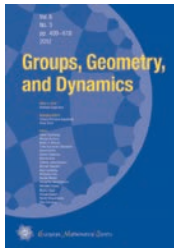


NEWSLETTER

OF THE EUROPEAN MATHEMATICAL SOCIETY





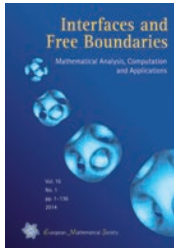
ISSN print 1661-7207
ISSN online 1661-7215
2016. Vol. 10. 4 issues
Approx. 1200 pages. 17.0 x 24.0 cm
Price of subscription:
338 € online only
398 € print+online

Editor-in-Chief:

Rostislav Grigorchuk (Texas A&M University, College Station, USA; Steklov Institute of Mathematics, Moscow, Russia)

Aims and Scope

Groups, Geometry, and Dynamics is devoted to publication of research articles that focus on groups or group actions as well as articles in other areas of mathematics in which groups or group actions are used as a main tool. The journal covers all topics of modern group theory with preference given to geometric, asymptotic and combinatorial group theory, dynamics of group actions, probabilistic and analytical methods, interaction with ergodic theory and operator algebras, and other related fields.



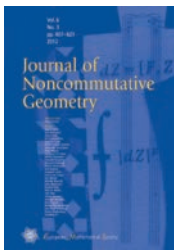
ISSN print 1463-9963
ISSN online 1463-9971
2016. Vol. 18. 4 issues
Approx. 500 pages. 17.0 x 24.0 cm
Price of subscription:
390 € online only
430 € print+online

Editors-in-Chief:

José Francisco Rodrigues (Universidade de Lisboa, Portugal)
Charles M. Elliott (University of Warwick, Coventry, UK)
Harald Garcke (Universität Regensburg, Germany)
Juan Luis Vazquez (Universidad Autónoma de Madrid, Spain)

Aims and Scope

Interfaces and Free Boundaries is dedicated to the mathematical modelling, analysis and computation of interfaces and free boundary problems in all areas where such phenomena are pertinent. The journal aims to be a forum where mathematical analysis, partial differential equations, modelling, scientific computing and the various applications which involve mathematical modelling meet.



ISSN print 1661-6952
ISSN online 1661-6960
2016. Vol. 10. 4 issues
Approx. 1200 pages. 17.0 x 24.0 cm
Price of subscription:
298 € online only
358 € print+online

Editor-in-Chief:

Alain Connes (Collège de France, Paris, France)

Aims and Scope

The *Journal of Noncommutative Geometry* covers the noncommutative world in all its aspects. It is devoted to publication of research articles which represent major advances in the area of noncommutative geometry and its applications to other fields of mathematics and theoretical physics. Topics covered include in particular: Hochschild and cyclic cohomology; K-theory and index theory; measure theory and topology of noncommutative spaces; operator algebras; spectral geometry of noncommutative spaces; noncommutative algebraic geometry; Hopf algebras and quