & p_{\mathtt{AAAC}} & p_{\mathtt{AAAG}} & \cdots & p_{\mathtt{AATT}} \\ p_{\mathtt{ACAA}} & p_{\mathtt{ACAC}} & p_{\mathtt{ACAG}} & \cdots & p_{\mathtt{ACTT}} \\ p_{\mathtt{AGAA}} & p_{\mathtt{AGAC}} & p_{\mathtt{AGAG}} & \cdots & p_{\mathtt{AGTT}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{\mathtt{TTAA}} & p_{\mathtt{TTAC}} & p_{\mathtt{TTAG}} & \cdots & p_{\mathtt{TTTT}} \end{pmatrix} \end{array}.$$

If $p = \varphi^{GMM}_T(\theta)$ for some parameters $\theta$ on the general Markov model then this matrix has rank less than or equal to four when $T$ is the tree 12|34 of Figure 3. On the contrary, if $T = 13|24$ or $T = 14|23$ and $p = \varphi^T_{GMM}(\theta)$ then this matrix has rank 16 (for parameters $\theta$ general enough). That is, the order five minors of this matrix are phylogenetic invariants for $T = 12|34$ (they belong to $I_{GMM}(12|34)$ but not to $I_{GMM}(13|24)$ or $I_{GMM}(14|23)$).

The set of phylogenetic invariants is different for each tree topology and therefore can be used to recover the tree topology in phylogenetics as follows. Given an alignment on $n$ species, let $\rho_{x_1 \ldots x_n}$ be the relative frequency of the $n$-tuple $x_1, \ldots, x_n$ occurring as a column of the alignment. If the given alignment had been produced according to a phylogenetic tree $T$ under one of the models above then the phylogenetic invariants of $T$ would vanish over the vector of relative frequencies $\rho = (\rho_{\mathtt{A}\ldots\mathtt{A}}, \ldots, \rho_{\mathtt{T}\ldots\mathtt{T}})$ (although we would need an infinite alignment!) or, equivalently, $\rho$ would be a point of the corresponding algebraic variety. In practice, genomes do not evolve under any mathematical evolutionary model nor on a phylogenetic tree; but if the evolutionary model considered fits the data well, then the phylogenetic invariants of the "correct" tree topology evaluated at the vector of relative frequencies of columns of the alignment should be close to zero. That is, theoretically, phylogenetic invariants can be used to infer the tree topology the data comes from (see [15] and [10] for different approaches to this tree topology reconstruction using phylogenetic invariants).

One could ask whether it is easy to obtain phylogenetic invariants or whether a complete set of generators of the ideal is needed. The generators of $I_{\mathcal{M}}(T)$ could be obtained, in theory, using computational algebra software (such as `Singular` [19] or `Macaulay2` [18]). But computational algebra requires huge memory capacity and, in practice, this is not even possible for three-leaved trees. For example, for the strand symmetric and the general Markov models, this type of software does not allow the computation of $I_{\mathcal{M}}(T)$ for $n = 3$ (and actually a whole set of generators is still unknown for these models). In fact, providing a set of generators of the ideal of a three-leaved tree under the general Markov model has become a challenge for the community working in this field and it is known as the *salmon problem* (as E. Allman has offered a personally caught salmon as a prize, see http://www.dms.uaf.edu/~eallman/Papers/salmonPrize.pdf).

We are a bit more lucky when dealing with Jukes-Cantor and Kimura 2- and 3-parameter models because a certain change of variables (a discrete Fourier transform) converts $\varphi^{\mathcal{M}}_T$ into a monomial parameterisation. In this case, software devoted to toric varieties allows the computation of generators of $I_{\mathcal{M}}(T)$ up to $n = 5$ leaves (the interested reader can find them at the webpage [17]). To have an idea of what we are talking about, the ideal $I_{\mathcal{M}}(T)$ for four leaves and the Kimura 3-parameter model has 8002 generators.

Obviously, biologists are not happy with five species trees and we need to provide them phylogenetic invariants for any number of species. The following theoretical result allows one to compute the invariants for trees on $n$ leaves from the invariants of three-leaved trees and the minors of certain matrices associated to the edges of the tree (as in example 3.2).

**Theorem 3.3** ([14], [3], [31], [11])**.** *Let $T$ be a phylogenetic tree of $n$ species evolving according to one of the equivariant models $\mathcal{M}$ above. There exists an algorithm to obtain a set of generators of $I_{\mathcal{M}}(T)$ from the invariants of a 3-leaved tree and the minors of certain matrices associated to the edges of $T$ (the so-called edge invariants).*

It is worth pointing out that a complete list of invariants for a tree on three leaves is not easy to obtain. As we mentioned above, such a list does not exist for the general Markov model or the strand symmetric model. This means that the previous theorem cannot be used in practice.

Nevertheless, one would hope that such a complete list of invariants is not needed, whereas suitably selected invariants should be enough for phylogenetic reconstruction purposes. For example, one only needs to consider those polynomials that define the variety $V_{\mathcal{M}}(T)$ at the points that correspond to distributions (this idea was explored in [7] for the Kimura 3-parameter model and decreased the 8002 invariants mentioned above to 48, for instance). On the other hand, if one is interested in just recovering the tree topology (not the substitution parameters or branch lengths), the focus should be in *phylogenetic* invariants. The following result proves that phylogenetic invariants are actually the edge-invariants presented in Theorem 3.3 above.

**Theorem 3.4** ([9])**.** *Let $T$ be a phylogenetic tree of $n$ species evolving under an equivariant evolutionary model as above. Then, for phylogenetic reconstruction purposes it is enough to consider only edge-invariants of $T$.*

Although its proof is quite technical, this result could have been easily expected. Indeed, there is a result in combinatorics guaranteeing that any tree can be reconstructed by the bipartitions it induces on its set of leaves. A *bipartition* of a set $L$ is a pair of supplementary non-empty subsets (for example, $\{\{1,2\},\{3,4\}\}$ is a bipartition of $L = \{1,2,3,4\}$). Two bipartitions $\{A_1, A_2\}$ and $\{B_1, B_2\}$ of the same set are said to be *compatible* if at least one of the four intersections $A_1 \cap B_1$, $A_1 \cap B_2$, $A_2 \cap B_1$, $A_2 \cap B_2$ is not empty. If $T$ is an unrooted tree whose leaves are labelled by the set $L$ then each edge in $T$ induces a bipartition on $L$, corresponding to the two subsets of leaves split by that edge. It turns out that the set $bi(T)$ of $2n-3$ bipartitions induced by the edges of $T$ is composed of pairwise compatible bipartitions. The following result is attributed to Buneman and is the combinatorial version of Theorem 3.4 above:

**Theorem 3.5** (Buneman, [5]). *Let $L$ be a set of $n$ elements and $S$ a collection of $(2n-3)$ bipartitions of $L$. Then $S$ is formed by pairwise compatible bipartitions if and only if there exists an unrooted tree $T$ with leaves labelled on $L$ such that $bi(T) = S$. In this case, the tree $T$ is unique.*

## 4 Phylogenetic reconstruction methods

### Maximum likelihood

One of the most common phylogenetic reconstruction methods is by maximum likelihood estimate. Given an alignment $D$ and an evolutionary model $\mathcal{M}$, one wants to obtain the tree topology $T_0$ and the substitution parameters $\hat{\theta}$ which maximise $Prob(D|\mathcal{M}, T, \theta)$ among all possible tree topologies and substitution parameters. To this end, the maximum likelihood estimate of the substitution parameters is obtained separately for each tree topology $T$ using some of the available optimisation methods and then one chooses the tree topology and the parameter estimates which maximise the likelihood among all tree topologies.

This method has a clear drawback: the number of (unrooted) tree topologies on $n$ leaves is $(2n-5)!!$, which grows factorially in $n$, so that it becomes unfeasible to do an exhaustive search through all tree topologies for more than 15 leaves. The vast majority of phylogenetic reconstruction software (such as the widely used PHYLIP [16] or PAML [32]) uses some branch and bound algorithm and not all tree topologies are considered. On the other hand, numerical optimisation methods do not guarantee a global maximum in general and, even more, it is unknown whether there is a unique local maximum for biologically relevant parameters.

### Neighbor-joining

By far, the most used phylogenetic reconstruction method is neighbor-joining (it has more than four million entries in Google!). This is a *distance-based method*, that is, all the information from an alignment on a set of species $\{1, \ldots, n\}$ is condensed into a *dissimilarity function* $d : \{1, \ldots, n\} \times \{1, \ldots, n\} \longrightarrow \mathbb{R}_{\geq 0}$ (symmetric and with zero diagonal entries). This dissimilarity function is intended to approximate the evolutionary *distance* (without triangular inequality) between pairs of species or, in other words, it should account for the amount of mutations that separate both species. Obviously, not all mutations that have occurred during evolution can be observed in the contemporary species sequences (for instance, there may be an `A` mutating to `T` and finally coming back to `A` in the current species) and the dissimilarity function has to take this into account. For example, the *Jukes-Cantor distance* between two DNA sequences defined as $-\frac{3}{4}\ln(1 - \frac{4}{3}f)$, where $f$ is the fraction of different nucleotides in both sequences, approximates the amount of mutations (observed and unobserved) if the species have evolved under the Jukes-Cantor model.

Given a dissimilarity function $d$, the first step in the neighbor-joining algorithm chooses two species $x$ and $y$ minimising the function $D_{x,y} = d(x, y) - \frac{1}{n-2}\sum_z (d(x, z) + d(y, z))$. These two species are joined on a cherry (that is, two leaves joined by two edges and an interior node) and the interior node is treated as a new species substituting the former $x$ and $y$. In this way the number of species is decreased at each step and the function $D$ is redefined accordingly.

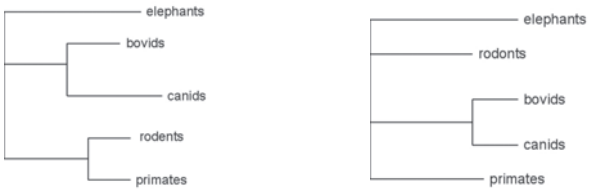



**Figure 4. (a) Correct phylogenetic tree of primates, rodents, bovids, canids and elephants. (b) Incorrect tree reconstructed by neighbor-joining and maximum likelihood.**

This algorithm produces the correct phylogenetic tree if the sequences actually come from a tree and the distances used are the lengths of the corresponding paths. However, when dealing with biological sequences, their estimated distances do not correspond to the branch lengths of any particular tree and the tree constructed by the neighbor-joining algorithm may not have a realistic biological interpretation. In spite of this, it is thought to be a highly reliable method and, as there is no need to search through the whole space of tree topologies, it is used to produce phylogenetic trees for large number of species.

### Phylogenetic reconstruction based on invariants

Phylogenetic reconstruction methods based on invariants can be found in [15], [6] and [8]. The method tested in [6] considers a set $I_T$ of generators of the corresponding ideal for each 4-leaved tree topology $T$ as in Figure 3 and, given an alignment corresponding to a point $p \in \mathbb{R}^{4^4}$, uses the function $c(T) = \sum_{f \in I_T} |f(p)|$ as a *cost* for the topology $T$. The topology which reaches the lowest cost is estimated as the correct topology. Whereas the results obtained with this method are slightly worse than those obtained by maximum likelihood or neighbor-joining, it is worth pointing out that the evolutionary models described here are much more general than the models considered in these widely used methods.

Indeed, the Markov processes are usually considered in continuous time, that is, the substitution matrices are of type $S_e = exp(Qt_e)$, where $Q$ is an instantaneous mutation rate matrix and $t_e$ denotes the number of substitution events occurred along edge $e$. In most common applications the matrix $Q$ is the same for all the edges in the tree and the evolutionary process is said to be *homogeneous*. This kind of process is used to model the evolution of species which evolve at approximately the same rate. This hypothesis is violated by most groups of species (for example, even inside the group of mammals, rodents evolve faster than primates). The parameters for the models we have considered in this paper are the entries of the substitution matrices $S_e$ and therefore they account for non-homogeneous evolutionary processes. In [6] it is proven that methods based on phylogenetic invariants outperform common phylogenetic reconstruction methods when dealing with non-homogeneous data. For example, the phylogenetic tree of primates, rodents, bovids, canids and elephants is drawn in Figure 4(a), but this tree is incorrectly reconstructed by neighbor-joining and maximum likelihood (which reconstruct the tree in 4(b)). Methods based on invariants should reconstruct the phylogenetic tree of this set of species correctly.

Although we have shown in 3.4 that the invariants which really matter for the reconstruction of the tree topology are the edge-invariants, there is no phylogenetic reconstruction method based solely on edge-invariants. In any case, the number of edge invariants grows exponentially in $n$ so that not all of them should be used for large sets of species. Moreover, the number of unrooted tree topologies ($(2n-5)!!$ as mentioned above) makes it impossible to use a different set of invariants for each tree. A reasonable approach could be combining phylogenetic invariants with other existing methods. For instance, if a good inference method based on invariants is provided for quartet trees then it could be incorporated into *quartet-based methods* (see [27]).

## 5 Conclusions

Presenting evolutionary models as polynomial maps allows one to relate phylogenetic questions to problems in algebraic geometry. We have seen that computational algebraic tools are not of much help in this case but we have shown that theoretical results can indeed be used in phylogenetic reconstruction. The applications of algebraic geometry in evolutionary biology do not end here. For example, they can be applied to deal with identifiability issues of complex evolutionary models such as *phylogenetic mixtures*. Phylogenetic mixtures take into account the possibility that distinct parts of the genome have evolved in different ways (for example, genes are not likely to mutate whereas other regions of the genome mutate easily). DNA sequences are said to be a phylogenetic mixture on $r$ trees if we can split the corresponding alignment into $r$ pieces such that each of them comes from a particular phylogenetic tree (the $r$ trees can have the same or different topology). Biologists do not know the maximum number of phylogenetic mixtures that one should use (i.e., the maximum $r$ for which the parameters can be identified from the alignment) and they recommend (without any mathematical basis) not to use more than four or five. But an alignment from a phylogenetic mixture on trees $T_1, \ldots, T_r$ is just a point on a linear variety generated by points in the varieties $V_{\mathcal{M}}(T_i)$. In this way, advanced tools in algebraic geometry dealing with secants and joins of varieties can be used to determine the maximum number of phylogenetic mixtures to use.

On the other hand, we have already mentioned that the techniques introduced here have also been applied to other problems. However, there are still many other areas to explore using these tools. In any case, there is a long way to go to convince biologists to use them. Indeed, these tools are often not directly applicable to real situations and should be used together with statistics, combinatorics and computational tools. Using a multidisciplinary point of view we could give back to biology all the knowledge we got from it in the shape of mathematical problems. Exactly as Joel E. Cohen says in [13]: "Mathematics is biology's next microscope, only better; biology is mathematics' next physics, only better."

**Acknowledgement.** Part of this report has been inspired by the article by the same author published in Spanish in *La Gaceta de la Real Sociedad Matemática Española* (vol. 15, 2012). The author has been partially supported by Ministerio de Economía y Competitividad MTM2009-14163-C02-02 and Generalitat de Catalunya, 2009 SGR 1284.

## Bibliography

[1] ES. Allman and JA Rhodes. Phylogenetic invariants. In *Reconstructing evolution*, pages 108–146. Oxford Univ. Press, Oxford, 2007.

[2] ES Allman and JA Rhodes. The identifiability of tree topology for phylogenetic models, including covarion and mixture models. *Journal of Computational Biology*, 13:1101–1113, 2006.

[3] ES Allman and JA Rhodes. Phylogenetic ideals and varieties for the general Markov model. *Advances in Applied Mathematics*, 40:127–148, 2008.

[4] D Barry and JA Hartigan. Asynchronous distance between homologous DNA sequences. *Biometrics*, 43(2):261–276, 1987.

[5] P Buneman. The recovery of trees from measures of dissimilarity. In Edinburgh University Press, editor, *Mathematics in the Archaeological and Historical Sciences*, pages 387–395, 1971.

[6] M Casanellas and J Fernandez-Sanchez. Performance of a new invariants method on homogeneous and nonhomogeneous quartet trees. *Mol. Biol. Evol.*, 24(1):288–293, 2007.

[7] M Casanellas and J Fernandez-Sanchez. Geometry of the Kimura 3-parameter model. *Adv. in Appl. Math*, 41:265–292, 2008.

[8] M. Casanellas and J. Fernandez-Sanchez. Reconstrucción filogenética usando geometría algebraica. *Arbor. Ciencia, pensamiento, cultura*, 96:207–229, 2010.

[9] M Casanellas and J Fernandez-Sanchez. Relevant phylogenetic invariants of evolutionary models. *Journal de Mathématiques Pures et Appliquées*, 96:207–229, 2011.

[10] M Casanellas, LD Garcia, and S Sullivant. Catalog of small trees. In L. Pachter and B. Sturmfels, editors, *Algebraic Statistics for computational biology*, chapter 15. Cambridge University Press, 2005.

[11] M Casanellas and S Sullivant. The strand symmetric model. In L. Pachter and B. Sturmfels, editors, *Algebraic Statistics for computational biology*, chapter 16. Cambridge University Press, 2005.

[12] J Cavender and J Felsenstein. Invariants of phylogenies in a simple case with discrete states. *J. Classification*, 4:57–71, 1987.

[13] JE Cohen. Mathematics is biology's next microscope, only better; biology is mathematics' next physics, only better. *PLoS Biol*, 2(12), 12 2004.

[14] J Draisma and J Kuttler. On the ideals of equivariants tree models. *Mathematische Annalen*, 344:619–644, 2009.

[15] N Eriksson. Tree construction using singular value decomposition. In L Pachter and B Sturmfels, editors, *Algebraic Statistics for computational biology*, chapter 19, pages 347–358. Cambridge University Press, 2005.

[16] J Felsenstein. Phylip (phylogeny inference package) distributed by the author. department of genome sciences, university of washington, seattle. http://evolution.genetics.washington.edu/phylip.html.

[17] LD Garcia and J Porter. Small phylogenetic trees webpage. http://bio.math.berkeley.edu/ascb/chapter15/.

[18] D R Grayson and M E Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[19] GM Greuel, G Pfister, and H Schoenemann. Singular: A computer algebra system for polynomial computations. Available at http://www.singular.uni-kl.de/, 2003.

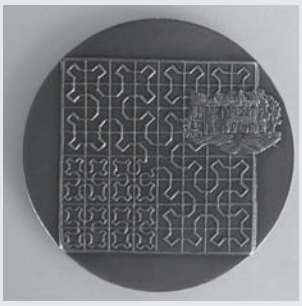
[20] TH Jukes and CR Cantor. Evolution of protein molecules. *In Mammalian Protein Metabolism*, pages 21–132, 1969.

[21] A Kedzierska, M Drton, R Guigó, and M Casanellas. SPIn: model selection for phylogenetic mixtures via linear invariants. *Molecular Biology and Evolution*, 29:929–937, 2012.
[22] M Kimura. A simple method for estimating evolutionary rates of base substitution through comparative studies of nucleotide sequences. *J. Mol. Evol.*, 16:111–120, 1980.
[23] M Kimura. Estimation of evolutionary sequences between homologous nucleotide sequences. *Proc. Nat. Acad. Sci. , USA*, 78:454–458, 1981.
[24] JA Lake. A rate-independent technique for analysis of nucleaic acid sequences: evolutionary parsimony. *Mol. Biol. Evol.*, 4:167–191, 1987.
[25] L Pachter and B Sturmfels, editors. *Algebraic Statistics for computational biology*. Cambride University Press, November 2005. ISBN 0-521-85700-7.
[26] G Pistone, E Riccomagno, and HP Wynn. *Algebraic Statistics: Computational Commutative Algebra in Statistics*. Chapman & Hall/CRC, December 2000.
[27] V Ranwez and O Gascuel. Quartet-based phylogenetic inference: improvements and limits. *Mol Biol Evol*, 18:1103–1116, 2001.
[28] J Ripplinger and J Sullivan. Does choice in model selection affect maximum likelihood analysis? *Systematic Biology*, 57(1):76–85, 2008.
[29] D Sankoff. Designer invariants for large phylogenies. *Mol. Biol. Evol.*, 7:255–269, 1990.
[30] MA Steel. Recovering a tree from the leaf colourations it generates under a markov model. *Applied Mathematics Letters*, 7:19–24, 1994.
[31] B Sturmfels and S Sullivant. Toric ideals of phylogenetic invariants. *Journal of Computational Biology*, 12:204–228, 2005.
[32] Z Yang. PAML: A program package for phylogenetic analysis by maximum likelihood. *CABIOS*, 15:555–556, 1997.

*Marta Casanellas [marta.casanellas@upc.edu] is an associate professor at the Universitat Politècnica de Catalunya, Barcelona, Spain. After obtaining a PhD in mathematics in 2002, she moved to the University of California at Berkeley on a Fulbright postdoc position for one year. There she pursued her studies in pure algebraic geometry but after a while she became interested in the applications of pure mathematics to evolutionary biology. Since then, she has combined both research areas and collaborates with biologists. She is the PI of a research group in Spain and her publications include papers in high impact journals and book chapters.*

# The 6ECM Medal

Krzysztof Ciesielski (Jagiellonian University, Kraków, Poland)

The initiator of the organisation of 6ECM in Kraków in 2012 was Andrzej Pelczar (1937–2010), professor of the Jagiellonian University and EMS Vice-President (1997–2000). Among his ideas concerning the congress was a special medal for the occasion; it was a new idea and had not been done before. The Faculty of Mathematics and Computer Science of the Jagiellonian University and Województwo Małopolskie (Małopolska Region) managed to realise this thought of Pelczar and the medal was issued.

The medals were made of bronze and issued in three limited edition series. The medals from the first series were covered with silver and were given to invited speakers and people who greatly contributed to the congress. The medals from the second series were given to others who had actively worked on the organisation of the congress and to the authors of the articles in the special volume of the journal of the Polish Mathematical Society "Wiadomości Matematyczne" published on the occasion of 6ECM. The medals from the third series could be purchased. Medals of all the series were designed with the same pattern.

The 6ECM Medal was designed in 2012 by Kraków's artist Professor Stefan Dousa, who did it as a personal favour for mathematics, mathematicians and particularly Andrzej Pelczar.

The obverse of the medal depicts the 6ECM logo and a view of Kraków Market Square. On the reverse of the medal are the approximations of the Sierpiński space-filling curve (the paper about this curve was published exactly 100 years ago in the Bulletin of the Academy of Arts and Science in Kraków) and a picture of Collegium Novum, Jagiellonian University. The drawing of Collegium Novum was also on the cover of the special issue of "Wiadomości Matematyczne" and the article about the Sierpiński curve was contained there.

# On Mathematics in Kraków Through the Centuries[1]

Krzysztof Ciesielski and Zdzisław Pogoda (both Jagiellonian University, Kraków, Poland)

Polish mathematics achieved fame in the first half of the 20th century. This is mainly credited to Stefan Banach with the Lvov School of Mathematics and the Warsaw School of Mathematics but the background of Polish mathematics at a high level is largely down to Kraków and the Jagiellonian University, especially the period at the beginning of the 20th century. Later, Kraków mathematicians also obtained many magnificent results and Polish mathematics, although not so famous, did exist in a previous period of about five centuries, again mainly connected to Kraków and the Kraków University.

The story begins in 1364, when Polish king Casimir the Great (Kazimierz Wielki) established a university in Kraków, which was one of the first universities in Central Europe (only Charles University in Prague is older). Nowadays this is called the Jagiellonian University, the name taken from Polish king Władysław Jagiełło, who renovated and extended the university at the beginning of the 15th century, according to the last will of his wife Jadwiga, a granddaughter of Casimir the Great. Jadwiga ordered that after her death her jewellery would have to be used in the renovation of the university (then called the Kraków Academy, the name being changed to the Jagiellonian University in the 19th century).

In the beginning, classical topics divided into trivium and quadrivium were lectured at the university. Quadrivium contained arithmetic, geometry, astronomy and music. About 1405 a Kraków citizen Jan Stobner founded a Chair of Mathematics and Astronomy. This was an event of great influence in the development of mathematics at Kraków Academy, as the Head of the Chair could stay and work there for a longer time and, consequently, could specialise in some areas. In those times, a scientist had to be prepared to lecture many subjects and frequently drawing of lots decided what would be lectured. The existence of a Chair guaranteed some kind of stability. The second Chair connected with mathematics was founded about 1450 by Marcin Król of Żurawica (c.1422 – c.1453). This was a Chair of Astrology (but it must be pointed out that astrology was at that time treated very seriously and creating horoscopes usually involved complicated calculation). Król reformed teaching mathematics at the university and wrote some mathematical monographs, in particular *Geometriae practicae seu Artis mensurationum* and *Algorismus minutarium*. In those years education at Kraków University was at a very high level. For example, among scholars educated in Kraków there were five who between 1448 and 1471 headed a Chair at the University of Bologna. One of the most famous graduates of Kraków Academy was Mikołaj Kopernik (Nicolaus Copernicus) (1473 – 1543) who became a student there in 1491. Kopernik many times emphasised the role of Kraków Academy in his education.

**The monument of Mikołaj Kopernik in front of Collegium Witkowskiego, Jagiellonian University, Kraków**

In the first decades of the 16th century a lot changed in European universities under the influence of the Renaissance. The Arts played the main role. In Kraków, the development of mathematics was not financed sufficiently. Only in the first half of the 17th century in Kraków Academy did there appear a mathematician of European level: Jan Brożek (Joannes Broscius) (1585 – 1652). He was also a philosopher, an astronomer, a physician and a theologist. Besides his scientific achievements, he generously donated to the university. His main mathematical achievements were obtained in the theory of numbers. He mainly investigated prime numbers and perfect numbers. He wrote many dissertations and books about numbers, logarithms and several applications of geometry. He pointed out several mistakes in papers written by others. Unfortunately, he lived and worked far from mathematical centres and his research was, in fact, not known abroad. Brożek did not find successors in Kraków.

The 17th and 18th centuries were a period of rapid development of mathematics in Europe. Sad to say, this was not the case of Poland. No report can be made of any expansion of science here. The situation was improved at the end of the 18th century thanks to reforms introduced

1 The article first appeared in the special issue of *Wiadomości Matematyczne* (vol. 48(2012), no. 2, eds: K.Ciesielski, T. Nadzieja, K.Pawałowski) published on the occasion of the 6ECM in Kraków.

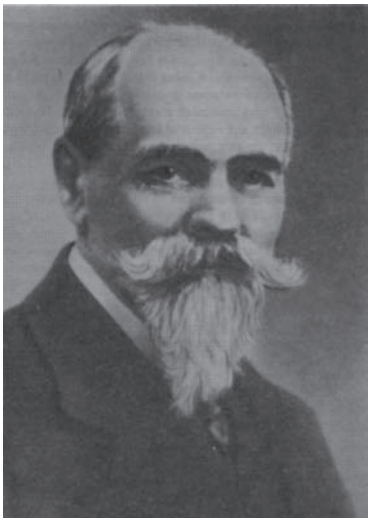
by the Commission of National Education (Komisja Edukacji Narodowej) and personally Hugo Kołłątaj (1750–1812) and Jan Śniadecki (1756–1830). Śniadecki was undoubtedly the best Polish mathematician born in the 18th century. Despite his scientific achievements (in particular, he was the forerunner of probability in Poland) he worked very actively in teaching and he wrote some mathematical books. Several terms in Polish mathematical terminology propagated by Śniadecki are still used. It must be noted that by the efforts of Śniadecki two mathematical Chairs at Kraków Academy were founded. They were called the Chair of Elementary Mathematics and the Chair of Higher Mathematics.

In 1795 Poland lost its independence and up to the end of World War I had been divided among Russia, Prussia and Austro-Hungary. In the part of Polish territory under Austrian power the situation was not bad; in particular, the universities in Kraków and Lwów (Lvov) still continued to function and the lectures were conducted in Polish. The development of science, including mathematics, could also be observed. In 1815 the Kraków Learned Society (Krakowskie Towarzystwo Naukowe) was founded; it was transformed into the Academy of Arts and Science (Akademia Umiejętności) in 1872. Since 1817, the society has published together with Kraków University a scientific journal *Rocznik Towarzystwa Naukowego z Uniwersytetem Krakowskim Połączonego*. All distinguished Kraków mathematicians published papers there (in Polish). In 1885 the Academy of Arts and Science started publishing the bulletin of the academy. In this journal, the series of mathematical science was included and there were also papers published in foreign languages. At the university, good mathematicians lectured and presented some interesting courses. The first mathematician who reached international fame and worked in Kraków appeared in the second half of the 19th century: Franciszek Mertens (1840–1927).

Mertens studied mathematics in Berlin. In 1865–1884 he headed a Chair at the Jagiellonian University. Then he moved to Graz and later to Vienna. He worked mainly on analytic number theory, algebra and mathematical analysis. His name is attached to the theorem about the multiplication of series. Other results of his are the determination of the sign of Gauss sums and an elementary proof of the Dirichlet theorem on quadratic form and prime numbers. However, nowadays, his name is probably known most of all because of the Mertens Conjecture. It says that the so-called Mertens function is bounded by the square root function. The result would have implied the Riemann hypothesis but the conjecture was proved to be false in 1985, almost 100 years after its statement. In some sources, Mertens is not presented as a Polish mathematician. Indeed, the matter is slightly complicated. He was born in a Polish town Środa (close to Poznań, then under Prussia). In his family he had Polish, French and German roots. But, importantly, Mertens regarded himself as a Pole, which follows from several documents in the Jagiellonian University archives and the Polish Academy of Arts and Science archives. Mertens spoke and wrote Polish perfectly and fluently. He published a lot in Polish, even when he moved from Kraków. Thanks to Mertens, who also lectured modern mathematics, students in Kraków could learn at a higher level.

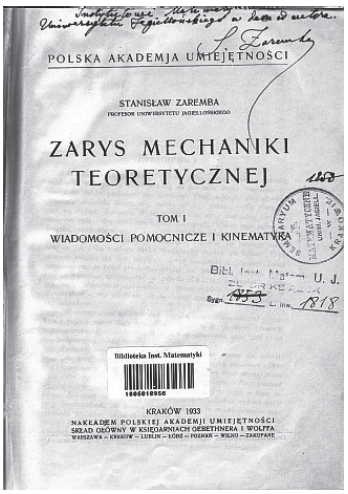
The position of Polish mathematics changed rapidly in the first half of the 20th century. The source of this was in Kraków, where the scientific activity of two mathematicians implemented modern mathematics at the university.

The most important role was played by Stanisław Zaremba (1863–1942), who is regarded as the best Polish mathematician at the end of the 19th century and the start of the 20th century. He studied in Petersburg where he got a diploma in engineering in 1886. Then he moved to Paris. In 1889 he obtained a PhD in mathematics from Sorbona. His doctoral dissertation was the solution of a problem stated by the French Academy of Science in 1858. Many mathematicians had earlier presented solutions which were not accepted, Riemann among them. Zaremba was known in France as an outstanding mathematician; he married a French lady Henriette Cauvin and he could have made a great career there, as Paris was a very important centre of world mathematics. However, he thought that in the Polish territory there was a need to introduce modern mathematics and he took a Chair at the Jagiellonian University in 1900. He started lecturing many modern topics, inviting several eminent mathematicians from abroad.



**Stanisław Zaremba**

The main scientific results of Zaremba were obtained in partial differential equations, especially concerning problems originating from mathematical physics and applications. Some of his most important results concern the elliptic equation $\Delta u + \xi u + f = 0$. The famous Zaremba example showing that the classical Dirichlet problem may have no solution is nowadays cited in classical textbooks as well as during plenary lectures at conferences. The beauty of this result was hidden in a very clever method of showing the nonexistence of any solution. Zaremba's list of publications contains over 100 items; according to Henri Lebesgue, Zaremba never




**The book on theoretical mechanics by Zaremba with his dedication for the Mathematical Institute of the Jagiellonian University**

wrote a needless paper. Zaremba was also an author of textbooks. He considered this aspect of mathematical activities as very important.

Another Chair was headed from 1895 by a great Polish mathematician Kazimierz Żorawski (1866–1953). Żorawski graduated from the Imperial University of Warsaw and got his doctorate in 1891 from the University of Leipzig. There he was interested in the theory of continuous groups, later known as Lie groups. His thesis, written under the supervision of Lie, concerned his preferred research topic, i.e. the equivalence of analytical or geometrical objects with respect to some group of transformation and the construction of differential invariants of such objects. Żorawski was the first Polish mathematician who worked actively on differential geometry. Among other results, he introduced some kind of generalisations of Christoffel symbols. He also presented some generalisations of the theory of a space with an affine connection, the theory which was created and developed later by Schouten and Weyl. Żorawski obtained many pioneering results, unfortunately most of them going unnoticed.

The work of Zaremba and Żorawski had already led to remarkable results before World War I. Many new courses were offered to students, including, for example, set theory. The standard of the lectures increased significantly. Many graduates worked on serious problems and later taught other students. A number of students appeared to be very good mathematicians and later on they had remarkable influence in the development of mathematics in Kraków. Still before World War I, more outstanding mathematicians started work in Kraków, in particular Antoni Hoborski (1879–1940) and Alfred Rosenblatt (1880–1947). Both obtained PhDs from the Jagiellonian University in 1908. Their advisor was Zaremba; however, they turned to other areas of mathematics. Hoborski worked in differential geometry and Rosenblatt was a pioneer of algebraic geometry in Kraków. Moreover, in 1911, another eminent mathematician got a Chair in the university, i.e. Jan Sleszyński (1854–1931). He was an author of papers in analytic functions theory and number theory and an original monograph about the theory of proof.

In 1893 the Maths and Physics Jagiellonian University Students' Society was founded. One of its founders and the first president was Zdzisław Krygowski. (Note that Krygowski, who later obtained a PhD from the Jagiellonian University, played a fundamental role in the development of mathematics at Poznań University which was created in 1919.) At the beginning of the 20th century the Students' Society worked very actively. It organised scientific meetings and published many lecture notes based on the lectures presented by the university professors. This society is probably one of the oldest students' organisations in the world and has been very active continuously up to present day; moreover, the students have not limited themselves to scientific events.


**The portrait of Zaremba in the office of the Jagiellonian University Students' Maths Society (nowadays)**

Also, it happened that mathematicians from other cities spent some time in Kraków. Wacław Sierpiński (1882–1969) from Warszawa (Warsaw) got his doctorate from the Jagiellonian University. He came to Kraków for the academic year 1905/1906 and presented his dissertation in 1906. Another Warsaw mathematician Stefan Mazurkiewicz (1888–1945) obtained his habilitation from the Jagiellonian University in 1919.

Stefan Banach (1892–1945) also had many connections with Kraków. Banach was born in Kraków and spent his childhood here but on completion of his secondary education in 1910 he decided to study engineering. He could not do it in Kraków, as there was no technical university, so he moved to Lwów. After a few years World War I began, Banach gave up this study and came back to Kraków. He enriched his mathematical knowledge by self-study and attended some lectures at the Jagiellonian University, in particular given by Zaremba. In 1916 Hugo Steinhaus (1887–1972), who was staying for some period in Kraków, during an evening walk at the Planty Gardens unexpectedly heard the words "Lebesgue integral". It turned out that two young people, Banach and Otto Nikodym (1887–1974), were talking about mathematics. During a talk, Steinhaus communicated to them a problem he was working on and Banach brought him the solution a few days later. Then Steinhaus realised that Banach had a superb mathematical talent. A couple of years later, Steinhaus got a Chair at the Jan Kazimierz

**The monument of Stefan Banach in Kraków (in front of the building of the former Mathematics Institute)**

University of Lvov and offered Banach a position of assistant at the Technical University of Lvov.

In 1918 Poland again became an independent country. This was a good period for some remarkable development of science. Great mathematical centres were created in Lwów (with Banach, Steinhaus and Mazur) and Warszawa (with Sierpiński, Mazurkiewicz and Kuratowski). Nevertheless, Kraków was also very important to Polish mathematics.

In an independent country it was possible to establish a national scientific society. In April 1919 the Constituting Session of the Polish Mathematical Society was held in Kraków. Zaremba was elected the first president of the society for a two-year period. Up to World War II the seat of the society headquarters was in Kraków and Zaremba was always the acting vice-president. It was Zaremba who (on behalf of Poland) signed in 1920 the act creating the International Mathematical Union, during the ICM in Strasbourg.

A new mathematical journal *Annales de la Société Polonaise des Mathématiques* was founded in 1921 in Kraków by Zaremba. The journal still exists but in 1953 it was taken by the Polish Academy of Science (like other Polish mathematical journals) and was continued as Annales Polonici Mathematici; nevertheless, the main editors have always been from the Jagiellonian University.

Zaremba continually played the main role in mathematics at the Jagiellonian University. Żorawski in 1917–1918 was the rector of the Jagiellonian University but soon moved to Warszawa. Hoborski took an active part in the creation of the new university in Kraków, i.e. the Academy of Mining (nowadays Akademia Górniczo-Hutnicza or AGH). He became its member of staff and the first rector but for many years he lectured at the Jagiellonian University as well. Rosenblatt continued his work. It is worth mentioning that in the Zentralblatt für Mathematik database there are 197 papers listed that were written by him. Several young, outstanding mathematicians, educated in Kraków, joined the mathematical staff at the Jagiellonian University, in particular Franciszek Leja (1885–1979), Witold Wilkosz (1891–1941), Tadeusz Ważewski (1896–1972) and Stanisław Gołąb (1902–1980). The mathematics teaching appeared to be at a remarkably high level. Mathematically, Kraków represented first of all mathematical analysis and related areas, especially differential equations, but several other advanced courses were also organised, for example on topology, geometry, number theory and algebra. In particular, there were courses on algebraic functions and Riemannian surfaces, on the Stieltjes integral and on Hilbert spaces. Also, many topics concerning different applications of mathematics were lectured. Among the mathematicians who delivered mathematical courses for a short period of time were: Jerzy Spława-Neyman (1884–1981) – a famous probabilist and statistician, known mainly for the results he obtained later in the USA; Włodzimierz Stożek (1883–1941) – later in Lwów; and Otton Nikodym (1887–1974) – later in Warszawa and after World War II in the USA.

Let us come back to mathematicians who had a great influence on Kraków mathematics in the period between the wars. Franciszek Leja studied in Lwów but in 1910 moved to the Kraków area and in 1913 got a position at the Jagiellonian University. In 1916 he obtained a PhD solving a problem stated by Lie. In 1924 he was nominated a professor at the Technical University of Warsaw. He spent 12 years there and thereafter came back to Kraków to take a Chair left by Zaremba after his retirement. Leja is regarded as a founder of the Kraków School of Analytic Functions. Nevertheless, the area of his mathematical research was much broader. Leja is particularly known because of the famous Leja's method of extremal points and Leja's polynomial lemma, which gives a uniform estimation for some family of polynomials in a neighbourhood of a sufficiently regular compact subset of $\mathbb{C}$. Moreover, it was Leja who first introduced topological groups.

Witold Wilkosz played a great role in the development of mathematics in Kraków. He was a schoolmate of Banach. Wilkosz, Banach and Nikodym for years discussed mathematical problems together. It was Wilkosz who in the 1920s reorganised the system of mathematical studies at the university. He presented a very broad mathematical interest and deep knowledge. His main results were from the foundations of mathematical analysis. He was well known as a man who always had time to discuss mathematical problems with others and delivered many popular lectures. Wilkosz wrote many textbooks on different branches of mathematics and some popular books. Also, for many years he was a scientific tutor of the Students' Maths Society; he succeeded Zaremba in those duties.

Of particular importance there is the role of Tadeusz Ważewski in the development of Kraków mathematics. Ważewski studied at the Jagiellonian University in 1914–1920. He started from physics but very quickly turned to mathematics. Ważewski was a pupil of Zaremba. He spent three years in Paris and got a doctoral diploma from Sorbona. Ważewski's research started from topology. In his doctoral dissertation he obtained interesting results on dendrites (locally connected continua not containing simple closed curves). Back in Kraków, he worked

for some time on topology and continua but quickly his interest turned to analysis and differential equations, especially topological methods in differential equations and qualitative theory. He obtained many deep and extremely valuable results. He also wrote some papers on control theory. He introduced the notion of asymptotic coincidence of solutions of differential equations which turned out to be very useful in further investigation by many others. Ważewski presented a very clever proof of the theorem of de l'Hospital rule where he managed to unify all the cases where the rule is applied. However, his most famous result is the Ważewski Retract Theorem from 1947. The retract method used for the investigation of the behaviour of solutions of differential equations led to many further and powerful results. In 1960 Solomon Lefschetz presented the opinion that Ważewski's retract method was the most original achievement in the theory of ordinary differential equations since World War II.

**Tadeusz Ważewski**

Stanisław Gołąb was a favourite pupil of Hoborski. Hoborski's dream was the creation of a strong centre of differential geometry in Kraków and Gołąb continued efforts in this direction. His doctoral paper, accepted by the Jagiellonian University, was prepared abroad, first of all in the Netherlands where he worked with Schouten. Gołąb's research was not restricted to geometry; he also wrote papers on analysis, topology, logics, and functional and differential equations. His most important results were obtained in differential geometry, especially concerning tensor analysis. Gołąb and Schouten introduced some rules for local tensor calculus, known as the "Kern-Indexe Methode". Gołąb is regarded as one of the creators of the theory of geometrical objects. He made a classification of several important families of such objects. He was also known as an excellent teacher and a man with a great sense of humour.

It should be noted that before World War II the results of Kraków mathematicians were so respected in the mathematical world that several of them were invited speakers at the International Congresses of Mathematicians. Up to 1939, invited lectures at ICMs were presented by S. Gołąb (3 times), F. Leja (3 times), A. Rosenblatt (3 times), T. Ważewski, W. Wilkosz and S. Zaremba (5 times).

Polish mathematics was struck very strongly during World War II. This was also the case for Kraków mathematicians. Zaremba, Hoborski and Wilkosz died. Lwów was moved to the Soviet Union and Lwów mathematicians who survived moved to other cities. Banach accepted an offer of a Chair at the Jagiellonian University but he died a few days before a planned transfer to Kraków. It was Ważewski who played the main role in rebuilding Kraków mathematics after the war.

The idea of this essay was to first treat this topic from an historical point of view, so post-war mathematics in Kraków will only be mentioned here. We restrict ourselves to mathematicians born before World War II and only some mathematicians will be listed. Note that some topics are discussed with more detail in the special issue of Wiadomości Matematyczne published on the occasion of the 6ECM in Kraków.

After World War II, the school of analytic function established by Leja grew into a large mathematical school of several complex variables, led for many years by Józef Siciak (b. 1931). He obtained many remarkable results in this area. The function known as Siciak's extremal function is a fundamental tool in pluripotential theory. Some of Siciak's pupils turned to other areas of mathematics which became the origin of subsequent groups, in particular working on approximation theory and algebraic geometry. The school of geometry, led by Gołąb, became much stronger than it had been before the war. After some time a group was formed working on functional analysis. Ważewski's work led to the creation of the Kraków School of Differential Equations, known also as the Ważewski School. Let us list some of Ważewski's pupils.

Jacek Szarski (1921–1980) wrote many important papers on differential equations and differential inequalities, as well as a fundamental textbook on differential inequalities, the first complete monograph on the subject. He was probably the youngest ever recipient of a PhD in mathematics from the Jagiellonian University. Zdzisław Opial (1930–1974) was a mathematician with a very broad mathematical interest and an author of outstanding results in differential equations, especially in second order ordinary equations. The Opial inequality appears frequently in the literature. He also worked in the history of mathematics and was very active in many aspects of mathematical education. He is regarded as one of the most brilliant Kraków mathematicians in history; unfortunately, he tragically died young. Andrzej Pliś (1929–1991) obtained remarkable results in the theory of ordinary and partial differential equations. He is known particularly for the creation of many sophisticated and original counterexamples. Andrzej Lasota (1932–2006) moved from Kraków to the Silesian University in Katowice in 1976 but to the end of his life he had strong connections with the Jagiellonian University. He was an author of outstanding results in differential equations, probability, ergodic theory and fractals. He worked very actively in the applications of mathematics. Together with Maria Ważewska-Czyżewska (the

daughter of Ważewski), from the Medical University in Kraków, he gave a mathematical model of the process of reproduction of blood cells. Czesław Olech (b. 1931), a member of staff of the Kraków branch of the Polish Academy of Science but lecturing also at the Academy of Mining and Metallurgy and the Jagiellonian University, moved from Kraków to Warszawa in 1970. A large number of his magnificent results concern ordinary differential equations and control theory. He proved some theorems connected with the famous Jacobian Conjecture. Andrzej Pelczar (1937–2010) obtained valuable results on stability and several generalisations of the retract theorem. He worked actively in the history of mathematics. Under Pelczar's direction, the next group working on topological methods and dynamical systems was created. He was a rector of the Jagiellonian University and a vice-president of the European Mathematical Society.

Stanisław Łojasiewicz (1926–2002) wrote his doctoral dissertation under Ważewski's supervision but he did not work on differential equations. Łojasiewicz was one of the most outstanding Polish mathematicians of the second half of the 20th century. He solved a fundamental problem of the division of distributions by analytic functions, which led to the creation of a new branch of mathematics, i.e. semianalytical geometry. In the literature, we read now about the Łojasiewicz inequality and Łojasiewicz exponents. Another scientific mathematical group created in the Jagiellonian University emerged under Łojasiewicz's leadership, concentrating on semianalytical geometry and singularities.

In addition note that when John Paul II visited Poland in 1987, a special meeting with the Pope was organised in Lublin for a group of scientists. Most of the mathematicians invited there were Ważewski's PhD students.

Soon after World War II, two new universities with mathematical departments were established in Kraków. Kraków Technical University (Politechnika Krakowska) was formed from some faculties of the Mining Academy. Kraków Pedagogical University was intended mainly to educate school teachers. Anna Zofia Krygowska (1904–1988) who achieved international fame in the didactics of mathematics worked there. It should be noted that Krygowska got her PhD from the Jagiellonian University on the basis of a paper on geometry and it was Ważewski who was her supervisor.

To end the post-war story, let us emphasise that among 19 presidents of the Polish Mathematical Society after 1945 there were five from the Jagiellonian University: Ważewski, Leja, Szarski, Pelczar and Bolesław Szafirski (b. 1935). No other Polish mathematical institution gave such a number of presidents to the society after World War II.

## References[2]


[1] D. Ciesielska, K. Ciesielski, Stefan Banach remembered in Kraków, *Math. Intelligencer* 30 (2008) no. 4, 31–35.

[2] K. Ciesielski, 100th anniversary of the Jagiellonian University Students' Maths Society, *Math. Intelligencer* 17 (1995) no. 1, 42–46.

[3] K. Ciesielski, Z. Pogoda, Conversation with Andrzej Turowicz, *Math. Intelligencer* 10 (1988) no. 4, 13–20.

[4] R. Duda, Facts and Myths about Stefan Banach, *European Math. Soc. Newsletter* 71 (2009), 29–34.

[5] E. Jakimowicz, A. Miranowicz (eds.), *Stefan Banach. Remarkable life, brilliant mathematics*, Gdańsk University Press, Gdańsk, 2010.

[6] R. Kałuża, *Through reporter's eyes: The life of Stefan Banach*, Birkhäuser 1996.

[7] J. Kowalski, Polish Mathematical Society, *European Math. Soc. Newsletter* 54 (2004), 24–29.

[8] A. Pelczar, Selected Chapters of the History of Mathematics in Poland, in: *From shared traditions to prosperous bilateral future in Swiss-Polish relation* (Proceedings of the Conference: Swiss-Polish Cohesion Dialogue between Science, Economy and Culture, Bern, 22 November 2007), Empa, Bern, 2009, 49–62.

[9] A. Pelczar, Stanisław Zaremba (120th anniversary of obtaining Ph.D. at the Paris University), *Copernicus Center Reports* 1 (2010), 91–119.

[10] J. Piórek, Polish Mathematical Society: From the minutes of the Mathematical Society in Cracow, *European Math. Soc. Newsletter* 32 (1999), 17–18.

[11] Z. Pogoda, Kazimierz Żorawski and the Cracow Mathematical School, in: *31 Mezinárodní Konference Historie Matematiky,* Velké Meziříčí, 2010, (J.Bečvář, M.Bečvářova, eds.) Matfyzpress 2010, 211–216.


*Reprinted with permission from Wiadomości Matematyczne*

*Krzysztof Ciesielski [Krzysztof.Ciesielski@im.uj.edu.pl], left, and Zdzisław Pogoda [Zdzislaw.Pogoda@im.uj.edu.pl] work at the Jagiellonian University in Kraków, from which they obtained their PhDs. Ciesielski's specialty is dynamical systems and Pogoda's specialty is differential geometry and its applications. They also work on history of mathematics. They work actively in raising public awareness of mathematics in different areas and they have coauthored several hundreds of popular articles and a few books. For their books they received the prestigious Steinhaus Award from the Polish Foundation for Science Advancement and the Main Dickstein Prize of the Polish Mathematical Society.*

2 The list of references is far from complete. As the special issue of *Wiadomości Matematyczne* was intended for English-speaking readers, no reference in Polish is cited.

# Public Key Cryptography, Number Theory and Applications

Preda Mihăilescu (University of Göttingen, Germany) and Michael Th. Rassias (ETH Zürich, Switzerland)

*In this article we review the advent and development of public key cryptography. The exposition is driven by the application aspect, while providing more details for certain issues in which beautiful number theory is involved.*

## 1 Introduction

In the early 1970s, the US army entertained the ARPA-net, an ancestor of the internet, and between 1972 and 1974 a number of universities on the East and West Coast were connected to this net for research and experimental purposes. The notion of remote computer-communication became tangible for the users of the net. It is conceivable that, under these conditions, the question of how to communicate in a secure way in a wide area net – like the ARPA – became an actual reality for those using the net. In fact, the concept of public-key cryptography, which gives the simple conceptual frame for algorithms successfully solving this problem, was born in Stanford from the joint work of W. Diffie and R. Hellman who studied public key infrastructures and R. Merkle who studied secret key distribution. Here is the way Diffie and Hellman presented the problem in [DH], a paper which mentions the joint work with Merkle: "In turn, such applications (fast computers) create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature."

### Public Key Cryptography arises

The idea was remarkably simple and efficient. Traditionally, a protected communication was established by using secret key cryptography. Two major characteristics of this craft, which still played an important role during the Second World War, are that the sender and receiver must agree upon a common secret key prior to communication and that it was a widespread conception that keeping the encryption method secret was a sensible method for increasing security. In a wide area communication network, in which numerous peers can communicate over large distances, the chance of establishing a common secret key prior to communication are low. This was more than just an abstract realisation of the inventors of public key cryptography; it was a fact of which all users of the ARPA-net were aware.

The new concepts are widely known and are currently taught in school. We will briefly review them in order to introduce notation which will be useful when discussing some interesting instances, allowing us to bring in more mathematics. If $X$ is any peer who wants to engage in secure network communication, he should start by generating a set of data, which is bundled into his own *secret key* $S_X$. A subset of this data, bundled in the *public key* $P_X$ will be made public to all peers with whom he might wish to communicate. The two keys should have the following two properties:

1. Both keys can be used for encrypting texts according to some algorithm yet to be defined; messages encrypted by $S_X$ can be decrypted by $P_X$ and vice versa. Moreover, the keys should be sufficiently random: the chance of two peers accidentally generating the same secret key should be close to zero.
2. It should be computationally unfeasible to derive $S_X$ from $P_X$.

On the basis of these premises, if two peers A and B – cryptographers like using names so these peers are often called Alice and Bob – want to communicate, then Alice sends to Bob messages encrypted by $P_B$, which she may retrieve from the public key repository. However, only Bob can decrypt the message so the communication is secure. On the basis of this idea, a further application emerged: it is often useful to be able to certify the ownership of some message, to *sign* the message in a unique and non-repudiable way. In this case, secrecy is less of a concern than ownership. The solution consists of associating a short cryptographic *hash-value* $H$ to the message, which is encrypted by the secret key $S_A$. Any receiver will then be able to regenerate the hash value on their own, decrypt the encrypted hash with $P_A$ and then compare the two results. If they match, Bob has a proof that it was Alice who has sent the message. It was in the same context that the paradigm was set that security of encryption algorithms is increased by their becoming public and not the contrary, as had been previously perceived. The reasoning behind this is that algorithms known to the scientific community would be well analysed and the process of academic scrutiny would help select the most secure and efficient algorithms. *Security lays solely in the secrecy of the keys* is the slogan of this paradigm. In fact this sensible point of view quickly spread within the scientific community. Public key cryptography changed not only the concept of secret communication but also the way of perceiving security: an algorithm is more reliable when it has long resisted public scrutiny by the cryptographic community and not when it is based on sophisticated "secret tricks". Within the next 20 years this point of view probably reached most of the banks. In the late '90s, manufacturers of cryptographic hardware had only a precious few customers insisting on the "privilege" of purchasing machines which ran according to some unique and "secret" algorithm.

### The invention of the classical systems: DH and RSA

In the next two years after the abstract definition of public key cryptography, two major algorithms that implement this idea and are still in use today were invented. The first is based on the difficulty in solving the *discrete logarithm* problem in the multiplicative group of finite fields and it was proposed

by Diffie, Hellman and Merkle, the inventors of public key cryptography. The algorithm was initially meant to serve for a variant of the public key cryptography idea, in which Alice and Bob only wish to establish a shared secret key – they do not wish to encrypt with the same algorithm; rather, they will proceed by using the secret key for some classical, faster secret key encryption scheme. Incidentally this two-step approach to encryption is the core idea in the TSL protocol, developed between 1992 and 2002 and currently used in all confidential https communications on the internet – for instance when you book a flight or buy a book from Amazon.

If $\mathbb{F}_q$ is some large finite field and $g \in \mathbb{F}_q^\times$ is a generator of the multiplicative group of the field – both being public data – then Alice and Bob start by choosing some random one time keys $A_R, B_R$ which are elements of $\mathbb{Z}/((q-1)\cdot\mathbb{Z})$. Then Alice sends to Bob $M_A = g^{A_R}$ and receives from Bob $M_B = g^{B_R}$. The reader can verify that by using the private data and the data received, both Alice and Bob may retrieve $S = g^{A_R \cdot B_R}$, which is the data from which the common secret key is extracted. However, an eavesdropper, who is always called Eve[1] in cryptography, would only know $g^{A_R}$ and $g^{B_R}$ but not $A_R$ or $B_R$. The problem of recovering these secret data from the ones communicated on the net is the discrete logarithm problem in finite fields, which is known to be a hard problem.[2] It is however not hard in the strong sense of complexity theory, since it is not known to reduce to any NP complete problem; the same holds in fact for the problem of factoring integers. The procedure is widely known as the *Diffie-Hellman key exchange algorithm* and it does not provide a direct solution to the problem of public key encryption/decryption and of signatures.

This was provided one year later, in 1977, by R. Rivest, A. Shamir and L. Adleman at MIT. Their algorithm, widely known as RSA after the initials of their names, uses the problem of factoring integers as the problem intended to prevent recovery of the secret key from the public ones. A secret key consists of $S_A = \{p, q, d\}$, where $p, q$ are two large primes satisfying some additional randomness conditions and

$$0 < d < (p-1)(q-1), \quad \text{with} \quad (d, pq(p-1)(q-1)) = 1$$

is a random number; if

$$e \in \mathbb{N} \text{ such that } ed \equiv 1 \bmod (p-1)(q-1),$$

the public key consists only of $P_A = (n, e)$, with $n = p \cdot q$. In some instances $e$ is a fixed number for the whole system, so $d$ will be determined by the holder of the secret key using the same defining congruence. With these prerequisites, if $M$ is a short message, it will be identified with a number in $\mathbb{Z}/(n\cdot\mathbb{Z})$ and its public key encryption $M_e \equiv M^e \bmod n$ can be computed in the open but can only be decrypted by Alice, the holder of $d$, since $M \equiv M_e^d = M^{ed} \bmod n$. Conversely, if Alice encrypts $M$ with $d$, then anyone can recover $M$ and upon doing so will have proof of Alice having produced the encryption; indeed, only the owner of the secret key could produce this encryption, which can thus act as a private signature of Alice.

In 1978, Hellman and Merkle invented a public key cryptosystem that did not rely on number theory but rather on the NP-complete *knapsack* problem. In 1983, J. L. Massey and J. K. Omura developed a variant of the Diffie-Hellman key exchange, which works as a public key encryption scheme too. It has the advantage that, like for the key exchange, a single public key can be used by a whole *domain* – the public key consists of a large prime $p$ and a generator $g \in \mathbb{F}_p^\times$.

Despite initial attempts of the NSA to inhibit the publicising of the ideas of public key encryption and RSA, these had already been brought to public perception in 1977 by Martin Gardner in his widely read column Mathematical Games in the Scientific American magazine and were eventually published in the communications of the ACM [RSA]: the way to public key cryptography was open! While the NSA tried to stop the diffusion of the public key idea, it turned out that the idea had already been invented in 1970 by a researcher for MI6's General Communication Head-Quarters GCHQ, who had also discovered the DH and RSA algorithms in 1971 and 1972 … but in the reverse order, with RSA discovered first. The information was declassified and made public in 2000 and the director of RSA's research team Dr Burt Kaliski confirmed the truth of the information. This news was accepted with some reticence by the community, which speculated upon an a posteriori wish for academic acknowledgement from a person who had accepted working in secrecy. However, both the idea and the most widely spread instances of public key cryptography have the making of good mathematical work - they were discovered independently by people working on the same question.

## 2 Cryptanalysis

The first major success of public key cryptography was that the expectation came true and the domain of cryptanalysis – concerned with the analysis of possible attacks against cryptographic schemes – became a flourishing academic domain of investigation. One of the most spectacular successes was due to the development of the *lattice reduction* algorithm by A. Lenstra, H. Lenstra Jr. and L. Lòvasz, the LLL-algorithm. Given a lattice $\mathcal{L} \subset \mathbb{Z}^n$, there exists a base consisting of shortest vectors. Classical algorithms for finding such a base are known from the work of Charles Hermite. Only, in the case when the base is presented by an initial generating system of very large vectors, the process is exponential. The algorithm was developed from techniques used by Lòvasz in integer programming; the idea was to use an approximate Gram-Schmidt-reduction which provides some *close* to minimal vectors in $\mathcal{L}$. The advantage is that the algorithm runs in polynomial time and has therefore a wide variety of applications both in cryptography and in number theory itself. One of the first applications of LLL was in showing that the keys of the knapsack cryptosystem could be cracked in polynomial time: in order to do that, one had only to solve a particularly simple *subfamily* of problems belonging to the knapsack family. This result showed the advantage of public academic scrutiny of cryptographic schemes, since it had only taken five years to reveal the weaknesses of one of them, but it also blocked the way for applications of the knapsack. Some improved versions have been presented that could never be attacked – but they never made it to public applications.

The most important effect of cryptanalysis was less visible. The community quickly developed its own language and defined a variety of subtle *attack scenarios*, in which the eavesdropper *Eve* was offered increasing levels of advantages:

Eve can simply tap a wire communication or she might also collect large amounts of data signed by Alice or even induce her into signing a chosen suite of messages. Later, the encryption hardware began being regarded as a point of attack, as it was observed that physical measurements on a chip while it is computing an RSA encryption may reveal some bits of the secret key. In this way, well defined attack scenarios are used for checking the security of various cryptosystems and protocols.

This is a good place to mention the fact that cryptography advances with a tension between the needs for security and for efficiency. It has happened repeatedly that the latter has led to the usage of particular constellations of keys that allow for faster computations. But eventually, when simplification has reached too far, an attack has been discovered; certain keys, or even whole cryptographic schemes, are then discarded. It is for instance useful to have a universal, short public exponent $e$ for the RSA scheme and this had also been used in practice in the late 1980s. But D. Coppersmith showed that if $e$ is too small, it is easy to gather sufficiently many messages signed by the same key $S_A$ and then use simple arithmetic in order to crack that key. Therefore, the smallest fixed key currently allowed by standards is $e = 2^{16} + 1$ and this may change with the growth of computing and storage capacities.

It is easy to verify that an efficient method for factoring integers breaks the RSA scheme and a solution to the discrete logarithm problem breaks the DH key exchange and the Massey-Omura cryptosystem. On the other hand, there is no proof either for the expectation that efficient attacks on RSA are equivalent (in a complexity theory understanding) to factoring integers, or that breaking the DH scheme is equivalent to solving the discrete logarithm problem. In fact various scenarios of cryptanalysis investigate conditions under which successful attacks can be completed *without* solving the underlying hard problems.

The closest mathematical problem is the *DH*-problem: given a prime $p$ and a generator $g \in \mathbb{F}_p^\times$, let

$$A = g^a, B = g^b, C = g^{ab} \in \mathbb{F}_p$$

be given for unknown $a, b \in \mathbb{Z}/((p-1)\cdot\mathbb{Z})$; find the values of $a$ and $b$. It is used for theoretic analysis of provable security of cryptographic schemes, the investigation of which was initiated by Maurer [Ma] and established by Shoup and various coauthors, e.g., in [CS].

## Dickman's Theorem and its impact

In the 1930s, J. Dickson considered the question of estimating the largest prime factors of some random integer $n$. Using heuristic estimates on the repartition of primes he found for instance that if $p|n$ is the largest prime dividing $n$ then $p = O(n^{\ln 2})$. More generally, an integer $n > 1$ is $y$-smooth if none of its prime factors exceeds $y$. The function

$$\psi(x, y) = \sharp\{\ 1 \le n \le x\ :\ n \text{ is } y\text{ - smooth }\}$$

counts the smooth numbers less than $x$. Dickman also proved that for all $u > 0$ there is a real number $\rho(u)$ such that

$$\psi(x, x^{1/u}) \sim \rho(u)x.$$

The function $\rho(u)$ was described in terms of a differential equation, in which $u$ was fixed for $x \to \infty$. Half a century later, the gap was filled by Canfield, Erdős and Pomerance [CEP], who proved that

**Theorem 1** (Canfield, Erdős and Pomerance)**.**

$$\begin{aligned} \psi(x, x^{1/u}) &= xu^{-u+o(u)}, \\ &\quad \textit{uniformly, for} \\ u &< (1-\epsilon)\ln x/\ln\ln x \textit{ when } u \to \infty. \end{aligned} \tag{1}$$

This theorem is at the heart of all the state-of-the-art algorithms for factoring integers and discrete logarithm in multiplicative groups. The classical application to factoring integers is the *quadratic sieve method* and it has its origin in the following simple observation of Fermat: if $m$ is a composite integer then the congruence $x^2 \equiv c \bmod m$ will have at least four solutions and there are $x, y$ such that $x \not\equiv \pm y \bmod m$ but $x^2 \equiv y^2 \bmod m$. Then $(x + y, m)$ is a nontrivial factor of $m$. Theorem 1 helps find such pairs $x, y$, as follows: for numbers $x(i)$ in some interval $\lceil \sqrt{n} \rceil + i, 0 \le i \le B$, one computes the remainder[3]

$$r(i) = x(i)^2 \ \text{rem}\ m$$

and retains only those values of $x$ for which $r$ is a $B$-smooth number. By choosing $B$ accordingly, it is possible to factorise $r(i)$ efficiently. After gathering sufficiently many such relations, one may hope that the product of some $r(i)$ is a square: namely, that there is an index subset $J \subset [0, B]$ such that

$$\prod_{i\in J} r(i) = R^2,\ R \in \mathbb{Z}.$$

Then letting $X = \prod_{i\in J} x(i)$, we obtain the congruence $X^2 \equiv R^2 \bmod m$. If, in addition, $X \not\equiv \pm R \bmod m$, which should happen with probability $\ge 1/2$, then $(X \pm R, m)$ is a nontrivial factor of $m$. The method relies on some empirical assumptions on the repartition of factors of $r(i)$: namely, that the distribution of these residues is such that one may apply the relation (1) for estimating the probability that one of these numbers is $B$-smooth. These allow one to establish an *optimal* bound

$$B \sim \exp(\sqrt{\ln(m)\ln\ln(m)}).$$

This and similar functions occur often in algorithms using smoothness, so it received a name:

$$L(n; a) := \exp\left(\ln(n)^a \ln\ln(n)^{1-a}\right).$$

In our case $B = L(n; 1/2)$ and the quadratic sieve runs in time polynomial in $B$ – experience having so far confirmed the underlying heuristical assumptions. The following nice example is taken from the book of R. Crandall and C. Pomerance [CP]: let $m = 1649$, with $41 = \lceil \sqrt{m} \rceil$. We find

$$41^2 \equiv 32 \bmod m; \quad 42^2 \equiv 115 \bmod m; \quad 43^2 \equiv 200 \bmod m.$$

Since $32{\cdot}200 = 2^{5+3}{\cdot}5^2 = 80^2$, we let $R = 80$ and $X = 41{\cdot}43 = 42^2 - 1 \equiv 114 \bmod m$, finding that $114^2 \equiv 80^2 \bmod m$ and eventually $17 = (114 - 80, 1649)$, which is a nontrivial factor.

For the discrete logarithm problem in $\mathbb{F}_p^\times$, which consists of determining $x$ such that $g^x \equiv b \bmod p$, one uses smooth numbers as follows. Fix a smoothness bound $y$ and let $q_1, \ldots, q_r < y$ be all the primes up to $y$. For random values of $m$, one computes $u = g^m \text{ rem } p$ and keeps only those values of $u$ which are $y$-smooth. After collecting sufficiently many relations, one will then be able to compute the discrete logarithms $l_i$ such that $q_i \equiv g^{l_i} \bmod p$. Next, one tries random values of $k$ searching such ones that make $v = bg^{-k} \text{ rem } p$ be a $y$-smooth number. The precomputed values $l_i$ will then help determine $x = k + \log_p(v)$ from the prime decomposition of

the $v$. This algorithm also relies on heuristic assumptions, on the basis of which the running time is $L(p, 1/2)^{\sqrt{2}}$.

At the end of the 1980s, John Pollard found a way of applying the idea of the quadratic sieve to integers in number fields rather than $\mathbb{Q}$. The method was first applied to the factorisation of the Fermat number $F_9 = 2^{2^9} + 1$. In the following years, it was generalised and improved by a series of mathematicians, starting with A. Lenstra and M. Manasse. The resulting number field sieve is currently the asymptotically fastest factoring method and it runs in time $O(L[n; 1/3])$. Similar methods are known for the discrete logarithm method: they use number fields in case of larger characteristics and function fields for small characteristics. Like in the case of factoring, their running time is also $O(L[n; 1/3])$. Current records reach as high as 7–800 binary digits for factoring composites of general form and ~ 5–600 for the discrete logarithm in prime fields.

## 3 Elliptic curves

In 1984, René Schoof opened the way for discovery of a polynomial time algorithm for counting the number of points on an elliptic curve over a finite field. This brought the groups of algebraic geometry to the realm of applications and algorithms. Within one year, H. W. Lenstra Jr. proposed an important variant of Pollard's rho-method for factoring, based on elliptic curves: the *ellptic curve method* or ECM. Also, V. Miller and N. Koblitz proposed independently the use of elliptic curves for cryptography. The ECM method has a runtime comparable to the quadratic sieve but it behaves particularly well for numbers $m$ which have some small prime factors (i.e. sensibly smaller than $\sqrt{m}$: the runtime is estimated to be $L(p; 1/2)^{\sqrt{2}}$, where $p$ is the smallest prime dividing $m$).

### Counting points

The idea of Schoof is both elegant and important, beyond even the immediate algorithmic and cryptographic applications: it led to an area of research for practical algorithms for counting points on finite varieties. This research area is still growing, while the main domain of application has ceased to be cryptography for at least a decade. The algorithms are more and more used for larger computations related to mathematical questions such as the Birch Swinnerton-Dyer conjecture and other properties of $L$-series. See also [Ra] for an interesting elementary theoretical application of point counting.

Initially, Schoof [Sc1] started from the following simple remark: if $E_p(a, b) : Y^2 = X^3 + aX + b$ is an elliptic curve defined over the finite field $\mathbb{F}_p$, of which one assumes that it is ordinary, then Riemann's conjecture for elliptic curves implies that, in $\mathrm{End}(E_p, \overline{\mathbb{F}}_p)$, the Frobenius verifies the quadratic equation

$$\Phi^2 - t\Phi + p = 0. \tag{2}$$

Since $E_p$ is fixed by $\Phi$, we have $|E_p(a, b)| = p - t + 1$. Counting the points is thus equivalent to determining the value of the *trace of the Frobenius* $t$; since the Hasse inequality states that $t < 2\sqrt{p}$, it suffices to determine the remainder $t \mod \ell$ for some small primes with

$$L = \prod \ell > 2\sqrt{p}.$$

Therefore, the core step of the algorithm consists of modelling the $\ell$-torsion $E_p[\ell]$ into an algebra

$$\mathbb{B} = \mathbb{F}_p[X, Y]/\left(\psi_\ell(X),\ Y^2 - (X^3 + aX + b)\right),$$
$$P = \left(X + (\psi_\ell(X)),\ Y + (Y^2 - (X^3 + aX + b))\right) \in \mathbb{B},$$

in which $\psi_\ell(X)$ is the $\ell$-division polynomial which has as roots all the $x$-coordinates of $\ell$-division points. Therefore, any such point enjoys the properties which define the *generic* $\ell$-torsion point $P \in \mathbb{B}$. It is then a straightforward computation to determine $t \mod \ell$ from the identity

$$\Phi^2 P + pP = t\Phi P.$$

The seminal idea of Schoof to determine the parameters of the Riemann $\zeta$-function from projections in torsion spaces, and thus counting points on varieties over finite fields, was both improved for simple varieties, such as elliptic curves, and extended to more general abelian varieties. In the first case, the primary thing to do was to reduce the size of the algebra $\mathbb{B}$ – which can be done by finding smaller factors of $\psi_\ell(X) \bmod p$.

The breakthrough in this direction was indicated by Noam Elkies (see [Sc2]), who brought in modular forms, thus showing how to find in half of the cases some factors $f(X)|\psi_\ell(X)$ of linear degree, compared to the quadratic degree in $\ell$ of the division polynomial. The $\ell$-torsion $E_p[\ell] \cong \mathbb{F}_\ell^2$ as a vector space, fixing two linear independent points $P, Q \in E_p[\ell]$, we see that $G := \mathrm{Gal}\,(\mathbb{B}/\mathbb{F}_p)$ acts on the vector space $E_p[\ell]$ by acting on the base $P, Q$. We obtain a representation $\rho : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$, with respect to which $\rho(\Phi)$ verifies the same quadratic equation. If $\delta$ is the discriminant of this equation, according to the value of the Legendre symbol $\left(\frac{\delta}{\ell}\right) \in \{1, 0, -1\}$, the matrix $\rho(\Phi)$ is diagonalisable, has normal upper triangular form or has eigenvalues in $\mathbb{F}_{\ell^2}$. In the first case, there are two *eigenpoints* $P, Q$ of the Frobenius and the orbit of their $x$ coordinates under multiplication on the curve is galois invariant. We obtain the *eigenpolynomials*

$$f_P(X) = \prod_{k=1}^{(\ell-1)/2} (X - ([k]P)_x) \mid \psi_\ell(X),$$

where

$$\deg(f_P) = (\ell - 1)/2 \quad \text{and} \quad \deg(\psi_\ell) = (\ell^2 - 1)/2,$$

together with a new algebra $\mathbb{B}'$, obtained by replacing $\psi_\ell$ with $f_P$. For the computation of $F_P$, Elkies considered the function field $\mathbb{C}[[j(q)]]$. Some classical arguments on Eisenstein series and $\Gamma_0(\ell)$-modular forms imply that for each $j$-invariant $j_m$ of an $\ell$-isogenous curve to $E_p$ – or, also, for each zero of the modular equation $\Phi_\ell(X, j(q))$ – there is a polynomial $f_j(X) \in C[[j(q)]][X]$ which has the $x$-coordinates of the kernel of the respective isogeny as zeroes. The polynomials can be constructed in the function field by manipulations of $q$-expansions and they have the useful property that all the coefficients are algebraic integers. The insight of Elkies was to show that one can substitute for $j_m$ the value of some zero $\Phi_\ell(X, j(E_p)) \bmod p$ and reduce the coefficients of $f_j(X)$ modulo $p$, thus obtaining some eigenpolynomial corresponding to the value of $j_m$. Indeed, if $\mathbf{E}$ is any curve over $\overline{\mathbb{Q}}$ which reduces to $E_p$ at some prime ideal above $p$ then its $j$-invariant reduces to the one of $E_p$ and so do the invariants

of its $\ell$-isogenies. Therefore, if the modular equation has linear factors $j_m$ over $\mathbb{F}_p$, by inserting these in the expression for $f_j(X)$, upon reduction at the same prime, the coefficients of the polynomial $f_j$ map to the ones of some eigenpolynomial. Using improved algorithms for manipulation of series [BMSS], one can compute the eigenpolynomials in time $O(\log^3(p))$, the running time being dominated by the computation of zeroes of $\Phi_\ell(X, j(E_p)) \bmod p$. Further improvements can be achieved by using the galois structure of the resulting algebras [MV].

For curves defined over finite fields of small characteristic $p$, it is possible to project to $p^N$-torsion. Using different flavours of cohomology combined with Newton iterations, various authors starting with T. Satoh, K. Kedlaya and A. Lauder have developed the most efficient point counting algorithms for elliptic curves. Some of them are generalised to super elliptic curves, elliptic surfaces, etc.

### Cryptography

The elliptic curve based cryptographic schemes which have survived scrutiny and become part of current standards on public key cryptography are essentially variants of the Diffie-Hellman key exchange scheme and are based on the difficulty of solving the discrete logarithm problem: find $x$ such that

$$[x]P = Q, \quad \text{for} \quad P, Q \in E_p(a, b)$$

being points on an elliptic curve, such that $Q$ is known to generate a cyclic group of high order. Unlike in finite fields, the DL problem on elliptic curves is not known to allow any sub-exponential time solutions. The best known methods have runtime $O(\sqrt{p})$, where $p$ is the characteristic of the (prime) field over which $E_p$ is defined. As a consequence, one can work in much smaller groups than in the case of the multiplicative groups of finite fields, still achieving the same estimated security of a scheme, with respect to state-of-the-art attacks. This advantage led to a new wave of interest for elliptic curve cryptography in connection with security of mobile phones. Over the last two decades, the evolution in this direction oscillated between the search of special curves with most efficient group operations[4] and the care required to maintain security, when using special cases. The core problem in this respect is the reduction to the discrete logarithm in finite fields, using Weil pairings and descent methods. The use of the Weil pairing for the discrete logarithm on some special elliptic curves was pointed out for the first time by Gerhard Frey. The problem came to light when Frey was asked to estimate software using special curves with fast group operation for its security. He was able to show that for the specific curves, the Weil pairing reduced the elliptic curve logarithm problem to one in finite fields of critically small size. The idea was taken over by A. J. Menezes, P. C. van Oorschot and S. A. Vanstone and is currently known in the literature under the name of *MOV attack*. Much experience has been gathered in this field yet, even nowadays, the attraction of efficient arithmetic for mobile phones leads to the use of special curves – e.g. the so-called Koblitz curves, defined over fields $\mathbb{F}_p$ of small characteristic and having $a, b \in \mathbb{F}_p$ – which are close to the critical area where one may expect that reduction to some feasible discrete logarithm in finite fields is just one idea away. Despite standardisation, which made cryptographic developments obsolete on the internet, there are thus reasons why research in this particular area is still very fertile. We recommend the detailed and lively survey of Heß et al. [HeSSL].

## 4 Quantum cryptography and other interesting applications

The main intensively used public key cryptography methods rely on the number theoretic problems described above. There have been numerous interesting attempts to use the large list of NP complete problems in order to derive some trapdoor function (the one allowing the concealment of the secret key behind the public ones) – the knapsack problem is only one of the most famous ones. We can hardly go into the detail necessary in order to pay justice both to the interest of the attempts and the reasons for their failure or restricted use.

One cannot complete even a brief survey of public key cryptography without mentioning several examples which have withstood the test of time and do have either a theoretical interest or even a practical niche of application. Since the early 1980s the Canadian mathematicians G. Brassard and C. Crépeau have suggested the use of quantum effects for security applications: the simple idea was that Eve could not tap a quantum communication wire without destroying the information content transmitted, so security would be provided by a *self-destruction mechanism* introduced by quantum mechanics in the confidential information transmitted. The physical and cryptographical aspects of the idea have been in active research ever since and, in the first decade of this century, several practical implementations of quantum[5] cryptography have been announced, reaching over distances of up to 100 km.

Public key cryptography is much slower than secret key encryption – by at least a factor of 1000, as a rule of thumb. This has led to the wish to design some fast asymmetric schemes, even at the cost of, say, very large keys. A successful solution in this respect was invented by three number theorists: J. Hoffstein, J. Pipher and J. H. Silverman, who called their method "Number Theorists aRe Us": NTRU [HPS]. The method found a niche of applications and has the intriguing property that lattice reductions are used both for legitimate decryptions as well as for attacks. The asymmetry is thus not one between polynomial and exponential algorithms but is rather due to the high dimensions of lattices in which reduction must happen for the attacker.

A further family of interesting public key schemes uses non commutative groups – such as, for instance, *braid groups* (e.g., see [MSU]). Their developers make a point out of the fact that, if one day quantum computing is feasible, all number theoretic schemes can be broken in short polynomial time. However, using the current models of quantum computing, no attack to braid group cryptography is known.

## Notes

1. This is one of the few instances of which we are aware in which a politically incorrect denomination introduced in the '70s, was neither revindicated nor changed up to the present. The reason

may possibly lay in the fact that political correctness lacks fantasy, so people can hardly imagine Adam offering the apple to Eve.

2. It has been neither proved nor disproved that solving the discrete logarithm problem is the only way for Eve to recover the secret key $S$. Since this is an independent problem of interest on its own, it has received more recently a name: the DH - Problem, after Diffie-Hellman.
3. In computational algebra, the notation $x$ rem $y$ stands for the unique representative of the equivalence class of $x$ mod $y$ which lays in the interval $[0, y)$.
4. On the one hand, the base fields are much smaller – 200 bits for the size of the base fields is still a very safe bound, which compares well, in terms of security, to RSA moduli of over 1000 bits – but on the other hand additions on a curve require more operations than a mere multiplication in $\mathbb{Z}/(n \cdot \mathbb{Z})$. This explains the reason for the efficiency struggle.
5. The reader should not confuse *quantum cryptography* with *quantum computing*, where quantum effects are used to help computations and not only secure information transmission: the physical challenges are even larger in the latter case.

## Bibliography


[BMSS] A. Bostan, F. Morain, B. Salvy and É Schost: *Fast algorithms for computing isogenies between elliptic curves*, Math. Comp. **77** (2008), 1755–1778.

[CEP] E. R. Canfield, P. Erdős, C. Pomerance, *On a problem of Oppenheim concerning Factorisatio Numerorum*, J. Number Theory 17 (1983) 1–28.

[CS] R. Cramer and V. Shoup, *Signature Schemes based on strong RSA assumptions*, Extended abstract in Proc. ACM CCS 1999.

[CP] R. Crandall and C. Pomerance, *Prime Numbers – A Computational Perspective*, Springer, 2004.

[DH] Whitfield Diffie and Martin Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory; Nov. 1976.

[EL] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational Perspectives on Number Theory: Proc. Conf. in honour of A. O. L. Atkin (D. A. Buell and J. T. Teitelbaum, eds.), AMS/International Press, 1998, 21–76.

[HeSSL] F. Heß, A. Stein, S. Stein and M. Lochter, *The Magic of Elliptic Curves and Public Key Cryptography*, Jahresbericht Deutsch Math.-Ver. **1**14 (2012), 59–88.

[HPS] J. Hoffstein, J. Pipher and J.H. Silverman: *An Introduction to Mathematical Cryptography*, Springer (2008)

[Kb1] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp., **48**(1987), 203–209.

[Kb2] N. Koblitz, *Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[Len] H. W. Lenstra, *Factoring integers with elliptic curves*, Annals Math., **126**(3)(1987), 649–673.

[Ma] U. Maurer: *Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms*. Advances in Cryptology – Crypto '94, Springer-Verlag, (1994), 271–281.

[MV] P. Mihăilescu and V. Vuletescu, *Elliptic Gauss sums and applications to point counting.* J. Symb. Comput. 45, **8**(2010), 825–836.

[ML] V. Miller, *Uses of elliptic curves in cryptography*, Advances in Cryptology: Proc. of Crypto '85, Lecture Notes in Computer Science, **218**(1986), Springer-Verlag, New York, pp. 417–426.

[MSU] A. Myasnikov, V. Shpilrain and A. Ushakov, *Group-based Cryptography*, Advanced Courses in Math. CRM Barcelona, Birkhäuser Verlag (2008).

[Ra] M. Th. Rassias, *On the representation of the number of integral points of an elliptic curve modulo a prime number*, http://arxiv.org/abs/1210.1439.

[RSA] R. Rivest, A. Shamir and L. Adleman, *A method for obtaining signatures and public key cryptography*, Communications of the ACM, **21** (1978), 121–126.

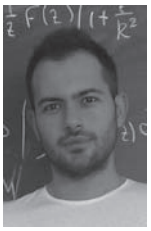
[Sc1] R. Schoof, *Elliptic Curves over Finite Fields and Computation of Square Roots mod p*, Math. Comp. **4**3(1985), 483–494.

[Sc2] R. Schoof, *Counting Point on Elliptic Curves over Finite Fields*, Journal de Th. des Nombres Bordeaux,

[Sil] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[Was] L. C. Washington, *Elliptic Curves-Number Theory and Cryptography*, CRC Press, London, New York, 2008.


*Preda Mihăilescu [preda@uni-math.gwdg.de] was born in Bucharest, 1955. He studied mathematics and computer science in Zürich receiving his PhD from ETH-Zürich. He was active during 15 years in the industry, as a numerical analyst and cryptography specialist. In 2002, Mihăilescu proved Catalan's conjecture. This number theoretical conjecture, formulated by the French mathematician E. C. Catalan in 1844, had stood unresolved for over a century. The result is known as Mihăilescu's Theorem. He is currently a professor at the Institute of Mathematics of the University of Göttingen.*



*Michael Th. Rassias [michail.rassias@math.ethz.ch] was born in Athens, 1987. He received his school education in Athens, during which he participated at various mathematical contests; he has received two gold medals at the Pan-Hellenic Mathematical Olympiads of 2002 and 2003, a silver medal at the Balkan Mathematical Olympiad of 2002 and a silver medal at the 44th International Mathematical Olympiad of 2003. He holds a Diploma from the School of Electrical and Computer Engineering of the National Technical University of Athens and a Master of Advanced Study in Mathematics from the University of Cambridge. He is currently a PhD student in Mathematics at ETH-Zürich, under the supervision of Professor E. Kowalski.*

# The Hirsch Conjecture Has Been Disproved: An Interview With Francisco Santos

Eva Miranda (Universitat Politècnica de Catalunya, Barcelona, Spain)

The famous Hirsch conjecture was formulated in 1957 in a conversation of Warren Hirsch with George Dantzig, the father of the simplex method. It asserts that given a polytope of dimension $d$ and $n$ facets, its combinatorial diameter is smaller than or equal to $n–d$, i.e. any two vertices of the polytope can be connected to each other by a path of at most $n–d$ edges.

The conjecture is related to the problem of complexity of the simplex method (it gives a lower bound). The conjecture has been open for 53 years and has attracted the interest of many mathematicians in discrete, combinatorial and computational geometry. The simplicity of its statement has also attracted mathematicians in other areas.

On 10 May 2010, the entry about the Hirsch Conjecture in Wikipedia was updated, announcing that Francisco Santos had found a counterexample to the Hirsch conjecture. Later, on 14 June, Francisco Santos posted a preprint where the first counterexample was given. It was a polytope in dimension 43 and with 86 facets. The paper is now published in *Annals of Mathematics* [Sa4]. The Hirsch Conjecture has been disproved.

When I knew that Francisco Santos would be visiting Barcelona to give an RSME colloquium, I could not avoid it. I had to interview him. We met in a jewel of modernism, Casa Fuster.[1] This is a transcript of the interview.

**Francisco Santos in Casa Fuster**

[1] Pictures taken in Hotel Casa Fuster during this interview have been reproduced with permission.

***First of all, let me congratulate you for disproving the Hirsch Conjecture. The result has now appeared in Annals of Mathematics.***
Thank you.

***In your career you have focused particularly in discrete geometry, combinatorics and algebraic geometry (starting with your PhD thesis). When did you start to get interested in the Hirsch Conjecture?***
I have known of it since I was a PhD student. It is one of the important conjectures in the area. Indeed you can find it in the book of Ziegler [Zi] which was a bedside book for me at that time. There are two notable moments: when I started to work on it hard and when I tried to disprove it. This was when I was on sabbatical at the University of California in 2007–2008 where I met Eddie Kim. Eddie Kim was doing his PhD thesis on a special case of the Hirsch Conjecture and we wrote a survey together about the timeline of the Hirsch conjecture. In 2009, I started to give talks about the Hirsch Conjecture without having disproved it.

But there was another key moment which was previous to this one: in January 2002 I met Victor Klee when I was visiting Seattle and gave a talk about a counterexample[2] related to polytopes. Victor Klee at that moment was retired. He was around 76 years old. He came to talk to me and said: "Since you seem to be good at counterexamples, why don't you try to disprove the Hirsch Conjecture?"

***So you were not thinking about this conjecture in 2002 before meeting Victor Klee?***
No. For me the Hirsch Conjecture was like the Riemann Hypothesis for number theorists. You don't work on it directly because it even scares you a little bit to face it directly.

***And Victor Klee was convinced that the conjecture was false?***
Victor Klee at that moment thought it was false. In fact, if you read his papers in the '70s and '80s you realise that he had spent more effort trying to disprove it rather than to prove it.

***And your initial guess about the conjecture was to prove it or disprove it?***

[2] Which can be found in [Sa1].

I did not have any initial guess. Victor Klee with Walkup had done some partial counterexamples. The initial conjecture was for polyhedra (not necessarily bounded) and Victor Klee with Walkup [KW] had found an unbounded counter-example. When I really understood this counterexample, I thought perhaps it could be exported somehow to construct a counterexample for bounded polytopes as well. It looked so simple that it made me think there was more room for work on the "counterexample side".

***Viktor Klee has been a great influence in your work, hasn't he?***

Viktor Klee was a great inspiration for me. I dedicate my paper to his memory not only because he was the one who tried harder to solve the Hirsch Conjecture but also that he motivated others to do it. His work on the conjecture extends further than his own papers; it also extends to his students and descendants who had his work as a heritage for more than 30 years: from Barnette who did his PhD with him in 1967 until Holt who graduated in 1996; or Mihalisin, who graduated in 2002 and worked with Klee in abstract models of the graph of a polytope (in 2002 Klee was already 76!); or even Sturmfels, who graduated with Klee in 1987 and likes to explain (half jokingly) that the first problem that Klee proposed to him was the Hirsch Conjecture but after a month of trying it, he realised it was too difficult and decided to go on with an easier problem.

Klee is an example of perseverance and generosity that one should admire. Also my method is inspired in his paper with Walkup in 1967 [KW]. Klee died in the Summer of 2007. This was an additional motivation for me to work harder on this problem with Kim when I was at UC Davis.

## Optimization: The origins

***The conjecture started with a conversation of Dantzig with Hirsch in 1957. Do you know the exact context of the conjecture?***

It is related to the simplex method. For the simplex method we need to know in how many steps the algorithm is going to finish. Even if it is not exactly the same this is related to the diameter of the polytope. I imagine that Hirsch proposed the upper bound n-d after making some experiments. It is a natural conjecture; even if it is false, it is a natural conjecture.

The simplex method (nobody knows if it is polynomial) works very well and works linearly in practice.

***What is the difference between the complexity of the polytope and the simplex method?***

The simplex method looks for its path along the graph of the polytope to reach the optimum. The Hirsch conjecture is about the diameter of the graph. If the diameter is 50 and you are not lucky and you are far from the solution you may go through all the vertices. So this would be like a lower bound for the algorithm. Once you are in one vertex, the simplex method has certain freedom to choose the forthcoming vertex (local rules). This choice is given by a pivot's rule.

***What is the Klee-Minty cube and what is it used for?***

The example of Minty and Klee is a cube (combinatorially) with 2d facets and diameter d. It is designed to trick the simplex algorithm with Dantzig's pivot rule and make it go through all the vertices.

One can choose different pivot rules for the simplex method and people have found analogue exponential (or, at least, superpolynomial) constructions to all the methods. In the Summer of 2010 Olivier Friedman found similar examples to the ones of Klee and Minty for three pivot rules: one of them is Zadeh's rule.

Zadeh's rule (which was in Norman Zadeh's PhD thesis in the '60s) tries to avoid facets which you have recently visited through the simplex algorithm. The cube example of Minty and Klee failed with Zadeh's rule. So Zadeh[3] had offered 1000 dollars to whoever found a polytope in which his rule failed to be polynomial. This price was given to Oliver Friedman by Zadeh precisely in a conference in 2011 at IPAM where I presented my counterexample.

**Francisco Santos during the interview**

***Polytopes show up in toric geometry. Do you think that this counterexample can have some applications to algebraic geometry?***

The refutation seems to have no applications to toric geometry. I do not know notions in toric geometry that are related to the diameter of the graph. In any case, other counterexamples in discrete geometry have applications to toric geometry like the one discussed in [Sa2].

## The counterexamples: methods

***The Hirsch conjecture has a history of more than 50 years. During all this period, big progress has been made computationally and theoretically to check that***

[3] Zadeh is no longer working as a mathematician. For the complete story about this, visit Gil Kalai's blog: http://gilkalai.wordpress.com/2011/01/20/gunter-ziegler-1000-from-beverly-hills-for-a-math-problem-ipam-remote-blogging/.

***certain polytopes were Hirsch. What is the role of computational geometry in this process? Do you think that the Hirsch conjecture could have been solved if you did not have the current computational tools at your disposal?***
The resolution is not computational. This counterexample could in principle have been found by Klee 40 years ago without the use of computers. The first counterexample is a 43-dimensional polytope P with 86 facets whose diameter is greater than 43 but it is not constructed directly; it is "derived" from a much smaller polytope (in "only" five dimensions) with certain properties. Computers have been useful for me to check the polytope and to experiment and explore in some particular example. In order for computers to be really effective you need to go to really high dimensions. In dimension 3 the Hirsch conjecture was known to be true and this was done by hand. In dimension 4 it was known to be true for less than 12 facets.

***Was this done with the help of computers?***
In dimension 4 for less than 9 facets it was done by hand (also by Klee and Walkup) and for 10, 11, 12 it was done using computers.

***Then they are useful in the sense that they are a help for inspiration?***
They have been useful to experiment. And they played a role in making me feel more certain when I announced the counterexample.

The counterexample has two parts: a theoretical reduction and an explicit construction. I felt reassured when I could check the explicit construction (certain polytopes satisfying a certain condition). Before announcing it, I had sent it to Julian Pfeiffe and to Eddie Kim to help me with the computational checks (computing distance between facets). So I felt quite relieved by having these computational verifications.

When I asked them to do these computations, I did not tell them why I needed them but I think they figured it out.

***In this direction, the work of Klee and Walkup[4] to prove that the d-step conjecture and the Hirsch conjecture are equivalent seems to be a key point in your work. What is the role the theoretical approach played through these 50 years in your work?***
Both parts of my construction can be traced to the 1967 paper of Klee and Walkup; the theoretical reduction is a generalisation of their d-step Theorem and the explicit construction is somehow inspired on their counterexample to the conjecture for unbounded polytopes (polyhedra). In the conference in honour of Klee in 2010, where I made the announcement of the counterexample, the title of my talk was "A counterexample to the Hirsch conjecture: Two theorems of Klee and Walkup".

[4] Klee and Walkup proved in [KW] that the study of the general Hirsch conjecture is equivalent to the study of the case $n = 2d$. This is called the $d$-step Theorem.

***So there is a combination of heritage and inspiration: the creativity of the construction and all this previous work?***
I had the initial idea of using spindles to disprove the conjecture on a plane trip to Paris. Once I had the theorem and the spindle idea to construct the counterexample it only took me a couple of days thinking about the construction of Klee and Walkup.

***How many vertices does this first example have?***
I do not know. To get the true counterexample from the intermediate explicit polytope involves an iteration of 38 times so it is difficult to control how many vertices the final polytope has. This iteration is based on the generalisation of the d-step Theorem. This part of the construction is a sort of blow up so the number of vertices can increase without control in each step.

***So $2^{40}$ is an upper bound. How is this bound found?***
I did this computation based on computations up to order 9 and on an upper bound for the explosions in each step.

***People working in computational geometry are probably interested in this kind of construction…***
To construct this polytope was interesting as a computational challenge. People working in algorithms are interested in actual computations. Also, computing explicitly the number of vertices is useful to get a direct verification of the counterexample of the conjecture without going through the details of proof.

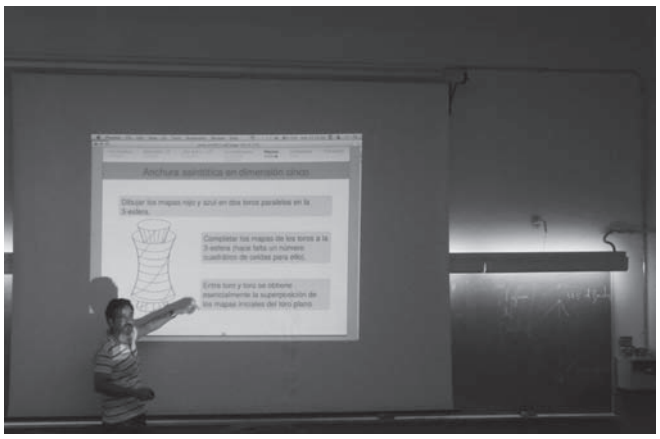
***What about the second counterexample?***
This counterexample was constructed together with Mastchke and Weibel. We proved that there is a 20-dimensional polytope with 40 facets whose diameter is greater than 20.

In this counterexample it was possible to compute the number of vertices of the final polytope, which is exactly 36442. This is because the initial construction had fewer vertices and we had to do the explosion only 20 times.

***And where did the idea of this second counterexample in lower dimensions come from?***
The starting point is the same: using the $d$-step Theorem with a prismatoid of lower dimension having the right properties.

The second part of this counterexample is based in finding a prismatoid in dimension 5 and width bigger than 5. Concretely we prove that there are 5-prismatoids of width six with only 25 vertices, versus the 48 vertices in the first construction that I made. This leads to lowering the dimension of the non-Hirsch polytopes from 43 to only 20.

A prismatoid is a polytope having all vertices in two parallel facets and the width is the distance between the two facets; with this procedure you find a counterexample to the dual to the Hirsch conjecture which can be stated as "The dual diameter of a d-dimensional polytope with n vertices is at most $n–d$".



**Francisco Santos explaining the second counterexample at Universitat de Barcelona.**

***In all this you use a lot the idea of duality?***
For me it is simpler to work in the dual model because it is more combinatorial. For the Hirsch conjecture, it is well known that we can assume that the polytope is simple (each facet is in general position and therefore only d facets intersect at each vertex). For instance the cube and the dodecahedron are simple polytopes. The dual of a simple polytope is simplicial (in each facet there are only $d$ vertices) like the octahedron and the icosahedron.

Simplicial polytopes from a combinatorial point of view are simpler. They are just simplicial complexes. This is why I always dualize the Hirsch conjecture.

So in this second counterexample, for the 5-prismatoids, with Weibel we found an example with distance 6 and with Maschke we found the distance is as big as wanted. The distance increases with the square root of the number of vertices (it is indeed a family of counterexamples). This is relevant to understand prismatoids and to understand the method of construction of counterexamples.

***How did you have this idea with Weibel?***
I started to look closer at the construction to try to simplify it and Weibel did the same, in parallel, with slightly different ideas. At some point he emailed me his findings and by combining them with mine we could improve both. My methods were more combinatorial but I was not using computers and he had a computational approach.

***And this was done in one month?***
In six months. This second counterexample was easier than the first because I had all the methods and only had to polish the first one.

***Is there a general interest in improving these counterexamples?***
It is not so easy and maybe it is not so relevant – maybe for a PhD student because of what you learn on the way.

***What is your overall perception of the roles of inspiration and work in disproving the Hirsch conjecture?***
There is this famous saying "When inspiration arrives it is better that it catches you working". In my case, my working method is to spin around the matter. It is maybe not a very efficient method because you often come back to old reasonings but it is fun. As I said, the idea of the spindle was an inspiration that I had on a plane from Paris to Bilbao. This idea came to me when I was reading a paper about Minkowski sums (one of the authors is Weibel) which provide a tool to analyse prismatoids, and everything fitted together. I like to think about old computations from new perspectives.

## New lines of research

***And now the big question is "what comes next"?***
I am travelling a lot and I also have a lot of new responsibilities. I am Vice-Dean and Coordinator of the Degree of Mathematics in my university, which takes a lot of time from me.

But of course I am still interested in the Hirsch conjecture. There is an idea that came up in a Polymath project.[5] Tim Gowers launched two or three years ago the Polymath project (the first one was on number theory and combinatorial proof). The idea was to try to make research in massive collaboration. Then he launched the first Polymath project on a Wikipage. Tim Gowers' main rule was not to spend too long in thinking about one problem; the idea was to create a net of collaborators. Indeed, Polymath 1 ended up with three publications which you can find in the arxiv.[6] Gil Kalai then launched Polymath 3 trying to prove the polynomial Hirsch conjecture.[7] Unfortunately, this Polymath project is nowadays not as active as the initial Polymath project was. But we now have a refined proposal for the polynomial Hirsch conjecture.

***Can you state now this new polynomial conjecture?***
I think that the right polynomial bound to consider as a new conjecture is $(n–d)d$. This would replace the initial Hirsch conjecture of $n–d$.

***Is this conjecture motivated by particular computations?***
It is based on an abstraction of certain properties on polytopes and in trying to prove this conjecture in a more general context. This conjecture would hold also for simplicial manifolds.

***How do you state this abstract polynomial Hirsch conjecture?***
You state it defining a class of objects, the so-called connected layer families which are pure simplicial complexes of dimension d with an extra property (local and recursive) and the conjecture is that for these families

5 You can find a list of Polymath projects at http://michaelnielsen.org/polymath1/index.php?title=Main_Page.
6 http://arxiv.org/find/math/1/au:+Polymath_D/0/1/0/all/0/1.
7 The Polymath 3 project about the polynomial Hirsch conjecture can be found at http://gilkalai.wordpress.com/2010/09/29/polymath-3-polynomial-hirsch-conjecture/.

the diameter cannot be greater than $nd–d$. The interesting thing is that there are examples of diameter exactly $nd–d$. We have examples of two families of connected layer families which are very different and which share these properties so I am quite certain that this conjecture holds.

So now I believe in the conjecture with upper bound of $nd–d$ or even $nd–d^2$. The change from $d$ to $d^2$ is what you gain when coming back from the abstract setting to the geometric one.

***What implications does the work of the polynomial Hirsch conjecture have in optimization? And what is the relation to question 9 in the list of Smale?***[8]
The relation is not direct. In mathematics the distance between theories and application is sometimes long. Let's assume that we prove this $nd–d$ upper bound holds; the question is does it have application in the simplex method? The truth is: not really. Applications are not very clear because for all known pivot rules one can always find examples which are not polynomial. If we could prove this polynomial upper bound then this would somehow corroborate that the simplex method is effective but does not seem to add special clues about its complexity unless the resolution is quite algorithmic. It is known that certain polytopes are Hirsch but there is no algorithm that finds the short path of length $(n–d)$. So indeed it seems more a theoretical question.

In relation with question 9 of the list of Smale: if we applied the simplex method with polynomial pivoting rule this would be a strongly polynomial algorithm.

The problem is also the model you take to measure complexity.

In complexity theory the model which is best known is the binary one: input and output are numbers in base 2 and you consider as a basic step a digit operation in base 2. The algorithms of interior point and the ellipsoid for linear programming are polynomial in this model. But there is another model (arithmetical model of computation). In this model you admit rational numbers as big as you want and you consider as an elementary step each arithmetic computation with them. The interior point and ellipsoid methods paradoxically are not polynomial in this model (because they are methods of successive approximation).

The standard algorithms (pivots) which are used in the simplex method are not polynomial (as shown by the counterexamples of Klee-Minty, Friedman…). The open question is: is there any pivot rule that makes the simplex method polynomial? Such an algorithm would be "strongly polynomial": polynomial in both models.

***Have you ever talked to Steve Smale about the Hirsch conjecture?***
No.

***What new lines do you expect that this could open?***
Some people want to find examples in lower dimension. Another option would be to study prismatoids of higher dimension but it does not seem very useful.

## Social impact

***In Spain you have really been on the media. What is the social impact this news can have?***
It has impact in the sense that it can give a good image of mathematics and research in mathematics. Unfortunately in the media this is not always the case; they want to transmit the idea that mathematicians are a bit strange. When I have talked to journalists I have always tried to transmit the idea that mathematicians are normal people and that mathematics is complicated but interesting and when you plunge into it then it can be fascinating.

The overall impression that I have of my interaction with the media is positive; I saw that the general audience is interested in mathematics. I think it is important to give an image of mathematics to reach the general public. Sometimes we censor ourselves because we do not give importance to the image of mathematics and also because we are a bit freaked out by the fact that in our field it is of extreme importance to use precise statements, and talking to journalists and the general public you may need to say things in a less precise way to get understood, which is what physicists do.

But we need to reach the media and the general public with positive messages about mathematics. For instance, I always say kids like mathematics until somebody convinces them of the opposite. Society sometimes sends the message that mathematics is complicated but kids like logics, geometry and solving things.

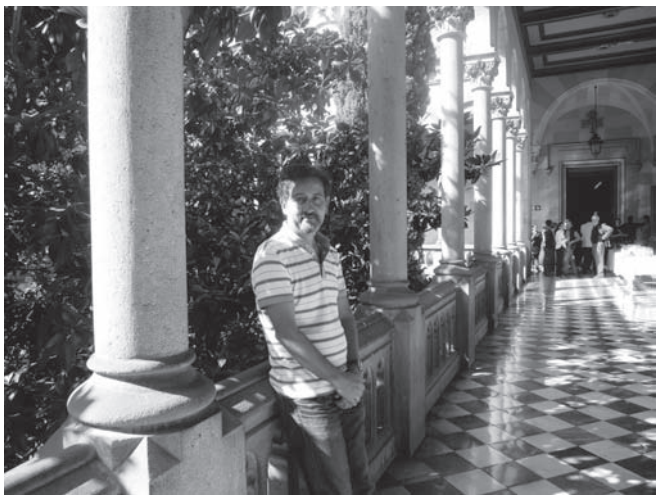
***How do you value individual work in your area versus joint work?***
I am used to working alone but I also have collaborations. Working with Polymath has been an interesting experience but it is also possible to work alone in this subject.

***Your collaborators are mainly European?***
In Europe, I have collaborators in France, Germany and Spain. But I also have a lot of connection to the US, specifically with Sturmfels and de Loera, both in California.

***The resolution of longstanding conjectures in this critical period seems to stimulate young students in maths. What advice would you give to young people?***
I would encourage good and interested students to pursue research but perhaps not necessarily in academia. We should forget the old mentality that is quite extended in Spain that PhD holders should stay in university. I feel that Germany and other countries are much better in this respect than Spain. The PhD should have a social value. But, of course, if we want to convince society of the value of PhDs we may need to make the PhDs more adapted to social needs.

***Thank you so much for this interview and congratulations again for your research.***
Thanks to you.

[8] The question 9 in Smale's list is the following: Is there an algorithm which is strongly polynomial to solve linear programming?



**Francisco Santos at Universitat de Barcelona**

## References


[Da] G. Dantzig, George B., *Linear Programming and Extensions*, Princeton Univ. Press. Reprinted in the series Princeton Landmarks in Mathematics, Princeton University Press, 1998.

[K] V. Klee, D.W Walkup, The $d$-step conjecture for polyhedra of dimension $d < 6$, *Acta Mathematica* 133: 53–78 (1967).

[KS] E.D. Kim and F. Santos, An update on the Hirsch conjecture, Jahresbericht der Deutschen Mathematiker-Vereinigung, Volume 112(2) (June 2010), 73–98.

[MSW] B. Matschke, F. Santos, C. Weibel, The width of 5-dimensional prismatoids, Preprint, February 2012, 28 pages. arXiv: 1202.4701.

[Sa1] F. Santos, A point set whose space of triangulations is disconnected, *J. Amer. Math. Soc.* 13 (2000), 611–637.

[Sa2] F. Santos, Non-connected toric Hilbert schemes, Mathematische Annalen, 2005, Volume 332, Number 3, Pages 645-665.

[Sa3] F. Santos, Sobre un contraejemplo a la Conjetura de Hirsch, La Gaceta de la RSME, Vol. 13 (2010), Num. 3, 525-538.

[Sa4] F. Santos, A counter-example to the Hirsch conjecture. Annals of Math. (2), 176 (July 2012), 383-412.

[Zi] G. Ziegler, "The Hirsch Conjecture", *Lectures on Polytopes*, Graduate Texts in Mathematics, 152, Springer-Verlag, pp. 83–93. 1994.


*Eva Miranda [eva.miranda@upc.edu] obtained her PhD in mathematics in 2003 at the University of Barcelona. After holding a postdoctoral Marie Curie EIF grant at the Université de Toulouse and a Junior Research Position Juan de la Cierva at Universitat Autònoma de Barcelona, she is currently a lecturer (tenure-track) at Universitat Politècnica de Catalunya. Her research interests focus on several problems in differential geometry and mathematical physics, namely symplectic, Poisson geometry and Hamiltonian dynamics. She has been an editor of the Newsletter of the European Mathematical Society since 2010."She is also a corresponding member of the Catalan Mathematical Society at the European Mathematical Society.*

# Mathematics and Geometric Ornamentation in the Medieval Islamic World

Jan P. Hogendijk (Utrecht University, The Netherlands)

*We discuss medieval Arabic and Persian sources on the design and construction of geometric ornaments in Islamic civilization.*

## 1 Introduction

Many medieval Islamic mosques and palaces are adorned with highly intricate geometric ornaments. These decorations have inspired modern artists and art historians, and they have been discussed in connection with modern mathematical concepts such as crystallographic groups and aperiodic tilings. The Islamic ornamental patterns can certainly be used to illustrate such modern notions.

Medieval Islamic civilization has also left us an impressive written heritage in mathematics. Hundreds of Arabic and Persian mathematical manuscripts have been preserved in libraries in different parts of the world. These manuscripts include Arabic translations of the main works of ancient Greek geometry such as the *Elements* of Euclid (ca. 300 BC) and the *Conics* of Apollonius (ca. 200 BC), as well as texts by medieval authors between the 8th and 17th centuries, with different religious and national backgrounds. In what follows reference will be made to 'Islamic' authors and 'Islamic' texts but the word 'Islamic' will have a cultural meaning only. Most 'Islamic' mathematical texts were not related to the religion of Islam and, although the majority of 'Islamic' authors were Muslims, substantial contributions were made by Christians, Jews and authors with other religious backgrounds who lived in the Islamic world.

Many Islamic texts on geometry are related to spherical trigonometry and astronomy, and most Islamic scholars who studied the *Elements* of Euclid were studying in order to become astronomers and possibly astrologers. Yet there are also Islamic works on geometrical subjects unrelated to astronomy. In almost all medieval Islamic geometrical texts that have been published thus far, one does not find the slightest reference to decorative ornaments. This may be surprising because the authors of these texts lived in the main Islamic centres of civilization and may have seen geometric ornaments frequently.

In this paper we will see that the Islamic geometric ornaments were in general designed and constructed not by mathematician-astronomers but by craftsmen (Arabic: *ṣunnāᶜ*). Our main question will be as follows: what kind of mathematical methods, if any, did these craftsmen use, and to what extent did they interact with mathematician-astronomers who were trained in the methodology of Greek geometry? We will discuss these questions on the basis of the extant manuscript material, which is very fragmentary. In Sections 2–5 we will discuss four relevant sources and we will draw our conclusions in Section 6. For reasons of space, we will restrict ourselves to plane ornaments and pay no attention to decorative patterns on cupolas and to *muqarnas* (stalactite vaults).

## 2 Abu'l-Wafā'

We first turn to the "book on what the craftsman needs of the science of geometry"[1] by the 10th-century mathematician-astronomer Abu'l-Wafā' al-Būzjānī. This work contains some information on the working methods of the craftsmen, which will be useful for us in Section 4 below. Abu'l-Wafā' worked in Baghdad, one of the intellectual centres of the Islamic world. He dedicated his booklet to Bahā' al-Dawla, who ruled Iraq from 988 to 1012 and who apparently employed mathematicians as well as craftsmen at his court. Almost all of the booklet consists of ruler-and-compass constructions belonging to plane Euclidean geometry. They are explained in the usual way, that is, by means of geometric figures in which the points are labelled by letters but without proofs. Abu'l-Wafā' says that he does not provide arguments and proofs in order to make the subject more suitable and easier to understand for craftsmen [1, 23].

The booklet consists of 11 chapters on: (1) the ruler, the compass and the *gonia* (i.e. a set square); (2) fundamental Euclidean ruler-and-compass constructions and, in addition, a construction of two mean proportionals, a trisection of the angle and a pointwise construction of a (parabolic) burning mirror; (3) constructions of regular polygons, including some constructions by a single compass-opening; (4) inscribing figures in a circle; (5) circumscribing a circle around figures; (6) inscribing a circle in figures; (7) inscribing figures in one another; (8) division of triangles; (9) division of quadrilaterals; (10) combining squares into one square and dividing a square into squares, all by cut-and-paste constructions; and (11) the five regular and a few semi-regular polyhedra. Abu'l-Wafā' does not mention geometric ornaments.

Most of the information on the working methods of craftsmen is contained in Chapter 10. In that chapter, Abu'l-Wafā' reports about a meeting between geometers and craftsmen in which they discussed the problem of constructing a square equal to three times a given square (for an English translation see [16, 173–183]). The craftsmen seem to have had three equal squares in front of them and wanted to cut them and rearrange the pieces into one big square. The geometers easily constructed the side of the required big square by means of Euclid's *Elements* but were unable to suggest a cut-

and-paste construction of the big square from the three small squares. Abu'l-Wafā' presents several cut-and-paste methods that were used by the craftsmen but he regards these methods with some disdain because they are approximations. Abu'l-Wafā' was trained in Euclid's *Elements* and therefore he believed that geometry is about infinitely thin lines and points without magnitude, which exist in the imagination only. He complains that the craftsmen always want to find an easy construction which seems to be correct to the eye but that they do not care about a proof by what Abu'l-Wafā' calls "the imagination". He declares that constructions that can be rigorously proven should be distinguished from approximate constructions and that the craftsmen should be provided with correct constructions so they do not need to use approximations anymore.[2] We do not know how the booklet was received but the 16th-century Persian manuscript which we will study in Section 4 contains a rich variety of approximate constructions.

## 3 The Topkapı Scroll

The craftsmen themselves seem to have left us with very few documents about their activities in the field of geometric ornamentation. The most important published example is the so-called Topkapı Scroll, which is now preserved in the Topkapı Palace in Istanbul and which has appeared in a magnificent volume [14]. This 29.5 m long and 33 cm wide paper scroll is undated and may have been compiled in North-western Iran in the 16th century but the dating is uncertain. The scroll consists of diagrams without explanatory text. Many of these diagrams are related to calligraphy or muqarnas and therefore do not concern us here. Some of the diagrams concern plane tilings. I have selected one non-trivial example in order to draw attention to the characteristic (and frustrating) problems of interpretation. The drawing on the scroll [14, p. 300] consists of red, black and orange lines, which are indicated by bold, thin and broken lines respectively in Figure 1 (for a photo of the manuscript drawing see also [17]). The broken lines in Figure 1 define a set of five tiles, called *gireh*-tiles in modern research literature from the Persian word *gīreh*, which means knot. The thin lines form a decorative pattern which can be obtained by bisecting the sides of the gireh-tiles and drawing suitable straight line segments through the bisecting points. It is likely that the pattern was designed this way but one cannot be sure because the scroll does not contain any explanatory text. The gireh tiles of Figure 1 have drawn recent attention because they can be used to define aperiodic tilings. In the absence of textual evidence, it is impossible to say whether the craftsmen had an intuitive notion of aperiodicity (for a good discussion see [8]).

## 4 An anonymous Persian treatise

One would like to have a medieval Islamic treatise, written by a craftsman, in which the design and construction of ornaments is clearly explained. Such a treatise has not been found and, thus far, only a single manuscript has been discovered in which diagrams on geometrical ornaments are accompanied by textual explanations. In this section we will discuss what this manuscript can tell us about the main question at the beginning of the paper. The manuscript is a rather chaotic collection of 40 pages of Persian text and drawings (for some photos see [14, 146–150]). The text consists of small paragraphs which are written close to the drawing to which they refer and, although the texts and drawings appear in a disorganised order and may not be the work of a single author, the collection will be considered as one treatise.[3] It may have been compiled in the 16th century, although some of the material must be older as we shall see.

The treatise belongs to a manuscript volume of approximately 400 pages [5, 55–56]. Some of the other texts in the manuscript volume are standard mathematical works such as an Arabic translation of a small part of Euclid's *Elements*. But the treatise itself does not resemble a usual work by a mathematician or astronomer in the Islamic tradition. It is assumed here that the treatise is the work of one or more craftsmen because it agrees with most of what Abu'l-Wafā' says about their methodology. The treatise provides much additional information on the working methods of the craftsmen and it also shows that they were really involved with the design and construction of geometrical ornaments. In order to illustrate these points, the following four examples 4.1 through 4.4 have been selected from the treatise.

### *4.1.*

The treatise contains many approximation constructions, including a series of ruler-and-compass constructions of a regular pentagon by means of a single compass-opening. In these constructions, the compass-opening is assumed to be either the side of the required regular pentagon or the diagonal, the altitude or the radius of the circumscribing circle. Here is one such construction with a paraphrasing of the manuscript text [12, 184b]. Figure 2 is a transcription of the figure in the manuscript, in which the labels (the Arabic letters *alif*, *bā'*, ...) are rendered as *A*, *B*, ..., and Hindu-Arabic number symbols are represented by their modern equivalents. The Persian text says:

> On the construction of *gonia* 5 by means of the compass-opening of the radius, from *gonia* 6. On line *AG* describe semicircle *ADG* with centre *B*. Then make point *A* the centre and describe arc *BE*. Then make point *G* the centre and on the circumference of the arc find point *D* and draw line *AD* to meet arc *EB* at point *Z*. Draw line *GZ* to meet the circumference of the arc at point *H*. Join lines *AH*, *GH*.[4] Each of the triangles *AZH*, *GZD* is *gonia 5*, and the original triangle *ADG* was *gonia 6*, ...

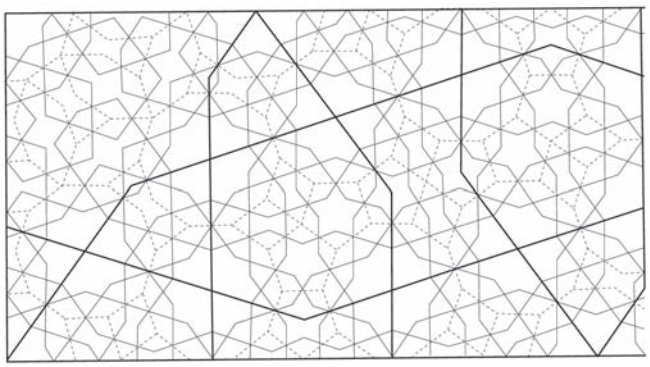


**Figure 1. Drawing by Dr Steven Wepster**

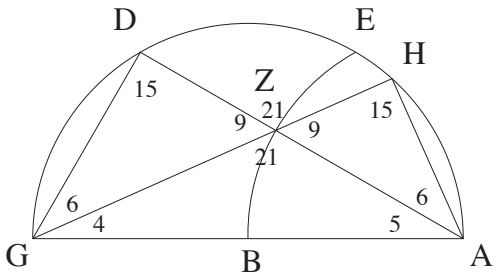



**Figure 2.**

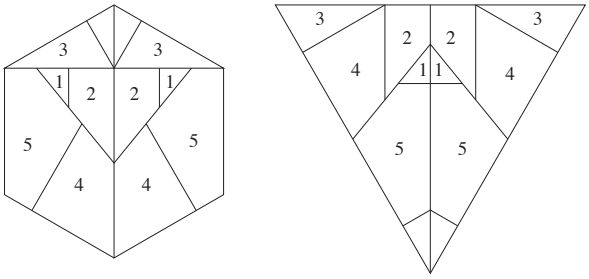



**Figure 3.**

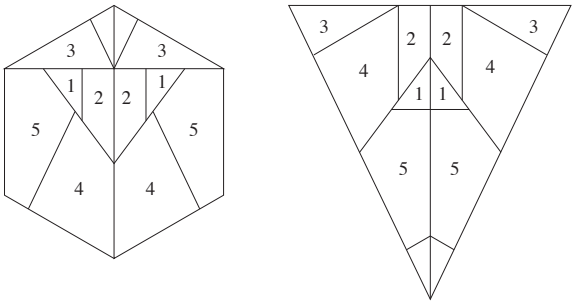



**Figure 4.**

Points $A, E, D$ and $G$ are four angular points of a regular hexagon and $DH$ is the side of the regular pentagon inscribed in the same circle. The construction is a good approximation[5] but it is not exact so Abu'l-Wafā' would not have approved it. In Chapters 3 and 4 of his booklet, Abu'l-Wafā' provided exact constructions of the regular pentagon using a fixed compass-opening. The *gonia* is mentioned by Abu'l-Wafā' as an instrument used by craftsmen. From the Persian treatise we infer that *gonia n* is a set square with angles $90^o$, $\frac{180^o}{n}$ and $90 - \frac{180^o}{n}$. In Figure 2, angles are expressed in units such that 15 units are a right angle. In the Islamic tradition, the division of the right angle into 90 degrees, subdivided sexagesimally, was only used in mathematical astronomy and mathematical geography.

*4.2.*

Abu'l-Wafā' says that the craftsmen are interested in cut-and-paste constructions, and the Persian treatise contains many such constructions. Some of these are explained by one or more paragraphs of text but the following example is presented without accompanying text.

Figure 3 displays a regular hexagon and an isosceles triangle, dissected into pieces such that both figures can be composed from these pieces. Figure 3 is derived from the manuscript [12, 197a] with the difference here that the isosceles triangle has been arbitrarily assumed to be equilateral and the figure has been drawn in a mathematically correct way. In the manuscript, the pieces are indicated by numbers (as in Figure 3) so the correspondence is clear. Since there is no text in the manuscript, the reader does not have a hint of how exactly the pieces have to be cut. Readers are invited to work out the details for themselves. After this exercise, they will probably be convinced that the manuscript was intended to be used under the guidance of a competent teacher who could provide further information. It should be noted that the pieces no. 1 and 2 in the manuscript are drawn in such a way that no. 1 is wider than no. 2. This may happen if the vertex angle of the isosceles triangle is less than $54^o$; Figure 4 has been drawn for a vertex angle of $\frac{360^o}{7}$. It is tempting to assume that the craftsmen had a general dissection of an isosceles (rather than an equilateral) triangle in mind but because there is no accompanying text, one cannot be sure. The construction is mathematically correct but there are also approximate cut-and-paste constructions in the Persian treatise.

It is not necessary to assume that the fancy cut-and-paste construction of Figures 3 and 4 was used in practice. Just like European arithmetic teachers in later centuries, Islamic craftsmen may have challenged one another with problems which surpassed the requirements of their routine work.

*4.3.*

The many drawings of geometric ornaments in the Persian treatise show that its authors were deeply involved with the design and construction of ornamental patterns. This example is also found on a real building, namely the North Cupola of the Friday Mosque in Isfahan, which was built in the late 11th century. The Persian text laconically introduces the ornamental pattern as follows ([12, 192a], [14, 148]) with reference to Figure 5.[6]

> Make angle $BAG$ three sevenths of a right angle. Bisect $AG$ at point $D$. Cut off $BE$ equal to $AD$. Produce line $EZ$ parallel to $AG$. Draw line $TI$[7] parallel to $BE$, bisect $TE$ at point $H$ and make $TI$ equal to $TH$. Extend $EI$ until it intersects $AB$ at point $K$. Produce $KL$ parallel to $BE$. With centre $Z$ draw circular arc $KMN$ in such a way that its part $KM$ is equal to $MN$. On line $AF$ take point $S$ and that is the centre of a heptagon. Complete the construction, if God Most High wants.

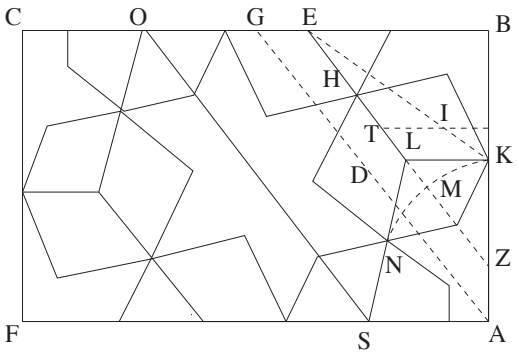



**Figure 5.**

Or construct angle $ELN$ equal to angle $ELK$ and by means of line $LN$ find the centre $S$.

Or cut off $EO$ equal to $EL$, so that $O$ is the centre of a heptagon. And make line $OS$ parallel to $GA$ and equal to $AG$.[8] Then point $S$ is the centre of another heptagon. Or else let $GO$ be equal to $AS$. God knows best.

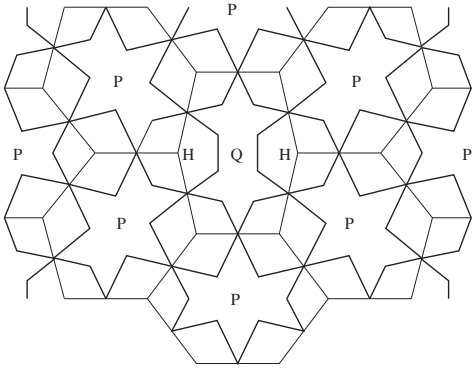



**Figure 6.**

The text does not inform the reader what should be done with the completed figure. Apparently the rectangular figure in the manuscript and its mirror image should be repeated as suggested by Figure 6. Thus one obtains the pattern in the north cupola of the Friday Mosque.[9]

The pattern can be linked to *gireh* tiles such as in Figure 1 above. These *gireh* tiles are not mentioned explicitly in the Persian treatise; all information in the treatise about Figure 5 is contained in the passages quoted above. Let $\alpha = \frac{1}{7} \times 180^o$ and take as gireh tiles two types of equilateral hexagons with equal sides (thin lines in figure 6), of type $P$ with angles $4\alpha, 5\alpha, 5\alpha, 4\alpha, 5\alpha, 5\alpha$ and of type $Q$ with angles $4\alpha, 4\alpha, 6\alpha, 4\alpha, 4\alpha, 6\alpha$. Now draw suitable lines through the midpoints of the sides, in such a way that the "stars" inscribed in $P$ and $Q$ emerge, with angles $2\alpha$ at the midpoints of the sides of the gireh tiles. The heptagons $H$ in Figure 6 are regular. Patterns with regular heptagons are rarely found on Islamic buildings so the pattern in the manuscript and on the North Cupola probably go back to the same designer or designers. The pattern on the North Cupola of the Friday Mosque consists of the thick lines in Figure 6 with some additional embellishments but without the *gireh* tiles in Figure 6.

### 4.4.

The fourth and final example from the Persian treatise will reveal some information about the relationship between craftsmen and Islamic mathematician-astronomers who had been trained in Greek mathematics. As an introduction, consider a pattern from the Hakim Mosque in Isfahan (Figure 7). The pattern is inspired by a division of a big square into a small square and four kites.[10] Two of the angles of each of the kites are right angles.

Figure 8 is a partial transcription of a figure in the Persian treatise [12, 189b] but the labels and broken lines are additions.[11] The figure displays a big square with side $ZP$, subdivided into a small square with side $RQ$ and four big kites such as $EQTZ$ and $RTPU$, each with two right angles and with pairwise equal sides ($QE = EZ$, $QT = TZ$, $RT = TP$, $RU = UP$). Note that the four longer diagonals of the

**Figure 7.**

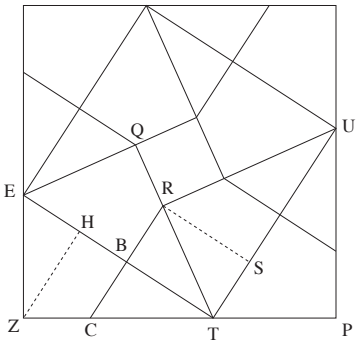



**Figure 8.**

big kites also form a square with side $ET$, which will be called the intermediate square. In the special case of Figure 8, the side $QR$ of the small square is supposed to be equal to the distance $RB$ between each angular point of the small square and the closest side of the intermediate square. Then each big kite such as $EQTZ$ can be divided into two right-angled triangles $BRT$, $BCT$ and two small kites such as $EQRB$, $EBCZ$ with two right angles and pairwise equal sides ($EQ = EB$, $RQ = RB$, $EB = EZ$, $CB = CZ$). Thus we have four big kites and eight small kites and, for easy reference, the resulting division of the big square will be called the twelve kite pattern.

Almost a quarter of the Persian treatise is somehow devoted to the twelve kite pattern. If we draw perpendiculars $ZH$ and $RS$ to $ET$ and $TU$ respectively, $ZH = RS = BT$. The two sides $EZ$ and $EB$ of the small kite $EBCZ$ are also equal, so in the right-angled triangle $EZT$ we have $ZH + EZ = ET$. The twelve kite pattern can be constructed if a right-angled triangle (such as $EZT$) can be found with the property that the altitude ($ZH$) plus the smallest side ($ZE$) is equal to the hypotenuse ($ET$). The text states that "Ibn-e Heitham" wrote a treatise on this triangle and constructed it by means of two conic sections, namely "a parabola and a hyperbola". No further details are given and no conic section is drawn anywhere in the Persian treatise. But the text contains a series of approximation constructions of the twelve kite pattern, such as the following [12, 189b] (Figure 9). The text reads:

Line $AD$ is the diagonal of a square. The magnitudes of $AB, BG$ are equal and $AD$ is equal to $AB$. Find point $E$ on the rectilinear extension of line $GD$. Then each of $EZ, ZH$ is equal to $AG$. Join

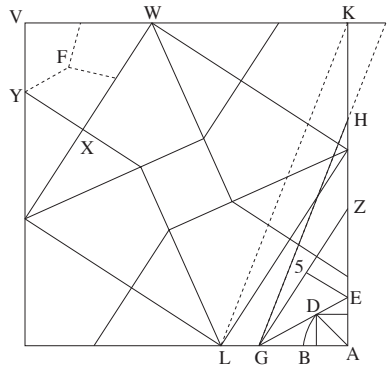



**Figure 9.**

line $GH$ and through point $K$ draw line $KL$ parallel to $GH$. Find point $L$; the desired point has now been obtained.

The approximation is sufficiently close for all practical purposes: if the side of the square is 1 metre, the difference between the correct and approximate positions of $L$ is only a few millimetres.[12] It does not follow that the approximation presupposes a deep mathematical knowledge. In the figure in the manuscript, the eight small kites are all subdivided into three even smaller kites with pairwise equal sides and at most one right angle. In Figure 9 the subdivision is indicated by broken lines in only one kite $VWXY$ (labels by the author) in the upper left corner. One may guess that $FV = \frac{1}{2}VW$ and note that $F$ is located on the bisector of angle $WVY$. The first step of the approximation boils down to the construction of a triangle $ADG$ similar to $VFW$.

For further details on the Persian treatise we refer to the planned edition with translation and commentary which is scheduled to appear in 2013.

## 5 Mathematicians on the twelve kite pattern

The reference to "Ibn e-Heitham" in the Persian treatise shows that the twelve kite pattern was also studied by mathematician-astronomers. We will now discuss what is known about these studies because they will give us some further hints about the interactions between mathematician-astronomers and craftsmen. "Ibn e-Heitham" is a Persian form of Ibn al-Haytham (ca. 965–1041), a well-known Islamic mathematician-astronomer who was interested in conic sections. His treatise on the twelve kite pattern has not been found but one of the extant works of the famous mathematician-astronomer and poet ᶜUmar Khayyām (1048–1131) is also of interest here. The work is written in Arabic and entitled "treatise on the division of a quadrant". It begins in the following uninspiring way (Figure 10, [10, 73]): "We wish to divide the quadrant $AB$ of the circle $ABGD$ into two parts at a point such as $Z$ and to draw a perpendicular $ZH$ onto the diameter $BD$ in such a way that the ratio of $AE$ to $ZH$ is equal to the ratio of $EH$ to $HB$, where $E$ is the centre of the circle and $AE$ is the radius." Khayyām does not give the slightest indication of the origin or relevance of this problem. He draws the tangent to the circle at $Z$, which intersects $BE$ extended at $T$ and he shows that in the right angled triangle $EZT$, the sum of the altitude $ZH$ plus the shortest side $ZE$ is equal to the hypotenuse $ET$.[13] Thus the problem is inspired by the twelve kite pattern but Khayyām does not mention the relationship with this pattern or with geometric ornamentation in general. In a new figure (not rendered here), Khayyām puts, in the notation of Figure 10, $EH = 10$ and $ZH = x$, so $ZE = \sqrt{100 + x^2}$ and by similar triangles $HT = \frac{x^2}{10}$. He then shows that the property $ZH + EZ = ET$ boils down to the cubic equation $x^3 + 200x = 20x^2 + 2000$, or in a literal translation of his words: "a cube and two hundred things are equal to twenty squares plus two thousand in number" [10, 78]. He then proceeds to construct a line segment with length equal to the (positive) root $x$ of this equation by the intersection of a circle and a hyperbola. An anonymous appendix [10, 91] to Khayyām's text contains a direct construction of point $Z$ in Figure 10 as a point of intersection of the circle and the hyperbola through point $B$ whose asymptotes are the diameter $AEG$ and the tangent $GM$ (broken lines in Figure 10). None of this was relevant to a craftsman who wanted to draw the twelve kite pattern and Khayyām declares that numerical solutions of the cubic equation could not be found. In order to find a numerical approximation of arc $ZB$, Khayyām rephrases the problem about the quadrant in trigonometrical form as follows: to find an arc such that "the ratio of the radius of the circle to the sine of the arc is equal to the radius of the cosine to the versed sine". In modern terms, if $\alpha = \angle ZET$ and the radius is 1, the ratio $AE : ZH = EH : BH$ is equivalent to $1 : \sin\alpha = \cos\alpha : (1 - \cos\alpha)$. Khayyām says that this problem can be solved by trial and error using trigonometrical tables and that he found in this way $\alpha \approx 57^\circ$, and if $AE = 60$ then $ZH \approx 50$, $EH \approx 32\frac{2}{3}$ and $BH \approx 27\frac{1}{3}$. He also says that one can solve the problem more accurately. Using the trigonometrical tables that were available in his time, he could have computed the required arc in degrees and minutes by linear interpolation.[14] This information on sexagesimal degrees and minutes may not have been of much use to craftsmen as we have already seen in 4.2 above. We may also compare with a reference by the Iranian mathematician and astronomer Al-Bīrūnī (976-1043) in a work on the qibla (direction of prayer towards Mecca). Al-Bīrūnī computes the qibla at Ghazni (Afghanistan) by trigonometrical methods as 70 degrees and 47 minutes west of the south point on the local horizon. He then adds a ruler-and-compass approximation construction for "builders and craftsmen", who "are not guided by degrees and minutes" ([4, 286], compare [3, 255–256]).

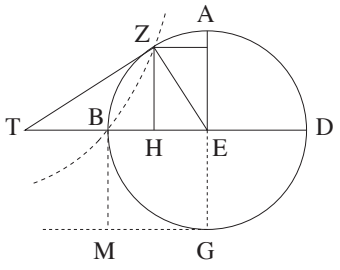



**Figure 10.**

## 6 Conclusion

We now return to the main question in the introduction to this paper. Because the evidence is so scarce, it is not clear to what extent we are able to generalise the information which we can obtain from the available manuscript sources. But if this can be done, the following may be suggested about the main differences between Islamic craftsmen who designed and constructed ornaments and Islamic mathematician-astronomers who were trained in Greek geometry:

– Mathematician-astronomers worked with geometric proofs in the style of Euclid's *Elements*. Craftsmen were familiar with the Euclidean way to draw figures, using letters as labels of points (but also the number 5 in Figure 9 above). Craftsmen did not use geometric proofs and they had not been trained in the methods of Euclid's *Elements*.
– Texts written by mathematician-astronomers usually contain sufficient explanation to understand the mathematics. An oral explanation is not absolutely necessary. Texts and diagrams by craftsmen are often ambiguous and oral explanations were essential.
– Mathematician-astronomers distinguished between exact and approximate geometrical constructions. Craftsmen did not distinguish between these constructions if the result was acceptable from a practical point of view.
– Craftsmen used some geometrical instruments not found in the theoretical works of Greek geometry, such as a set-square and a compass with fixed opening.

The following relationship between craftsmen and mathematicians may be suggested. Mathematicians such as Ibn al-Haytham and ᶜUmar Khayyām may have regarded the designs of craftsmen as a hunting ground for interesting mathematical problems. Thus the twelve kite pattern inspired constructions by means of conic sections, as in Figure 10 above. These constructions were a favourite research topic in the 10th and 11th century among Islamic mathematicians who had studied the *Conics* of Apollonius (ca. 200 BC). However, Khayyām did not reveal that his geometric construction problem was inspired by a decorative ornament.[15] Other Islamic geometric problems may also have a hitherto unidentified historical context related to ornaments.

The craftsmen knew that the mathematicians had worked on some problems related to ornamentation and they regarded the solutions with respect, even though they probably did not understand the details and technicalities. The Persian treatise states [12, 185a] that the construction of a right-angled triangle such as *EZT* in Figure 8 "falls outside the *Elements* of Euclid" and requires the "science of conic sections". No drawing of a conic section occurs anywhere in the Persian treatise.

Of course we cannot exclude the possibility that a few mathematicians were also involved in the design and construction of geometric ornaments. The heptagonal pattern in Figure 6 is explained in our treatise in the language of the craftsmen but since ᶜUmar Khayyām lived in Isfahan at the time that the North Cupola was built, it is possible that he was somehow involved in the design. That a combination of mathematical learning and manual skill was possible in Islamic civilization is shown by the case of Abū Ḥāmid al-Khujandī (ca. 980), who was trained in Greek geometry and astronomy, and who authored a number of geometrical and astronomical works as well as being a superb metalworker.[16]

The source materials that we have discussed in this paper give a fascinating glimpse into a design tradition about which little is known. Our knowledge is based to a large extent on one single Persian manuscript which is now preserved in Paris. It is likely that a systematic search in manuscript libraries in the Islamic world will produce many more relevant documents and lead to a significant increase in our insight into the working methods of the medieval Islamic craftsmen.

*Acknowledgement.*
I thank Viktor Blåsjö for his comments on a preliminary version of this paper.

First published in the Proceedings of the 6th European Congress of Mathematics. Reprinted with permission.

## Notes

1. Incomplete French and German versions are to be found in [21] and [20]. The complete version in Arabic is in [1] and in facsimile in [18].
2. Note that Abu'l-Wafā' presents an approximate construction of the regular heptagon by ruler and compass. Just like many of his Islamic contemporaries, he probably believed that the regular heptagon cannot be constructed by ruler and compass.
3. The treatise was translated into Russian [6, 315–340] and modern Persian [2, 73–93], and a full publication of it with English translation was planned by Alpay Özdural (see [15]), who unfortunately passed away in 2003 before he completed the project. The Persian text is scheduled to be published, with translation and commentary, by an interdisciplinary research team in 2013.
4. Instead of $GH$ the manuscript says incorrectly $DH$.
5. This is easily shown by modern elementary geometry. Suppose that the radius of the circle is 1 and drop a perpendicular $ZP$ onto $AG$. Then $ZA = 1, \angle ZAP = 30^o, ZP = \frac{1}{2}, AP = \frac{\sqrt{3}}{2}, GP = 2 - \frac{\sqrt{3}}{2}, \angle ZGP = \arctan\frac{ZP}{GP} \approx 23.8^o$. Because $\angle DGP = 60^o$, $\angle ZAH = \angle ZGD \approx 36.2^o$.
6. Broken lines in Figure 5 also appear as broken lines in the manuscript.
7. The text does not make clear that $T$ is an arbitrary point on segment $EZ$.
8. The manuscript has $AD$ by scribal error.
9. For a photograph see [9].
10. See [7]. The pattern is inscribed with calligraphy: Allāh in the central square and Muḥammad and ᶜAlī in the four kites.
11. The points in Figure 8 have been labelled to highlight the correspondence with Figure 10 below.
12. If the side of the "square" in the beginning is set equal to 1, we have $AD = \sqrt{2}, AG = 2\sqrt{2}, \frac{AE}{AG} = \frac{1}{2\sqrt{2}-1}$ so $AE = \frac{1}{7}\cdot(8 + 2\sqrt{2}), AZ = \frac{1}{7}\cdot(8+16\sqrt{2}), \angle ZGA \approx 57.12\ldots \approx 57^o7'$ (compare with footnote 14 below). Note that $\angle ZGA$ in Figure 9 corresponds to $\alpha = \angle ZET$ in Figures 8 and 10.
13. Proof: In Figure 10 by similar triangles $EH : EZ = EZ : ET$ and because $EZ = EB$ we have $EH : EB = EB : ET$ and therefore $EH : (EB - EH) = EB : (ET - EB)$, that is to say $EH : HB = EB : BT$. By assumption $EH : HB = AE : ZH$ so because $AE = BE$ also $EH : HB = EB : ZH$. We conclude $ZH = BT$, so $EZ + ZH = EB + BT = ET$.
14. If we use modern methods and put $x = \tan\alpha$, we have $HZ = 10x$ if $HE = 10$. So $10x$ is a root of Khayyām's cubic equation and therefore $x^3 + 2x = 2x^2 + 2$. The equation is irreducible over the rational numbers, so the twelve kite pattern cannot be

constructed by ruler and compass. The equation has one real root $x = 1.54369\ldots$ so $\alpha \approx 57.06^{o} \approx 57^{o}4'$.

15. When Khayyām's text on the division of the quadrant was published in 1960 [13] and in 1981 [10], the modern editors had no way of knowing that the problem was inspired by ornaments. Around 1995 Özdural discovered the connection as a result of his study of the anonymous Persian treatise [15].
16. He made one of the most beautiful astrolabes of the entire Islamic tradition, which is now in the Museum of Islamic Art in Doha, Qatar, see [11, 503–517] and also the illustration on the front page of [11].

## Bibliography


[1] (Abu'l-Wafā') Ṣ. A. ᶜAlī, ed., *Mā yuḥtāj ilayhi al-ṣāniᶜ min ᶜilm al-handasa, li-Abu'l-Wafā' al-Būzjānī*. Baghdad: University of Baghdad, 1979 [in Arabic].

[2] (Abu'l-Wafā') *Applied geometry, Abolvefa Mohammad ibn Mohammad Albuzjani, rewritten into modern Persian with appendices by Seyyed Alireza Jazbi.* Tehran: Soroush Press, 1991 [in Persian].

[3] (al-Bīrūnī) Jamil Ali, transl. *The Determination of the Coordinates of Positions for the Correction of Distances between Cities, a translation from the Arabic of al-Bīrūnī's Kitāb Taḥdīd nihāyāt al-amākin li-taṣḥīḥ masāfāt al-masākin*. Beirut: American University of Beirut, 1967.

[4] (al-Bīrūnī) P. Bulgakov, ed., *Kitāb Taḥdīd nihāyāt al-amākin li-taṣḥīḥ masāfāt al-masākin li Abī'l-Rayḥān … al-Bīrūnī,* Cairo 1962, reprint edition ed. F. Sezgin. Frankfurt, Institut für Geschichte der arabisch-islamischen Wissenschaften, 1992, series Islamic Geography vol. 25.

[5] Sonja Brentjes, Textzeugen und Hypothesen zum arabischen Euklid in der Uberlieferung von al-Ḥağğāğ b. Yūsuf b. Maṭar (zwischen 786 und 833), *Archive for History of Exact Sciences* **7** (1994), 53–92.

[6] M.S. Bulatov, *Geometricheskaya Garmonizatsiya v arkhitekture Srednei Azii IX–XV vv.* Moskou: Nauka 1988 [in Russian].

[7] Peter R. Cromwell, Elisabeth Beltrami, The Whirling Kites of Isfahan: Geometric Variations on a Theme. *Mathematical Intelligencer* **33** (2011), 84–93.

[8] Peter R. Cromwell, The Search for Quasi-Periodicity in Islamic 5-fold Ornament. *Mathematical Intelligencer* **31** (2009), 36–56.

[9] J.P. Hogendijk, Ancient and modern secrets of Isfahan. *Nieuw Archief voor Wiskunde* fifth series, **9** (2008), 121.

[10] (Khayyām) *L'Oeuvre Algébrique d'al-Khayyām*, ed. R. Rashed, A. Djebbar. Aleppo, Institute for History of Arabic Science, 1981.

[11] David A. King, *In Synchrony with the Heavens: Studies in Astronomical Timekeeping and Instrumentation in Medieval Islamic Civilization*, Volume 2: Instruments of Mass Calculation, Leiden: Brill, 2005.

[12] Manuscript Paris, Bibliothèque Nationale, Persan 169, fol. 180a–199a.

[13] Gh. Ḥ Mossaheb, Hakim Omare Khayyam as an Algebraist, Tehran: Bahman Printing 1960. Anjomane Asare Melli Publications No. 38.

[14] Gülru Necipoğlu, *The Topkapı Scroll: Geometry and Ornament in Islamic Architecture*. Santa Monica, Ca., Getty Center for the History of Art and the Humanities, 1995.

[15] Alpay Özdural, On Interlocking Similar or Corresponding Figures and Ornamental Patterns of Cubic Equations. *Muqarnas* **13** (1996), 191–211.

[16] Alpay Özdural, Mathematics and Arts: Connections between Theory and Practice in the Medieval Islamic World. *Historia Mathematica* **27** (2000), 171–201.

[17] Sebastian R. Prange, The tiles of infinity. *Saudi Aramco World* 60, September/October 2009, 24–31. http://www.saudiaramcoworld.com/issue/200905/the.tiles.of.infinity.htm

[18] A.Q. Qorbani, *Būzjānī-Nāmeh*. Tehran 1371 A.H. (solar)

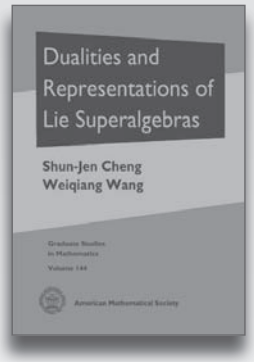
[19] F. Sezgin, ed., *Abu'l-Wafâ al-Būzjānī. Texts and Studies, Collected and Reprinted*. Vol. 2. Frankfurt, Institut für Geschichte der arabisch-islamischen Wissenschaften, 1998. Series: *Islamic Mathematics and Astronomy*, vol. 61.

[20] H. Suter, Das Buch der geometrischen Konstruktionen des Abu'l-Wefā', Beiträge zur Geschichte der Mathematik bei den Griechen und Arabern, Hsg, J. Frank, *Abhandlungen zur Geschichte der Naturwissenschaften und der Medizin* **IV**. Erlangen 1922. Reprinted in Heinrich Suter, *Beiträge zur Geschichte der Mathematik und Astronomie im Islam,* ed. F. Sezgin. Frankfurt, Institut für Geschichte der arabisch-islamischen Wissenschaften, 1986, vol. 2, 635–630. Also reprinted in [19, 280–295]

[21] F. Woepcke, Recherches sur l'Histoire des Mathématiques chez les Orientaux. Deuxième Article: Analyse et Extrait d'un recueuil de constructions géométriques par Aboûl Wafâ. *Journal Asiatique* **5** (1855), 218–255, 309–359. Reprinted in: Franz Woepcke, *Études sur les mathématiques arabo-islamiques*, ed. F. Sezgin. Frankfurt, Institut für Geschichte der arabisch-islamischen Wissenschaften, 1986, vol. 1, 483–572. Also reprinted in [19, 84–174]. Digital version: http://books.google.com/books?id=Z4gvAAAAYAAJ


*Jan P. Hogendijk [j.p.hogendijk@uu.nl] received his PhD in 1983 at Utrecht University, the Netherlands. His dissertation was a critical edition of the Arabic text with English translation of the reconstruction by Ibn al-Haytham (ca. 1000) of the lost Book 8 of the Conics of Apollonius (ca. 200 BC). He worked at Brown University (Providence RI, USA) and the J.W. Goethe University (Frankfurt am Main) and is currently a professor of history of mathematics in the Mathematics Department of Utrecht University.*

# American Mathematical Society



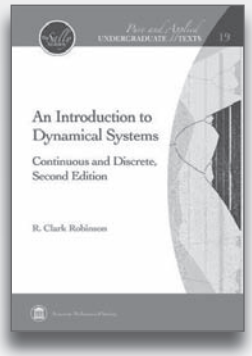

## DUALITIES AND REPRESENTATIONS OF LIE SUPERALGEBRAS

Shun-Jen Cheng, *Academia Sinica* & Weiqiang Wang, *University of Virginia*

Gives a systematic account of the structure and representation theory of finite-dimensional complex Lie superalgebras of classical type, and serves as a good introduction to representation theory of Lie superalgebras. Several folklore results are rigorously proved (and occasionally corrected in detail), sometimes with new proofs. Three important dualities are presented in the book, with the unifying theme of determining irreducible characters of Lie superalgebras. In order of increasing sophistication, they are Schur duality, Howe duality, and super duality.

**Graduate Studies in Mathematics, Vol. 144**

**Jan 2013 297pp 978-0-8218-9118-6 Hardback €60.00**




## AN INTRODUCTION TO DYNAMICAL SYSTEMS

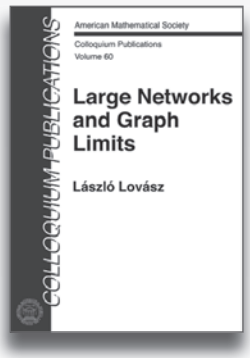
### Continuous and Discrete, Second Edition

R. Clark Robinson, *Northwestern University*

Provides a mathematical treatment of the introduction to qualitative differential equations and discrete dynamical systems. The treatment includes theoretical proofs, methods of calculation, and applications. The two parts of the book, continuous time of differential equations and discrete time of dynamical systems, can be covered independently in one semester each or combined together into a year long course.

**Pure and Applied Undergraduate Texts, Vol. 19**

**Jan 2013 760pp 978-0-8218-9135-3 Hardback €87.00**



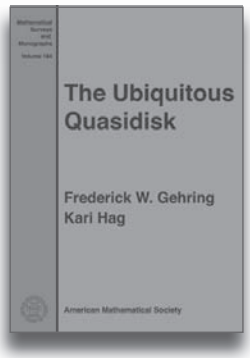

## LARGE NETWORKS AND GRAPH LIMITS

László Lovász, *Eötvös Loránd University*

Recently, it became apparent that a large number of the most interesting structures and phenomena of the world can be described by networks. To develop a mathematical theory of very large networks is an important challenge. This book describes one recent approach to this theory, the limit theory of graphs, which has emerged over the last decade.

**Colloquium Publications, Vol. 60**

**Dec 2012 475pp 978-0-8218-9085-1 Hardback €93.00**




## THE UBIQUITOUS QUASIDISK

Frederick W. Gehring & Kari Hag, *Norwegian University of Science and Technology*

Focuses on gathering the numerous properties and many different connections with various topics in geometric function theory that quasidisks possess. In 1981 Frederick W. Gehring gave a short course of six lectures on this topic in Montreal. In the late 1990s Gehring and Hag decided to write an expanded version of the Montreal notes. At three times the size of the original notes, this book is much more than just an extended version.

**Mathematical Surveys and Monographs, Vol. 184**

**Dec 2012 169pp 978-0-8218-9086-8 Hardback €70.00**

To order AMS titles visit **www.eurospanbookstore.com/ams**

**CUSTOMER SERVICES:**
Tel: +44 (0)1767 604972
Fax: +44 (0)1767 601640
Email: eurospan@turpin-distribution.com

**FURTHER INFORMATION:**
Tel: +44 (0)20 7240 0856
Fax: +44 (0)20 7379 0609
Email: info@eurospangroup.com

AMS
American Mathematical Society

distributed by **Eurospan** | group

# International Centre for Mathematical Meetings, Castro Urdiales, Spain

Juan Antonio Cuesta Albertos (Director of the International Centre for Mathematical Meetings)

## History

The International Centre for Mathematical Meetings (CIEM, from its Spanish name *Centro Internacional de Encuentros Matemáticos*) was created in January 2006 as a joint initiative of the Universidad de Cantabria and the City of Castro Urdiales, a nice, coastal town in the region of Cantabria, in the north of Spain. The university and the city had collaborated for several years, with the university organising courses, concerts and cultural activities in Castro Urdiales during the Summer, but then both sides decided that it was in their common interest to focus those activities thematically on mathematics and, at the same time, to expand them to other periods throughout the year.

2006 was a very important year for Spanish mathematics. Most notably, it was the year of the ICM-Madrid. The newly born CIEM took part in the ICM in two ways. On the one hand the Organising Committee of the ICM had one of its several meetings at CIEM on February 3rd. On the other hand, one of the first (and one of the biggest ever) events at CIEM was the second *International Conference on Mathematical Software*, a satellite conference of the ICM that gathered more than 100 mathematicians in Castro Urdiales.

But a second milestone from that year for mathematics in Spain, and one much more relevant to the history of CIEM, was the starting of the "*Consolider Mathematica*" (or iMATH) project. iMATH was an ambitious 5-year research project funded with a total of 7,500,000 euros by the Spanish Research Ministry. Its main goal was to improve the mathematical research in Spain as a whole and, in particular, to promote the communication between the different research groups and to boost transfer of knowledge from the mathematical laboratories and departments to the productive and social system. iMATH included 300 research groups and about 1700 mathematicians, what amounts to the vast majority of all the active researchers in mathematics in Spain.

**Scientific meeting**

At an early stage in the design of iMATH it was decided that an important part of its main organisational structure was a number of "nodes", whose role was to propose and organise a substantial part of the activities to be developed inside the project. Five nodes were chosen: one was the newly created CIEM and the others were the CESGA (the Supercomputation Centre in Galicia), the CRM (the Centre of Mathematical Research in Barcelona), the ICMAT (the Institute of Mathematical Sciences in Madrid) and the IMUB (the Mathematical Institute of the University of Barcelona). The node at CIEM would be mainly devoted to the organisation of meetings, short courses, workshops, etc.

**Seminar in the computer room**

## Facilities and organisation

Apart from some monetary contribution, the main contribution of the city of Castro Urdiales to CIEM was the building hosting it, called La Residencia. It is a nice, three-floored building dating from the early 20th century, very conveniently located on the beach and close to the town centre. After a refurbishment performed in 1997, La Residencia was devoted by the city to the celebration of all kinds of cultural activities. It has a conference room for about 90 people, a computer room, three smaller classrooms for about 25 people and a large exhibition room in the basement, where poster sessions and coffee breaks take place.

The centre does not have accommodation or meal facilities but it keeps agreements with hotels and restaurants located nearby, which allows reasonable prices to be offered to meeting attendants. CIEM, if asked for, also provides help with practical issues of meeting organisa-

**CIEM main building**

tion: registration, travel of invited speakers, social activities, etc.

CIEM is managed by its Director, a Steering Committee and a Scientific Committee. The director is a mathematician appointed by the university (currently J. A. Cuesta-Albertos), who also chairs both committees. The Scientific Committee currently consists of M. de León (CSIC-ICMAT, Madrid), E. Casas and T. Recio, both from the University of Cantabria, and the two former CIEM directors, L. González-Vega and F. Santos. The Steering Committee consists of the director plus one representative from the university and one from the city (typically the Vice-Chancellor for Research and the Councillor for Culture).

## How CIEM works

Every Spring, CIEM opens a call for activities for the next year. At the end of the application period (usually around the end of June) the Scientific Committee analyses the received proposals and elaborates a proposal that is submitted to the Steering Committee for its final approval. The proposal includes the calendar and the amount of money CIEM makes available to the organisers, who are responsible for providing or seeking extra financing if they need it.

**Coffee time**

The ideal number of participants in events hosted at La Residencia ranges between 25 and 50, and this is the size of most meetings. However, every year, we have some with more than 75, and sometimes up to 100, participants. CIEM accepts meetings lasting from two days to one week (exceptionally, two-week schools are also accepted). Due to the fact that Castro Urdiales is a Summer resort, CIEM does not accept proposals for the month of August, which is the peak of the Summer season. Organisers wanting to use July or early September should be aware that hotel prices will be higher.

In its seven years of history, CIEM has hosted 92 meetings (10 to 15 every year) with around 4,500 participants in total, from all around the world.

Partially due to its former role as the coordinator of the mathematics education part of iMATH, CIEM is also the site for the GeoGebra Institute of Cantabria. GeoGebra is a free and open software for dynamic geometry extensively used in secondary mathematics education. The objectives of the GeoGebra Institute of Cantabria are similar to those of other GeoGebra institutes: development, research, teaching and dissemination of the programme and its use.

## The location

Cantabria is a small region in the north of Spain, 150 km west of the French border. Contrary to most of Spain, this region is green and hilly. Its coastal line is full of nice beaches with yellow sand and very steep cliffs. Climate in the area is very temperate, with mean temperatures ranging from 9.5º C in January to 19.9º C in August.

**Castro Urdiales' harbour and Santa María Church**

Castro Urdiales is the third largest city in Cantabria (the largest one being Santander, the central site of the university). It is located by the seaside and has a population of 32,258 inhabitants, as of the 2010 census. Castro (as locals usually call it) already existed in Roman times, under the name of Portus Amanus. The urban area includes nice, not-too-crowded beaches and some interesting monuments like the Gothic Church of Santa María de la Asunción, whose construction started in the 13th century and finished in the 15th century. It also hosts a fishing port and a very friendly atmosphere. One of the nice features of CIEM is the size of the city: small enough to be walkable, allowing attendees to keep some meeting spirit even when they are not at CIEM, but big enough to offer a good choice of fine restaurants and other facilities.

### The present and the future

The history of CIEM has been closely tied to the iMATH project until that project finished in April 2012. In fact, more than two thirds of the events at CIEM in that period were connected to (and had partial financial support from) iMATH. That fact, together with the current financial crisis in Spain, of course puts challenges to the future of CIEM. Only time will tell how things develop but the fact is that we have eight activities programmed for 2013 (and a couple more could still be added, even if at the time of writing the official application period for 2013 has finished).

More information about the centre can be found at http://www.ciem.unican.es/.

## New Prize "EMS Monograph Award" by the EMS Publishing House

On the occasion of our tenth anniversary, we are happy to announce a new prize, open to all mathematicians. The **EMS Monograph Award** is assigned every two years to the author(s) of a monograph in any area of mathematics that is judged by the selection committee to be an outstanding contribution to its field. The prize is endowed with 10,000 Euro and the winning monograph will be published by the EMS Publishing House in the series "EMS Tracts in Mathematics".

#### Submission

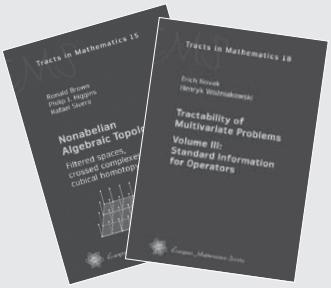
The monograph must be original and unpublished, written in English and should not be submitted elsewhere until an editorial decision is rendered on the submission. The first award will be announced in 2014 (probably in the June Newsletter of the EMS); the deadline for submissions is 30 June 2013. Monographs should preferably be typeset in TeX. Authors should send a pdf file of the manuscript by email and a hard copy together with a letter to:

European Mathematical Society Publishing House
ETH-Zentrum SEW A27, Scheuchzerstrasse 70, CH-8092 Zürich, Switzerland
E-mail: info@ems-ph.org

#### Scientific Committee

John Coates, Pierre Degond, Carlos Kenig, Jaroslav Nesetril, Michael Roeckner, Vladimir Turaev

### EMS Tracts in Mathematics




Editorial Board:
Carlos E. Kenig (University of Chicago, USA)
Andrew Ranicki (University of Edinburgh, UK)
Michael Röckner (Universität Bielefeld, Germany, and Purdue University, USA)
Vladimir Turaev (Indiana University, Bloomington, USA)
Alexander Varchenko (University of North Carolina at Chapel Hill, USA)

This series includes advanced texts and monographs covering all fields in pure and applied mathematics. Tracts will give a reliable introduction and reference to special fields of current research. The books in the series will in most cases be authored monographs, although edited volumes may be published if appropriate. They are addressed to graduate students seeking access to research topics as well as to the experts in the field working at the frontier of research.

**Most recent titles:**

Vol. 18 Erich Novak and Henryk Woźniakowski: *Tractability of Multivariate Problems. Volume III: Standard Information for Operators*
978-3-03719-116-3. 2012. 604 pages. 98.00 Euro

Vol. 17 Anders Björn and Jana Björn: *Nonlinear Potential Theory on Metric Spaces*
978-3-03719-099-9. 2011. 415 pages. 64.00 Euro

Vol. 16 Marek Jarnicki and Peter Pflug: *Separately Analytic Functions*
ISBN 978-3-03719-098-2. 2011. 306 pages. 58.00 Euro

# ICMI Column

Angel Ruiz (University of Costa Rica, San José, Costa Rica)

## CANP Costa Rica 2012: a great success

The *Mathematics Education Network of Central America and the Caribbean* has been born. *Escuela seminario internacional Construcción de Capacidades en Matemáticas y Educación Matemática*: CANP Costa Rica 2012, 6–17 August 2012, in San Jose, Costa Rica, was a great success.

The International Commission on Mathematical Instruction (ICMI) organised this event. It is the second venture of the *Capacity and Networking Project*, whose first project was in Mali (Africa) in 2011; the third will be held in Cambodia (Asia) in 2013. A general presentation of CANP was published by Bill Barton, ICMI President, in Issue 82 of the EMS Newsletter. It is one of the main projects of the ICMI. The event had the sponsorship of the International Mathematical Union (IMU), the International Council for Science (ICSU) and the Inter-American Committee on Mathematics Education (CIAEM), UNESCO, Mexico's Mathematics Research Center CIMAT, the Ministry of Public Education of Costa Rica and the University of Costa Rica.

The event brought together 67 researchers and educators of Colombia, Panama, Venezuela, Dominican Republic, Spain, Mexico, Cuba and Costa Rica. They took part in 23 different activities (conferences, courses, forums and symposia) on important themes of mathematics and mathematics education: Fundamental Mathematics in Primary and Secondary School, Contemporary Mathematics, Technologies, Competencies, Research, Preservice and In-service Teacher Preparation, Use of History of Mathematics and Epistemology of Mathematics. Under this international framework a public symposium was held: the *Costa Rican 25th Symposium on Math, Science and Society*, attended by 200 participants.

The most important result of CANP Costa Rica 2012 was the founding of the *Mathematics Education Network of Central America and the Caribbean*, which seeks to enhance capacities in mathematics and mathematics education in the region (see the website: http://redumatematicacyc.net).

*Angel Ruiz, Vice-president of the International Commission on Mathematical Instruction and President of the Inter-American Committee of Mathematics Education*

## Friends of Mathematics Education (FOME): A European Initiative

Mathematics has a unique place in the school curriculum. The stakes tend to be high for schools and students and there is no other school subject that has more or less the same curriculum across different countries, with the only differences being largely in pace or progression rather than substantive content. In addition, internationally accepted tests of comparative performance in mathematics, such as TIMSS and PISA, are widely used to shape policy and practice nationally. Since 1908, mathematics educators have been cooperating under the auspices of the International Commission of Mathematics Instruction (ICMI) and meet every four years at an international congress (ICME) to share overarching issues and challenges. Mathematics teaching at school has not only a proud history but is also crucial for a skilled workforce. There is considerable demand for a mathematically qualified workforce in a world driven by new technologies and automation. There are diverse initiatives to promote mathematics and to support the teachers of mathematics who are producing an appropriately skilled future workforce.

There have been many projects to support mathematics by major foundations across Europe, whether to support professional learning as above, to offer student enrichment or to scaffold early mathematical learning. However, the scope, extent and impact of these projects across Europe is neither known nor widely acknowledged in Europe.

The European Mathematical Society (EMS) – the union of the mathematical societies in Europe – set up a Committee of Education in 2009. The committee provided a first forum for interchange between mathematics educators and mathematicians. It recognised that there is no counterpart for what we have termed the 'Friends of Mathematics Education' (FOME). Professors Hoyles and Toerner, who have taken forward this FOME proposal and signed this paper, are members of the committee. They have made contact with various foundations and companies in different European countries and have received positive feedback: a first meeting of FOME is planned in Berlin, 14–15 March 2013. Further information about this initiative can be found at http://www.uni-due.de/mathematik/agtoerner/fome.shtml.

*Published at the request of*
*Guenter Toerner, Chair of the Committee for Education of the European Mathematical Society*

# ERME Column

João Pedro da Ponte (University of Lisbon, Portugal)

## Report of the Sixth YERME Summer School (YESS-6), Faro (Portugal), 23–28 August 2012

The Sixth YERME Summer School (YESS 6) took place, 23–28 August 2012, in Faro, Portugal, aiming to let young researchers from different countries meet and establish a friendly and cooperative style of work in the field of mathematics education research. YESS lets participants compare and integrate their preparation in mathematics

education research in a climate of peer discussion, with the help of highly qualified experts with varying fields of expertise. This event was an opportunity for young researchers to present their ideas, theoretical difficulties, methodological problems and preliminary research results, in order to get suggestions from other participants and experts about possible developments and different perspectives, opening the way to possible connections with other research projects and cooperation with researchers in other countries.

The participants included PhD students and post-doctoral researchers in mathematics education and others entering mathematics education research from European countries and neighbouring countries. There were 123 applicants, showing the interest raised by this ERME activity, and 73 were finally selected from Germany (18), Portugal (15), France, Italy and Norway (5), Turkey and UK (3), Cyprus, Greece, Israel and Sweden (2) and Algeria, Brazil, Canada, Czech Republic, Denmark, Ghana, Iceland, Libanon, Lybia, Spain and USA (1). The participants presented papers according to the situation of their studies and research work. This could include comprehensive information concerning personal graduate studies and/or research plans; presentations of research work in progress (goals, theoretical framework and methodology); or presentations of preliminary results (with essential information about their goals, theoretical framework and methodology).

The topics of the summer school were: Teacher knowledge and practice; Teacher education and professional development; Teaching and learning advanced mathematics; Cognitive and affective factors in learning and teaching mathematics; Theoretical perspectives, modelling and linguistic and representational aspects of teaching and learning mathematics. The scientific staff was composed of six leading experts in mathematics education: Ferdinando Arzarello, Markku Hannula, Barbara Jaworski, Maria Alessandra Mariotti, João Pedro da Ponte and Heinz Steinbring, and contributed to the Summer School by giving lectures and coordinating the working groups. Moreover, discussion groups were led by Paolo Boero and Rita Borromeo Ferri and there was a discussion devoted to issues that are relevant to the YERME organisation. The evaluation of the summer school was made by Paolo Boero. A complementary social program included a Fado night, a Brazilian night, a cultural session on mathematical competitions, an excursion to the old city of Tavira and a final outdoor night with opera and Portuguese music.

The drive for summer schools came from the spontaneous aggregation of young researchers of different countries at the CERME-II (2001) and CERME-III (2003) conferences. The aim was to create a cooperative style of working and a support to the development of professional preparation and careers in the field of mathematics education. Former YERME summer schools took place in Klagenfurt (Austria, 2002), Podebrady (Czech Republic, 2004), Jyväskylä (Finland, 2006), Trabzon (Turkey, 2008) and Palermo (Italy, 2010). This summer school took place at the University of Algarve in Faro (http://www.ualg.pt/), Campus da Penha, located in the South of Portugal. The organising committee included Ferdinando Arzarello and João Pedro da Ponte (ERME board representatives), Cláudia Canha Nunes and António Guerreiro (local group team representatives) and Paolo Boero (scientific coordinator). The local organisation was based at the Instituto de Educação da Universidade de Lisboa (João Pedro da Ponte, Cláudia Nunes and Marisa Quaresma) and the Escola Superior de Educação e Comunicação da Universidade do Algarve (António Guerreiro, Luciano Veia, Cristolinda Costa and Sandra Nobre).

# Models and Modelling in Mathematics Education

Mogens Niss (Committee for Education of the European Mathematical Society)

## Introduction and background

A major reason why mathematics is the world's single largest educational subject is the fact that mathematics is applied in a multitude of different ways in a huge variety of extra-mathematical subjects, fields and practice areas. Every time mathematics is used to deal with issues, problems, situations and contexts in domains outside of mathematics, mathematical models and modelling are necessarily involved, be it implicitly or explicitly. We begin by giving a brief outline of the basic concepts and terms of mathematical models and modelling before moving on to their educational aspects.

Consider some extra-mathematical domain and imagine that, for one reason or another, we want to come to grips with certain elements, features, phenomena, relationships, properties, issues, problems or questions pertaining to that domain, and that we intend to employ mathematics to do so. We then have to select, from the domain, those objects, relationships, phenomena, questions, etc. which we deem significant for our purpose. Each of the entities thus selected have to be represented by mathematical entities within some realm of mathematics which we reckon to be of relevance in the context. In other words, we map (translate) selected en-

tities, including questions, from the extra-mathematical domain under consideration into mathematical entities belonging and referring to the mathematical realm which has been chosen. The very point of involving mathematics is to seek mathematical answers (by mathematical means) to the translated questions in the mathematical realm and then translate the answers back into the extra-mathematical domain and interpret and evaluate them as answers to the extra-mathematical questions posed at the outset. This process, taking a point of departure in some extra-mathematical domain, moving into some mathematical realm so as to obtain mathematical conclusions and translating these back to the extra-mathematical domain, is known in the literature as the *modelling cycle* (see, for example, Niss, Blum and Galbraith, 2007, p. 4). It is important to keep in mind that building a mathematical model unavoidably involves deliberately and consciously ignoring lots of information, features, facts and circumstances that are judged to have minor importance in relation to the purpose and the context at issue. In other words, modelling oftentimes implies substantial simplification, stylisation, reduction of complexity, etc.

Against this background, a *mathematical model* can be defined in terms of an extra-mathematical domain, $D$, a mathematical realm, $M$, and a mapping (translation), $f$, from $D$ to $M$. Metaphorically, we can then think of a mathematical model as the triple $(D,f,M)$, which indicates that each of $D$, $f$ and $M$ is an indispensable component of the model. Sometimes $f$ is also called a "mathematisation" of $D$ by means of $M$. The use of the set-theoretical metaphor $(D,f,M)$ should not be over-interpreted, since $D$ and $M$ are not only meant to be "sets" consisting of objects (elements) but are also collections of relationships, phenomena, questions (and possible answers) and suchlike, and since $f$ not only operates on objects but also on the relationships, phenomena and questions selected to be the focus of our attention.

Let us illustrate these considerations with a simple example. If we want to decide which of two taxi companies, T and U, with different tariff schemes to choose for a taxi ride from A to B, the extra-mathematical domain ($D$) consists of taxi rides taking place in a topographical and commercial environment. Depending on the specific setting, significant entities include routes, distances, zones, neighbourhoods, time (of the ride, including waiting time, of the day, of the season, etc.), rates and money, whereas comfort and safety may not be deemed significant if the two taxi companies do not differ in those respects. Assume that we want to choose between T and U solely based on the cost of the rides and that the cost turns out to be determined by the zone location of A and B, the distance between them, and distance and zone dependent rate schemes used by T and U, respectively. Then a suitable mathematical realm ($M$) to represent the context and situation could consist of real functions, more specifically non-negative, piecewise linear functions defined on the non-negative reals, where the independent variable represents distance travelled and the dependent variable represents cost. The mapping $f$ then specifies the exact form of two functions, one for each company, and translates the questions from $D$ into questions concerning $M$. Choosing between the two companies would then amount to (a) determining the intervals in which one cost function exceeds the other and identifying the representation of the desired ride in one of these intervals, which leads to a mathematical conclusion of which function or functions have the lower value, and (b) translating this answer back to an answer saying "company T / U should be chosen for this ride" or "it doesn't matter which company you choose for this ride".

When a mathematical model is introduced (selected, modified or constructed) from scratch to deal with aspects of an extra-mathematical context and situation, we say that *mathematical modelling* is taking place. A person who from scratch introduces a model into a context is a *mathematical modeller* for that context. Sometimes a mathematical model is already present in a given context because it has been introduced by others. If so, we often speak of *an application* of mathematics. A person who investigates or assesses such a model may be called a *model analyst* for that context.

## The purpose, place and role of models and modelling

Since the late 1960s a growing community of mathematics educators have cultivated an interest in the purpose, place and role of mathematical applications, models and modelling in the teaching and learning of mathematics. This interest is based on two different but certainly compatible ideas. The first idea – of which "mathematics for applications, models and modelling" could be a slogan – is that the utilisation of mathematics in extra-mathematical contexts for extra-mathematical purposes is, in itself, an important activity and endeavour. Thus it should be a primary goal and task of mathematics education to enable students at various levels to engage in such activities. The second idea – sloganized as "applications, models and modelling for the learning of mathematics" – is that dealing with the activation of mathematics in extra-mathematical contexts for extra-mathematical purposes can foster motivation with (some) students for the study of mathematics and help support and consolidate their concept formation, sense-making and experience of meaning in and of mathematics. Thus, the teaching and learning of mathematics for its own sake can take advantage of applications, models and modelling. This is the case, for instance, with the so-called "realistic mathematics education" approach, taken by the Freudenthal Institute in the Netherlands. (For a more detailed account of these ideas, see Blum & Niss, 1991. The two "philosophies" are still significant within the field; see, for instance, Gravemeijer, 2007, and Lesh & Doerr, 2003.)

For a couple of decades mathematics educators working in this area focused on designing and implementing teaching plans and activities on applications, models and modelling, either as part of existing courses, curricula or programmes, or as entirely new teaching units, courses, curricula or programmes. To support all this, teaching materials, including textbooks, and assessment schemes were developed as well. Ideas, views and, above all, ex-

periences were presented and analysed in journals and books and were exchanged and discussed in conferences, such as the International Congresses on Mathematical Instructions (ICMEs) and particularly in the International Conferences on the Teaching of Mathematical Modelling and Applications (ICTMAs), inaugurated in the UK in 1983 and held biennially since then. The community which evolved around these conferences (the International Community of Teachers of Mathematical Modelling and Applications, also with ICTMA as its acronym) was officially established as an Affiliated Study Group of the International Commission on Mathematical Instruction (ICMI) in 2003. For a historical account of the conferences and the community, see Houston, Galbraith & Kaiser, 2008. For an account of the state of the art in the field, see Blum, Galbraith, Henn & Niss, 2007.

From the 1990s onwards, a large body of empirical research has been undertaken in order to investigate a variety of questions concerning the teaching and learning of models and modelling. In the remainder of this article we shall briefly outline a few of the most significant outcomes of this research.

## Selected solid findings

In the attempts during at least four decades to attribute a sizable place and role to models and modelling in different mathematics curricula and in different contexts of teaching and learning, two manifest observations emerged again and again. Later on these observations became supported by empirical research to such an extent that they have developed into solid findings of mathematics education research.

The *first* observation and finding is this: while knowledge of and skills in "pure" mathematics are, of course, necessary for an individual's ability to deal with models and to perform modelling, such knowledge and skills are far from sufficient for that undertaking. In other words, there is no guaranteed transfer from mathematical knowledge and skills to knowledge and skills concerning models and modelling. The literature contains many examples of students with a very good knowledge and skills base in mathematics who are not able (without specific teaching) to put their knowledge and skills to use in models and modelling contexts. One reason for this is that all the assumptions, simplifications and decisions, which usually have to be made in order to model a situation or context, involve considering and dealing with matters belonging to the extra-mathematical domain to be modelled. Moreover, it may be necessary to procure extra-mathematical facts, collect data or make measurements. All these things have to be handled on other than purely mathematical grounds. Some students – and some mathematics teachers, too – are unable, reluctant or unwilling to leave their mathematical quarters and do what it takes to engage with extra-mathematical matters while activating their mathematical knowledge and skills. Research publications underpinning this finding include Ikeda & Stephens (1998), Stillman (2002) and Kaiser & Maass (2007).

This first finding suggests that engaging in models and modelling has to be learnt in some way or another, but how can this take place? The big question then is whether it is possible to teach models and modelling in an effective manner so as to generate learning with students and, if so, under what conditions? Leaving aside for a moment the ensuing key questions of what learning of models and modelling means and of how we can recognise learning when it is present, we turn to the *second* observation and finding: the good news is that models and modelling can in fact be taught effectively so as to be learnt by students at various levels, but this requires investments and efforts in terms both of careful and focused design and of teaching and learning environments and activities, and in terms of sufficient time for the activities designed to unfold. It is part of this finding that genuine modelling skill cannot be developed with students by way of teaching focusing on stylised and stereotypical examples in the hope that this will result in transfer to real modelling situations and tasks. Research publications leading to the second solid finding include Ottesen (2001), Maass (2004), Blomhøj & Kjeldsen (2006) and Verschaffel et al. (1999).

We shall return to the questions set aside above. What does learning of models and modelling mean and how can we recognise it when we encounter it? Here, the so-called modelling competencies form the essential component. Theoretical and empirical research shows that being able to do modelling amounts to being able to successfully undertake a series of competencies called upon in the modelling cycle (see, for example, Blomhøj & Jensen, 2003, and Maass, 2006). A set of solid findings identifies the difficulties and challenges embedded in the set of modelling competencies, some of which give rise to obstacles to coming to grips with models and modelling (Galbraith & Stillman, 2006), whilst others put forward effective means for overcoming these difficulties and meeting these challenges. For example, the effects of the context of modelling tasks with an equivalent mathematical content can be dramatic, for better and for worse (Busse & Kaiser, 2003, Busse, 2011, and Stillman, 2000).

## References


Blomhøj, M., & Jensen, T.H. (2003). Developing mathematical modelling competence: conceptual clarification and educational planning. *Teaching Mathematics and Its Applications* 22(3), pp 123–139.

Blomhøj, M., & Kjeldsen, T.H. (2006). Teaching mathematical modelling through project work. *ZDM* 38(2), pp 163–177.

Blum, W., Galbraith, P.L., Henn, H.-W., & Niss, M. (Eds.) (2007). *Modelling and Applications in Mathematics Education. The 14th ICMI Study.* New York, NY: Springer Science + Business Media, LLC.

Blum, W., & Niss, M. (1991). Applied Mathematical Problem Solving, Modelling, Applications, and Links to Other Subjects – State Trends and Issues in Mathematics Instruction. *Educational Studies in Mathematics* 22, pp 37–68.

Busse, A. (2011). Upper secondary students' handling of real-world contexts. In G. Kaiser, W. Blum, R. Borromeo-Ferri, & G. Stillman, G. (Eds.) *Trends in teaching and learning of mathematical modelling*. ICTMA 14 (pp 37–46). New York, NY: Springer Science + Media, LLC.

Busse, A., & Kaiser, G. (2003) Context in application and modelling: An empirical approach. In Q. Ye, W. Blum, I.D. Huntley & N.T. Neil (Eds.), *Mathematical modelling in education and culture* (pp

95–107). Chichester, UK. Horwood.

Galbraith, P., & Stillman, G. (2006) A framework for identifying student blockages during transitions in the modelling process. *ZDM* 38(2), pp 143–162.

Gravemeijer, K. (2007). Emergent modelling as a precursor to mathematical modelling. In W. Blum, P. Galbraith, H.-W. Henn & M. Niss. (Eds.) (2007), *Modelling and Applications in Mathematics Education. The 14th ICMI Study* (pp 137–144). New York, NY: Springer Science + Business Media, LLC.

Houston, K., Galbraith, P., & Kaiser, G (2008). *The International Community of Teachers of Mathematical Modelling and Applications, also with ICTMA. The First Twenty-five Years*. www.icmihistory.unito.it, retrieved 3 October 2012.

Ikeda, T., & Stephens, M. (1998). The influence of problem format on students' approaches to mathematical modelling. In P. Galbraith, W. Blum, G. Booker & I.D. Huntley (Eds.) *Mathematical Modelling. Teaching and Assessment in a Technology-Rich World*. (pp 222–232). Chichester, UK: Horwood.

Kaiser, G., & Maass, K. (2007). Modelling in lower secondary mathematics classroom – problems and opportunities. In W. Blum, P. Galbraith, H-W. Henn & M. Niss. (Eds.) (2007), *Modelling and Applications in Mathematics Education. The 14th ICMI Study* (pp 99–108). New York, NY: Springer Science + Business Media, LLC.

Lesh, R. A., & Doerr, H. M (Eds.) (2003). *Beyond constructivism: Models and modelling perspectives on mathematics problem solving, learning and teaching*. Mahwah, N.J.: Lawrence Erlbaum

Maass, K. (2004). *Mahematisches Modellieren im Unterricht – Ergebnisse einer empirischen Studie*. Hildesheim: Franzbecker.

Maass, K. (2006) What are modelling competencies? *ZDM* 38(2), pp 113–142.

Niss, M., Blum, W., & Galbraith, P. (2007). Introduction. In W. Blum, P. Galbraith, H-W. Henn & M. Niss. (Eds.) (2007), *Modelling and Applications in Mathematics Education. The 14th ICMI Study* (pp 3–32). New York, NY: Springer Science + Business Media, LLC.

Ottesen, J. Do not ask what mathematics can do for modelling. In D. Holton (Ed.) *The teaching and learning of mathematics at university level. An ICMI Study*. (pp 335–346). Dordrecht, The Netherlands: Kluwer

Stillman, G. (2000). Impact of prior knowledge of task context on approaches to application tasks. *Journal of Mathematical Behavior* 19(3), pp 333–361.

Stillman, G. (2002). The role of extra-mathematical knowledge in application and modelling activity. *Teaching Mathematics* 27(2), pp 18–31.

Verschaffel, L., De Corte, E., Lasure, S., Van Vaerenbergh, G., Bogaerts, H., & Ratinckx, E. (1999). Design and evaluation of a learning environment for mathematical modeling and problem solving in upper elementary school children. *Mathematical Thinking and Learning*, pp 195–229.

# Grading Mathematics Education Research Journals

Guenter Toerner (Chair of EMS Committee for Education) and Ferdinando Arzarello (President of the European Society for Research in Mathematics Education, ERME)

## Presentation of the project and initial motives

Nowadays, all researchers are aware of the increasing importance accorded to the ranking and grading of scientific journals; it is now difficult to escape their influence. The systems that currently exist are often based on crude statistical analyses that have little to do with scientific quality (see, for example, Arnold & Fowler 2011). For these reasons, the Education Committee of the European Mathematical Society (EMS), together with the Executive Committee of the European Society for Research in Mathematics Education (ERME) and supported by the International Commission for Mathematical Instruction (ICMI), decided in 2011 to organise a consultation in order to propose a grading of research journals in mathematics education based on expert judgment. A similar project has already been carried out for chemical education and science education journals (Towns & Kraft, 2011).

The approach adopted was to initiate a process which will need further elaboration and regular updating. For this reason, amongst many possible choices of method, we always opted for what appeared to be the most straightforward. We present below our methods and the results obtained.

## Organisation of grading by experts

A working group, bringing together members of the ERME board and members of the EMS educational committee, was formed to take charge of the whole process. We (the members of this group) first prepared a long list comprising 49 journals. We graded the journals and compared our grades with the European Reference Index for the Humanities 2011 lists (https://www2.esf.org/asp/ERIH/Foreword/search.asp). This led us to retain a shortlist of 28 journals (all the mathematics education research journals mentioned as international on the ERIH list have been kept).

At the same time we constituted a panel of 91 experts in the field, representing the 42 countries members of the EMS and the ERME. Each country was represented by one to seven experts, according to the size of the mathematics education research community in each country.

These experts were contacted and asked to grade the journals, using the scale presented below. They were also invited to formulate any comments they wished to make on the process and to suggest other journal titles if they considered that important journals were missing from the list.

### Criteria

The experts were invited to grade the journals on a four-point scale: A*, A, B or C, or to declare that they did not know the journal and code it with an X. The scale was defined according to four dimensions, characterising each rank: recognition; review process and quality standards; editors and editorial board; and citations. For example, the ranks A and B are described as:

A
- Recognition: The journal is recognised amongst researchers around the world as a strong one in the field of mathematics education.
- Review process and quality standards: Through a systematic process of peer review the journal maintains high standards with a view to publishing research that displays the intellectual rigour, originality and significance that will be recognised as making a valuable contribution to the field.
- Editor(s) and editorial board: The editor(s) and the members of the editorial board of the journal are themselves highly regarded researchers, many already recognised as international leaders in the field of mathematics education.
- Citations: The journal is regularly cited in other journals, and many high quality research publications in mathematics education make some reference to work published in it.

B
- Recognition: The journal is recognised by researchers around the world as an estimable one in the field of mathematics education.
- Review process and quality standards: Through a process of peer review the journal sets standards of rigour, originality and significance that command international respect within the field.
- Editor(s) and editorial board: The editor(s) and the members of the editorial board of the journal are themselves well regarded researchers in the field of mathematics education.

### Answers and statistical choices

We received answers from 75 experts, representing 32 countries. In some answers, certain responses were missing; we replaced these by "X". A few experts proposed letters such as "D"; we replaced these with "C".

We decided to:

- Confirm a grade A* for all the journals rated A* by 50 experts or more (at least two thirds of the experts).
- Confirm a grade A (, B, C) to all the journals rated A (, B, C) or better by 50 experts or more (at least two thirds of the experts).
- Withdraw from the list all the journals that have more than 25 marked X (more than a third of the experts declare that they do not know the journal).

Some experts proposed additional titles. Nevertheless, no title was proposed by more than 8 experts; we thus decided not to add titles to the list.

### Results

Following these principles: two journals received a grade A*; five journals received a grade A; five journals received a grade B; and five journals received a grade C. Eleven journals were removed from the initial list of 28 because more than 25 experts declared that they did not know these journals.

The following table presents the final results of the grading process.

| Grade | Title |
|---|---|
| A* | Educational Studies in Mathematics |
| | Journal for Research in Mathematics Education |
| A | For the Learning of Mathematics |
| | Journal of Mathematical Behavior (The) |
| | Journal of Mathematics Teacher Education |
| | Mathematical Thinking and Learning |
| | ZDM: The International Journal on Mathematics Education |
| B | International Journal of Mathematical Education in Science and Technology |
| | International Journal of Science and Mathematics Education |
| | Mathematics Education Research Journal |
| | Recherches en Didactique des Mathématiques |
| | Research in Mathematics Education |
| C | Canadian Journal of Science, Mathematics and Technology Education |
| | Journal für Mathematik-Didaktik |
| | Nordisk matematikkdidaktikk / Nordic Studies in Mathematics Education, NOMAD |
| | Technology, Knowledge and Learning (formerly: International Journal of Computers for Mathematical Learning) |
| | The Montana Math Enthusiast |

### Limitations of the grading process and need for further studies

Naturally, this process has a number of limitations. We note some, here, that we discussed during our work and which were also expressed by some experts in their comments.

- A grading produced by European experts risks being Europe-centric.
- Only journals overtly focused on mathematics education have been included. Journals about education at large are also very important for the researcher in the field and are not mentioned in the list.
- The list contains mainly journals written in English.
- Journals about more specific topics, such as statistics education in particular, are unknown to many experts but may be of high scientific quality.

All these remarks correspond to real limitations of our study. They evidence the need for further studies: ICMI could decide a similar grading at a worldwide level and, equally, more local initiatives could better recognise

journals in languages other than English, or with specific foci. The scientific quality of journals is always evolving; a change in the reviewing process, for example, can lead to an improvement of a journal. Thus any grading should retain the possibility of updating and evolution; the grading proposed here is presented as our best attempt at assessing the current situation.

## References

Arnold, D. N., & Fowler, K.K. (2011). Nefarious numbers. *Notices of the AMS* 58 (3), 434–437.

Towns, M.H., & Kraft, A. (2011). The 2010 Rankings of Chemical Education and Science Education Journals by Faculty Engaged in Chemical Education Research. *Journal of Chemical Education* 2012, 89 (1), 16–20.

# Time Lag in Mathematical References

Thierry Bouche (Université de Grenoble, Saint-Martin d'Hères, France), Olaf Teschke (FIZ Karlsruhe, Berlin, Germany) and Krzyś Wojciechowski (University of Warsaw, Poland)

Results in mathematics do not just hold forever – we are also conscious of them for a long time. The Pythagorean Theorem still taught in schools may be an extreme example but also, in our specific research fields, specialists are usually aware of long-lasting conjectures which have influenced centuries of research or seemingly dead areas revived when looked upon by a new generation from a different angle.

Unfortunately, this very fascinating attribute of mathematical research has turned out to be a handicap in the scientometric age. When measures like impact factors came into use in the second half of the 20th century, they were initially limited to very recent data for very practical reasons: critical masses of references were generally not yet available or manageable for longer periods of time. As an effect, the computation of the usual impact factor is restricted to two years (some extensions go to the limit of at most five years). But what is lost? This leads to the natural question of the time lag for mathematics references, i.e. the average difference of the publication year of the citing and the cited article.

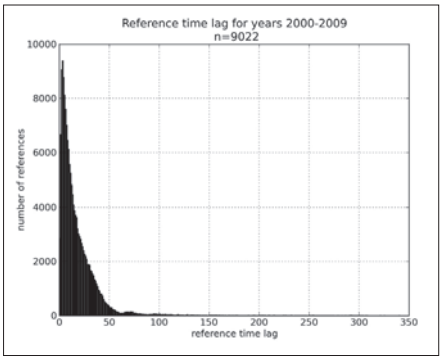
Surprisingly, this is not a question that is easy to answer. In an earlier issue, Rui Loja Fernandes[1] gave a good illustration in the example of the evaluation of the IST: Table 5 on p. 16 shows that both the aggregate cited and citing half-life in mathematics is longer than ten years on the sample of mathematics reflected in the ISI data. The recent progress of digital libraries over the last two decades contributes hitherto unavailable data to the pool and allows at least some glimpses into how mathematical information is alive through the decades.

Here, we start from two data sets which became only recently available: references extracted during the development of the European Digital Mathematics Library (EuDML)[2,3] and the set of references currently stored and identified in the zbMATH database.

Both sets are not ad hoc comparable: EuDML represents, with about 200,000 entries, a fraction of the literature now available in the public domain. For 44,817 articles (greater than 20%), references are now extracted from the digital full text but the data comes with the natural inaccuracies of automatic processing. Naturally, most of the cited articles are not contained in EuDML itself. On the other hand, the (about) 166,305 articles with references in zbMATH are a considerably smaller fraction of the total, greater than 3.2 million, items (just greater than 5%) but come along with the advantage of being mostly matched against the database, hence providing more accurate information.

However, there are also striking similarities: for both data sets, there are virtually no citing articles before 1890 and only very scarce cited articles before 1850. There is no surprise here. By now, references must obey at least rudimentary patterns (author, title, source, publication year) to be detected. This only came along with the appearance of scientific journals in larger numbers. (Note that the volumes of Euclid's *Elements* are rarely cited with their precise publication years).

Hence, when ignoring sparse data, we have a 120×140 years citation matrix, with zeroes below the obvious diagonal. (Actually, this is not so obvious in the case of zbMATH data: contrary to EuDML, there are several cases of negative time lag, which comes from the fact that "submitted/to appear"-articles in the references were identified in their final version in the zbMATH database, with a possibly delayed publication year. But this pertains to less than 0.1% of the references.) For easier representation, these data were grouped by decade of the citing articles; the typical picture can be seen below.




**Publication years of references of EuDML articles published 2000–2009; typically, the numbers can be approximated by a power law distribution.**

1 Evaluation of Faculty at IST – a Case Study. EMS Newsletter 84, 13–17.

2 http://eudml.org.

3 EMS Newsletter 76, June 2010, 11–16; ibid. 85, 57–58.

The following table shows both the average time lag and the median for EuDML and zbMATH references for the decades since 1890.

| | EuDML avg | zBMATH avg | EuDML median | zBMATH median |
|---|---|---|---|---|
| 1890–1899 | * | 9.88 | * | 8 |
| 1900–1909 | * | 9.07 | * | 7 |
| 1910–1919 | * | 10.07 | * | 7 |
| 1920–1929 | * | 13.07 | * | 10 |
| 1930–1939 | * | 11.13 | * | 8 |
| 1940–1949 | 16.39 | 15.74 | 12 | 12 |
| 1950–1959 | 11.46 | 12.66 | 8 | 8 |
| 1960–1969 | 10.39 | 11.14 | 7 | 8 |
| 1970–1979 | 10.10 | 10.80 | 7 | 8 |
| 1980–1989 | 12.40 | 12.18 | 9 | 10 |
| 1990–1999 | 14.99 | 13.28 | 11 | 10 |
| 2000–2009 | 17.41 | 14.64 | 12 | 11 |

**Average and median time lag in mathematical reference per decade. *No figures derived from EuDML because only scarce data available.**

One observation is a larger difference between EuDML and zbMATH data before 1930 and after 2000. The effect in the early decades is simply due to the fact that EuDML has very few articles with references in this period. Furthermore, the section of EuDML articles after 2000 is quite different from the earlier corpus because there are fewer sources which provide articles that recent.

When we exclude this, maybe the most striking observation is that both data sets show very similar patterns, with the main influences seeming not to be related to developments in mathematics but just to the two World Wars! The two local maxima in the '20s and '40s in the more comprehensive zbMATH data seem to be directly linked to the fact that there are many references bridging the war gaps. Consequently, the time lag is reduced in the following decades, reaching a minimum in the '70s. Interestingly enough, the time lag starts growing again after then, with no indication that the faster availability of information or the acceleration of academic activities in the last decades had any chance in stopping this process (on the contrary, the enhanced accessibility of older articles through digital libraries may actually have the effect of an increase of the citations with larger time lag). The most likely explanation for the minimum in the '70s is just that there were simply "not enough older papers there" to be cited due to wartime – an effect that is now slowly dissolving. It is still unclear when the growth of average time lag may come to an end but if we accept that the World War II gap came into full effect in time lag only three decades later, it may well be expected that the average time lag stabilises beyond 20 years.

Another question pertains to the small but visible differences in time lag for EuDML and zbMATH data for recent decades, where both services have a comparable magnitude of data and one would expect convergence. The higher time lag (by about 1.5 years over the last two decades) in EuDML seems to be influenced by two effects: firstly, zbMATH identifies more recent references which appear initially without a publication year and,


**Average reference time lag per year in zbMATH data.**

secondly, the zbMATH scope includes relatively more articles from areas like mathematical physics (MSC 70-86) or mathematics related to computer science (MSC 68), where the time lag in citations is significantly smaller than in the areas predominant in EuDML articles. On the other hand, the open access nature of EuDML articles seems to have no influence on time lag right now, which is not too surprising if we take into account that the average citation still goes back to the times when digital libraries had just begun.

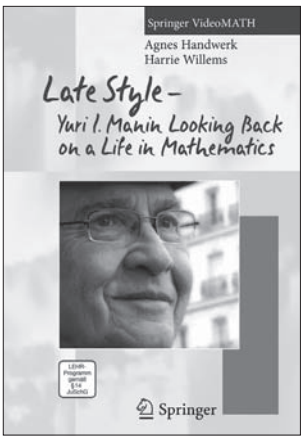
Without doubt, these are just first estimates – there will be more data available soon and many questions (e.g. normalisations with respect to publication growth or citing behaviour, differences according to MSC areas, sources, etc.) are just at the beginning. Just one thing seems to be certain – things just start to be interesting when going more than 10 years back – a period of time which is usually omitted.

*Thierry Bouche [thierry.bouche@ujf-grenoble.fr] is maître de conférences at Institut Fourier (Université Joseph-Fourier, Grenoble, France) and director of Cellule Mathdoc (a joint service unit of CNRS and UJF). He is scientific coordinator of the EuDML project, and member of the following committees: Electronic Publication Committee (EMS), Committee on Electronic Information and Communication (IMU), Conference on Intelligent Computer Mathematics steering committee.*

*Olaf Teschke [teschke@zblmath.fiz-karlsruhe.de] is member of the Editorial Board of the EMS Newsletter, responsible for the Zentralblatt Column.*

*Krzyś Wojciechowski [k.wojciechowski@icm.edu.pl] is a software architect in the Interdisciplinary Centre for Mathematical and Computational Modelling of the University of Warsaw. His professional interests concentrate mostly on data mining, machine learning and big data processing. He currently holds the position of technical coordinator in the EuDML project [http://eudml.org].*

# Book Reviews




Agnes Handwerk
Harrie Willems

**Late Style – Yuri Ivanovich Manin**
**Looking Back on a Life in Mathematics**

DVD-Video NTSC, 60 min.
Series: Springer VideoMATH
ISBN 978-3-642-24482-7

Reviewer: Thomas Vogt

There is a new mathematics film that is worth seeing if not buying: a sensitive portrait of the renowned Russian mathematician Yuri Ivanovich Manin. The documentary "Late Style" is the second piece by the filmmakers Agnes Handwerk and Harrie Willems in Springer's VideoMATH series. Their first documentary on the short life of the mathematical genius Wolfgang Doeblin is a hidden treasure from 2007. Now Yuri Manin…

The journalists and documentary film directors Agnes Handwerk (Hamburg) and Harrie Willems (Amsterdam) visited Manin again and again over several years, following him to Moscow, Paris and Bonn. Spending time with Manin over a long period of time they managed to catch private – almost intimate – situations, statements and thoughts. Taking him back to many places of his private and professional life in Russia, France and Germany the mathematician Manin and his work become alive in a very subtle way.

The film starts in Moscow with Yuri Manin studying documents from the Soviet era together with his wife Xenia Semenova. These images may stand for the thread of the film: a review of former documents, places and persons. Agnes Handwerk and Harrie Willems take Yuri Manin and take us (the viewers) to Manin's apartment in Moscow, to Moscow State University, to the institutes abroad where he worked and – in the end – to the place of his birth.

Back to Moscow in 1953: in the very year in which Stalin died, the new building of Moscow State University was opened – and Yuri Manin started his studies in mathematics. "When I entered Moscow University the most important new results in number theory then were connected with algebraic geometry…" remembers Manin. He then reads letters he sent to his mother in Simferopol – and the fruitful years of his studies at Moscow University become alive: the lessons of Igor Shafarevich that he attended and his (Manin's) urgent desire to solve the problems that were posed ("If I don't do it by tomorrow, it will be a disaster!").

Another technique Handwerk and Willems use to make the years of the Soviet era come alive is to show a good selection of photographs of that time: of Manin's fellow students and teachers, and private snapshots, for instance of a joint canoe trip with his teacher Shafarevich and co-students like Sergei Novikov and others. Manin talks about the International Congress of Mathematicians in Moscow in 1966, where he met colleagues from Western countries like Léon Motchane. The founder of the Institut des Hautes Études Scientifiques (IHÉS) at Bures-sur-Yvette near Paris invited him to France – an invitation that Manin would accept later on. And Manin reports about the diplomatic uproar which Fields Medallist Steven Smale provoked when he asked his colleagues to register opposition to the Soviet invasion of Hungary and to the American war in Vietnam.

The documentary filmmakers travelled with Manin to the IHÉS at Bures-sur-Yvette, where he had worked together with Alexander Grothendieck in the 1960s. The actual event in the film Manin takes part in is a celebration in honour of Grothendieck's 80th birthday in January 2009. This gives the film directors the opportunity to ask Manin about the influence Grothendieck had on him and on mathematics in general – and to show him during a lecture on "motives and quantum cohomology".

Then and repeatedly Handwerk and Willems ask Manin about the political events of that time and his opinion of these. They get rare political statements from Manin that way. Asked about the student revolts in France during the 1960s, for instance, Manin talks about a student who promoted Mao Zedong's ideas in the streets of Paris. "I was somewhat sad seeing them doing propaganda, doing things not worth of their enthusiasm … Mao Zedong … we knew very well what was Mao Zedong … he was much worse a version than Stalin … and to take him as ideal meant that they did not understand anything about reality … and that saddened me very much."

Manin was awarded the Lenin Prize in 1967. He realises that he is accepted and honoured by people he did not wanted to be accepted by. "I had to do something that would show them I'm not theirs – but didn't want to do anything more. I felt that I don't have the character of an active dissident or so. I just signed some protest letters; that was it. That was sufficient to show them that I'm not theirs but I did not continue this dissident's activities ... I just kept my small circle of students, of family and of mathematics, so that was my decision," says Manin. For that Yuri Manin got punished. He was not allowed to travel abroad for the next 20 years and not allowed to teach standard courses for students during their first years but only special seminars to the older ones. The aim was to restrict Manin; but what happened was that only the best students would come to him that way. "It was no punishment at all!" says Manin. Manin was not allowed to travel abroad but continued to communicate with mathematicians abroad like Deligne, Grothendieck, Mumford, Serre and Cartier.

In the second part of the movie some of Manin's colleagues and students are interviewed about Yuri Manin, among them Alexander Beilinson (University

of Chicago), a student of Yuri Manin in the 1970s, and Pierre Deligne (Princeton), who visited Manin in Moscow in 1972. "Manin was not in danger," says Deligne in the film, "but he suffered because his students suffered … their possibilities were very limited although they were very good." One of them was Michael Tsfasman, who had started his studies at Moscow State University in 1971. He reports in the film how two thirds of the students from Highschool No. 2, a top level college in Moscow, were not given the possibility to study because they were Jews, not communists or simply independent thinkers. Michael Tsfasman says he only got a chance to study at Moscow University because he was selected for the Russian team at the International Mathematical Olympiad (IMO); IMO participants were allowed to enter Russian top universities without exams and other selection processes.

Manin's life changed a lot after the fall of the Iron Curtain when he was allowed to travel again; for many years he had received invitations to congresses and meetings without being able to go to them. Friedrich Hirzebruch, professor of mathematics at Bonn University and the founder of the Max Planck Institute for Mathematics in Bonn, had invited Russian Mathematicians to Bonn every year since 1957, among them Yuri Manin. And Manin went to Bonn with four other mathematicians, on his way back to Russia from Paris in 1967. He gave a lecture about a problem in algebraic geometry at one of Hirzebruch's Arbeitstagungen. Hirzebruch reports in the film that he invited Manin again and again during the Cold War. After the Iron Curtain had finally fallen Manin accepted some invitations from Western universities and – enjoying the work abroad – resigned from his professorship at Moscow State University. One day Hirzebruch – close to his own retirement – visited Manin at Harvard and asked him to become his successor at the Max Planck Institute for Mathematics in Bonn; eventually Manin accepted. Another co-director of the Max Planck Institute of Mathematics, Don Zagier, talks in the film very warmly about Manin's style, about his greatest talent: how Manin was often able to see unexpected and surprising connections between two different branches of mathematics where no connections had appeared before – and establishing them successfully with creative ideas and persistency.

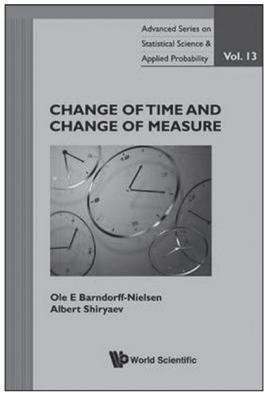
The last part of the movie is about Manin's childhood; it shows where and how he grew up. When Manin was five years old, he lost his father in World War II. His education started at School No. 7 in Simferopol, the capital of the Crimea; his first contact with another language was when he read Gulliver's Travels in English. Manin takes the viewers of the film back to his hometown Simferopol. We see Manin visiting the two houses of his childhood after decades of absence.

Then the title "Late Style" is explained at last. "Late style I think quite well explains this emotional atmosphere of returning to one's remote past," says Manin. "It's kind of you want to connect the beginning and the end of your life … you want to see some kind of entirety …"

**Photo taken by Michael Ebner**

*Thomas Vogt [th.vogt@fu-berlin.de] studied geology, German literature and science journalism in Berlin. He has written for a Berlin daily newspaper and has worked as a press officer for the Helmholtz Association and the Leibniz Association. In 2008 he provided content (print and online) for Germany's "Year of Mathematics" – a national campaign to present mathematics to society at large. Since then he has been press officer of the German Mathematical Society (DMV) and has provided news on mathematics for the media and the general public via DMV's mathematics media office.*

---




Ole E. Barndorff-Nielsen
Albert Shiryaev

**Change of Time and Change of Measure**

World Scientific, 2010
305 pages
ISBN-13 978-981-4324-47-2

Reviewer: Juan-Pablo Ortega

Mathematical finance is one of the most recent examples in the long list of successful instances of cross-fertilisation between pure mathematics and a domain of human knowledge in need of a rational and quantitative formulation of natural questions associated to it. Since Galilean times and up to the last century, this symbiosis linking mathematics to other disciplines took place mainly in the arenas of natural sciences and engineering. The important development during the last century of the mathematics of randomness (probability theory, theory of stochastic processes, statistical modelling, to give a few names) has created an array of powerful tools capable of handling the complex phenomena and uncertain outcomes usually studied within the realm of social sciences. Indeed, experience has shown that a probabilistic treatment of many problems arising in, for example, demography, economics, epidemiology and finance is much more pertinent than the one coming from classical deterministic methods. Even though this conceptual leap took some time to be assimilated, its result seems to be by now an established certitude.

This book takes two major ideas at the core of mathematical finance, namely the use of equivalent (martingale) measures and the equivalent (change of time and stochastic volatility) representations of a stochastic process, and uses them as a motivation to describe a variety of topics in stochastic analysis. The result is a beautiful and well-articulated monograph, full of information, where the interplay between deep mathematical ideas and extremely explicit and applied financial problems and their solutions is generously exemplified.

The change of time and the stochastic integral representation problems aim at rewriting a given stochastic process in terms of a simpler one (it can be a Brownian motion or, in general, a semimartingale) via a stochastic change of time and stochastic integration, respectively. The first approach is analysed in Chapter 1 of the book, in which all the necessary concepts having to do with stopping times and random changes of time are described, as well as the Dambis-Dubins-Schwarz Theorem that explains how any continuous martingale can be obtained out of a Brownian motion via a random change of time. The integral representation problem is tackled in Chapters 2 and 3 and gives the authors the opportunity to construct in a reduced number of pages a delightful presentation of the most relevant results in relation with stochastic integration and stochastic differential equations.

The existence and uniqueness results that are presented in those pages and that solve the described representation problems are not just deep and beautiful mathematical theorems but they also constitute key results in the understanding of important questions in mathematical finance. This interplay is presented mainly in Chapters 10 and 11. Indeed, the change of time representation provides mathematical legitimacy to a common interpretation of volatility among finance practitioners that consists of visualising moments of high fluctuation of the prices with an acceleration of the so-called operational or business time. Moreover, the existence of an integral representation for a process with a predictable integrand amounts in financial language to the availability of a self-financing trading strategy that replicates (or hedges, in financial jargon) a derivative product whose underlying asset has a dynamical behaviour described by the process in question. This makes of this mathematical construction, together with the notion of martingale or risk-neutral measure that we will review later on, a main building block of the no-arbitrage pricing and hedging theory of derivative securities. Indeed, when the underlying asset is described by a lognormal process (also called geometric Brownian motion), it gives rise to the Black-Scholes-Merton formulas for the price and the hedges of European style options, for which Robert Merton and Myron Scholes received in 1997 the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel (usually referred to as the Nobel Prize in Economics) and that made viable the massive and industrial scale trading of these securities.

Changes of measure are treated in Chapters 6 and 7. The goal is again reducing a given stochastic process to a simpler one by using in this case an equivalent probability measure; more specifically, the procedure aims at constructing a new measure that is absolutely continuous with respect to the original one, such that the law of the stochastic process under study "seen with the eyes" of this new measure coincides with the one coming from a simpler process like Brownian motion. There are several constructions available in the literature that serve this purpose. The book examines two of them: the Girsanov Theorem, of much use in mathematical finance, and the Esscher Transform, introduced initially in the context of actuarial sciences. Both procedures are constructive and provide new measures under which the stochastic process we are interested in becomes a martingale.

Again, the impact of these captivating mathematical constructions goes beyond a pure mathematical interest and has far-reaching implications in mathematical finance that are spelled out in Chapters 10 and 11. Indeed, the importance of the existence of an equivalent martingale measure for a (discounted) price process is captured in the so-called First Fundamental Theorem of Arbitrage Theory that establishes the equivalence between the availability of these measures and the absence of arbitrage opportunities in the market under study. This link is of paramount importance because many constructions in finance have the nonexistence of arbitrage opportunities, i.e. the impossibility of guaranteed profits without risk taking, as a fundamental hypothesis; this assumption is very plausible in highly liquid and efficient markets where results coming from mathematical finance are regularly applied.

Another fascinating link between two of the core ideas in the book, namely the existence of martingale measures and of integral representations and their application in mathematical finance, is provided by the Second Fundamental Theorem of Arbitrage Theory, also examined in Chapter 10. When we are in the presence of an underlying asset whose dynamics is such that there exists an integral representation for any contingent product, we say that the corresponding market is complete; according to what we said above, in complete markets any derivative product can be perfectly hedged/replicated. The Second Fundamental Theorem of Arbitrage Theory establishes the equivalence between the completeness of a market and the uniqueness of an equivalent martingale measure.

The book does not restrict itself to stating the basic concepts underlying mathematical finance and their connection with stochastic calculus that are available in so many other monographs. Indeed, it manages to present in a reduced number of pages most models that are used by practitioners when trying to solve the deficiencies of the Black-Scholes-Merton model that have been profusely documented over the years. Chapter 9 opens this discussion in the discrete time setup by introducing the ARMA/GARCH parametric family of time series models driven by a variety of different innovations (Inverse Gaussian, Generalised Inverse Gaussian, Generalised Hyperbolic, etc.) whose use aims at appropriately modelling stylised features of time series of financial returns that are em-

pirically observed, like, for example, leptokurtosis (the likelihood of extreme events is higher than the one associated to the Gaussian distribution), volatility clustering (moments of high volatility tend to accumulate in time) or asymmetry (bad market days create more volatility than good ones). The analogue of this discussion in continuous time is carried out in Chapter 12, which contains a pleasantly readable presentation of stochastic volatility and Lévy processes introduced in the light of the integral and change of time representations, respectively, at the heart of the book.

Even though the book includes self-contained accounts of a variety of topics in stochastic analysis, like stochastic integration, stochastic differential equations, equivalent martingale measures, Lévy processes and stochastic volatility models, to name a few, it is not written as a textbook and is not well suited for a reader who would like to use it as an entry door to the field; the proofs for most results are not included, the book is not linear and, despite the presence of numerous examples, the book contains no exercises. Like most of the titles in World Scientific's Advanced Series on Statistical Science and Applied Probability, the reader is expected to have some acquaintance with the various subjects covered by the volume. The style of presentation and the contents makes this enjoyable book ideal for a reader interested in going deeper in understanding the area or in having a panoramic view of it. For that category of readers, this book will certainly provide an opportunity to learn additional results and to establish beautiful connections between them, all of it elegantly illustrated with one of the most relevant and impressive applications of this mathematical field.

*Juan-Pablo Ortega [juan-pablo.ortega@univ-fcomte.fr] is a Chargé de Recherche at the French Centre National de la Recherche Scientifique. He has a first degree in physics from the Universidad de Zaragoza (Spain) and a MA and PhD in mathematics from the University of California, Santa Cruz (USA). He was a recipient of the 2000 edition of the Ferran Sunyer i Balaguer Prize (with Tudor S. Ratiu) and was an invited speaker at the ECM, Barcelona, 2000. His research focuses on geometric mechanics and, more recently, statistical modelling, financial econometrics and mathematical finance.*

# Personal Column

*Please send information on mathematical awards and deaths to Mădălina Păcurar [madalina.pacurar@econ.ubbcluj.ro]*

## Awards

10 **EMS Prizes** have been awarded to young researchers not older than 35 years, of European nationality or working in Europe, in recognition of excellent contributions in mathematics: **Simon Brendle** (Stanford University, USA), **Emmanuel Breuillard** (Universite Paris-Sud, Orsay, France), **Alessio Figalli** (University of Texas at Austin, USA), **Adrian Ioana** (University of California at San Diego, USA), **Mathieu Lewin** (University of Cergy-Pontoise, France), **Ciprian Manolescu** (UC in Los Angeles, USA), **Grégory Miermont** (Université Paris-Sud 11, France), **Sophie Morel** (Harvard University, USA), **Tom Sanders** (University of Oxford, UK), **Corinna Ulcigrai** (University of Bristol, UK).

The 2012 **Nobel Prize in Economics** has been awarded to **Alvin Roth** (Harvard University, Cambridge, USA, Harvard Business School, Boston, USA) and **Lloyd Shapley** (University of California, Los Angeles, USA).

The 2012 **Blaise Pascal Medal** in Mathematics has been awarded to **Franco Brezzi** (Istituto di Matematica Applicata e Tecnologie Informatiche del C.N.R., Pavia, Italy).

The **Servant Prize** has been awarded to **Jean-Yves Chemin** (Université Pierre et Marie Curie, France).

The 2012 **Ramanujan Prize** for Young Mathematicians from Developing Countries has been awarded to **Fernando Codá Marques** (Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, Brazil).

The 2012 **Blackwell-Tapia Prize** has been awarded to **Ricardo Cortez** (Tulane University, USA).

The Prize **José Luis Rubio de Francia** 2011 has been awarded to **Alberto Enciso Carrasco** (ICMAT, Spain).

The 2012 **Ramiro Melendreras Prize** was awarded to **Francisco Javier Martín** (Universidad Complutense de Madrid, Spain ).

The 2012 **Shaw Prize** in Mathematical Sciences has been awarded to **Maxim L. Kontsevich** (Institut des Hautes Études Scientifiques, France).

The **Jaffé Prize** in mathematics has been awarded to **Jean-Pierre Labesse** (Université d'Aix-Marseille, France).

The 2012 **Sylvester Medal** has been awarded to Professor **John Toland** FRS (University of Cambridge, UK).

The **Louis Bachelier Prize** has been awarded to **Nizar Touzi** (École Polytechnique, France).

The 2012 **André Lichnerowicz Prize** in Poisson Geometry has been awarded to **Thomas Willwacher** (Harvard University, USA).

The 2012 **Henri Poincaré Prize** has been awarded to **Nalini Anantharaman** (CNRS / Université Paris-Sud, France), **Sylvia Serfaty** (CNRS/UPMC), **Barry Simon** (Caltech, USA) and **Freeman Dyson** (Princeton, USA).

The 2012 **Fundamental Physics Prize** has been awarded to **Maxim Kontsevich** (Institut des Hautes Études Scientifiques, France and University of Miami, USA), **Nathan Seiberg** (Institute for Advanced Study, Princeton, USA) and **Edward Witten** (Institute for Advanced Study, Princeton, USA).

**Ingrid Daubechies** (Duke University, USA, President of the IMU) has been ennobled to the title of **Baroness** by the king of Belgium for her work on wavelets.

The 2012 **Cantor Medal** of the German Mathematical Society (DMV) goes to **Michael Struwe** (ETH, Zürich), in recognition for his outstanding achievements in the field of geometric analysis, calculus of variations and nonlinear partial differential equations.

The 2012 **von Kaven-Prize** of the Deutsche Forschungsgemeinschaft (DFG) is granted to **Eva Viehmann** (TUM, München, Germany), for her excellent work in the field of arithmetic algebraic geometry.

The **Klaus Tschira Award** for understandable science in the category of mathematics for 2012 goes to **Andreas Potschka** (University of Heidelberg, Germany).

**Grégoire Allaire** (École Polytechnique, France) has been elected new **president of SMAI** (Société de Mathématiques Appliquées et Industrielles).

**Carles Simó** (Universitat de Barcelona) has been awarded the **National Research Award** 2012 from the Catalan Foundation for Research and Innovation, with support from the Government of Catalonia.

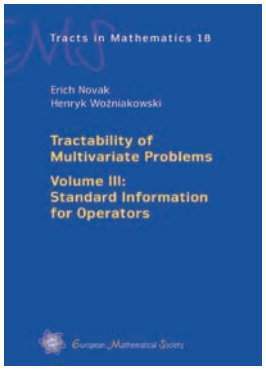
## Deaths

We regret to announce the deaths of:

**Shreeram Shankar Abhyankar** (2 November 2012, USA)
**Stelios Andreadakis** (9 February 2012, Greece)
**Nicolaas G. de Bruijn** (17 February 2012, Netherlands)
**Vladimir Savelievich Buslaev** (14 March 2012, Russia)
**Doris Lai Chue Chen** (3 June 2012, UK)
**Stefan Dodunekov** (5 August 2012, Bulgaria)
**Michael S. P. Eastham** (27 October 2012, UK)
**José Javier Etayo Miqueo** (11 September 2012, Spain)
**Pablo González Vera** (11 July 2012, Spain)
**Friedrich Hirzebruch** (27 May 2012, Germany)
**Joram Lindenstrauss** (29 April 2012, Israel)
**Jean-Louis Loday** (6 June 2012, France)
**Andrzej Orchel** (22 January 2012, UK)
**Christopher Shaddock** (8 March 2012, UK)
**Tonny Springer** (7 December 2011, Netherlands)
**John Taylor** (10 March 2012, UK)
**William Thurston** (21 August 2012, USA)
**Antonio Valle Sánchez** (24 June 2012, Spain)
**Thomas Wagenknecht** (1 May 2012, UK)

# New books published by the European Mathematical Society

**Individual members of the EMS, member societies or societies with a reciprocity agreement (such as the American, Australian and Canadian Mathematical Societies) are entitled to a discount of 20% on any book purchases, if ordered directly at the EMS Publishing House.**

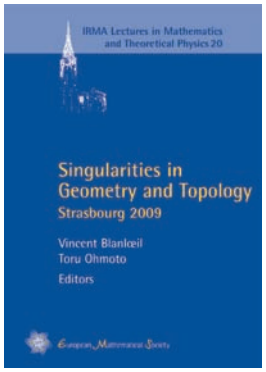



Erich Novak (University of Jena, Germany) and Henryk Woźniakowski (Columbia University, New York, USA, and University of Warsaw, Poland)

**Tractability of Multivariate Problems**. Volume III: Standard Information for Operators (EMS Tracts in Mathematics, Vol. 18)

ISBN 978-3-03719-116-3. 2012. 604 pages. Hardcover. 17 x 24 cm. 98.00 Euro

This is the third book of the comprehensive three-volume set studying the tractability of multivariate problems. It covers linear and selected nonlinear operators and can, to a large extent, be read independently of volumes I and II. The most important example studied is the approximation of multivariate functions. It turns out that many other linear and some nonlinear problems are closely related to the approximation of multivariate functions. While the lower bounds obtained in volume I for the class of linear information also yield lower bounds for the standard class of function values, new techniques for upper bounds are presented in volume III. One of the main issues here is to verify when the power of standard information is nearly the same as the power of linear information. In particular, for the approximation problem defined over Hilbert spaces, the power of standard and linear information is the same in the randomized and average case (with Gaussian measures) settings, whereas in the worst case setting this is not true.
The book is of interest to researchers working in computational mathematics, especially in approximation of high-dimensional problems. It may be well suited for graduate courses and seminars. The text contains 58 open problems for future research in tractability.

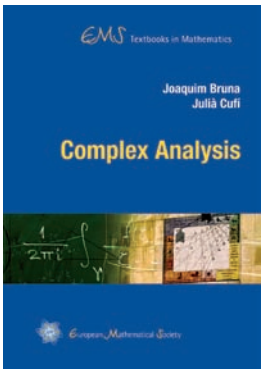



Vincent Blanlœil (Université de Strasbourg, France) and Toru Ohmoto (Hokkaido University, Sapporo, Japan)

**Singularities in Geometry and Topology.** Strasbourg 2009 (IRMA Lectures in Mathematics and Theoretical Physics, Vol. 20)

978-3-03719-118-7. 2012. 370 pages. Softcover. 17 x 24 cm. 48.00 Euro

This volume arises from the 5th Franco-Japanese Symposium on Singularities, held in Strasbourg in August 2009. The conference brought together an international group of researchers working on singularities in algebraic geometry, analytic geometry and topology, mainly from France and Japan. Besides, it also organized a special session, JSPS Forum on Singularities and Applications, which was aimed to introduce some recent applications of singularity theory to physics and statistics.
The book comprises research papers and short lecture notes on advanced topics on singularities. Some surveys on applications that were presented in the Forum are also added. Topics covered include splice surface singularities, *b*-functions, equisingularity, degenerating families of Riemann surfaces, hyperplane arrangements, mixed singularities, jet schemes, noncommutative blow-ups, characteristic classes of singular spaces, and applications to geometric optics, cosmology and learning theory.
Graduate students who wish to learn about various approaches to singularities, as well as experts in the field and researchers in other areas of mathematics and science will find the contributions to this volume a rich source for further study and research.

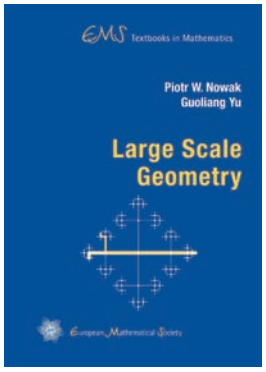



Joaquim Bruna and Julià Cufí (both Universitat Autònoma de Barcelona, Spain)

**Complex Analysis** (EMS Textbooks in Mathematics)

ISBN 978-3-03719-111-8. 2013. Approx. 592 pages. Hardcover. 16.5 x 23.5 cm. 58.00 Euro

The theory of functions of a complex variable is a central theme in mathematical analysis that has links to several branches of mathematics. Understanding the basics of the theory is necessary for anyone who wants to have a general mathematical training or for anyone who wants to use mathematics in applied sciences or technology.
The book presents the basic theory of analytic functions of a complex variable and their points of contact with other parts of mathematical analysis. This results in some new approaches to a number of topics when compared to the current literature on the subject.
The text can be used as a manual for complex variable courses of various levels and as a reference book. The only prerequisites for reading it is a working knowledge of the topology of the plane and the differential calculus for functions of several real variables. A detailed treatment of harmonic functions also makes the book useful as an introduction to potential theory.



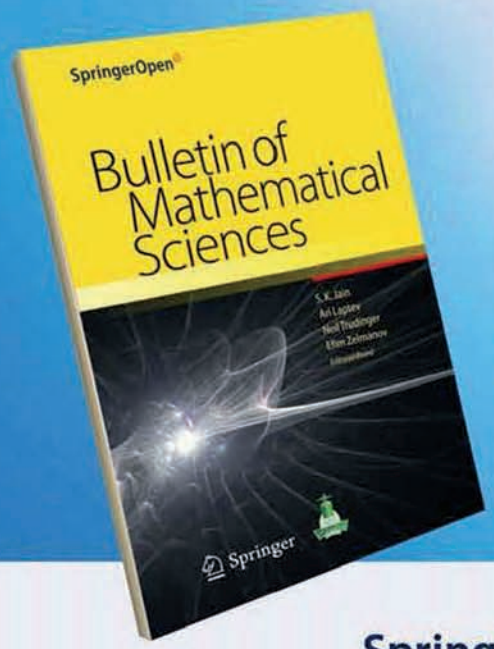

Piotr W. Nowak (IMPAN, Warsaw, Poland) and Guoliang Yu (Texas A&M University, College Station, USA)

**Large Scale Geometry** (EMS Textbooks in Mathematics)

ISBN 978-3-03719-112-5. 2012. 203 pages. Hardcover. 16.5 x 23.5 cm. 38.00 Euro

Large scale geometry is the study of geometric objects viewed from a great distance. The idea of large scale geometry can be traced back to Mostow's work on rigidity and the work of Švarc, Milnor and Wolf on growth of groups. In the last decades, large scale geometry has found important applications in group theory, topology, geometry, higher index theory, computer science, and large data analysis. This book provides a friendly approach to the basic theory of this exciting and fast growing subject and offers a glimpse of its applications to topology, geometry, and higher index theory. The authors have made a conscientious effort to make the book accessible to advanced undergraduate students, graduate students, and non-experts.

European Mathematical Society Publishing House
Seminar for Applied Mathematics, ETH-Zentrum SEW A27
Scheuchzerstrasse 70
CH-8092 Zürich, Switzerland
orders@ems-ph.org
www.ems-ph.org




# Bulletin of Mathematical Sciences

Launched by King Abdulaziz University, Jeddah, Saudi Arabia

SpringerOpen

## Bulletin of Mathematical Sciences

Launched by King Abdulaziz University, Jeddah, Saudi Arabia

OPEN ACCESS

### Aims and Scope

The *Bulletin of Mathematical Sciences*, a peer-reviewed open access journal, will publish original research work of highest quality and of broad interest in all branches of mathematical sciences.
The *Bulletin* will publish well-written expository articles (40–50 pages) of exceptional value giving the latest state of the art on a specific topic, and short articles (about 10 pages) containing significant results of wider interest. Most of the expository articles will be invited.



### Forthcoming articles include:

- **Loewy decomposition of linear differential equations**, by Fritz Schwarz
- **Optimal and isodual ternary cyclic codes of rate 1/2**, by Cherif Mihoubi und Patrick Sole
- **Negative spectra of elliptic operators**, by Stanislav Molchanov und Oleg Safronov
- **Direct-sum decompositions of modules with semilocal endomorphism rings**, by Alberto Facchini
- **Finite rank Bargmann-Toeplitz operators with non-compactly supported symbols**, by Grigori Rozenblum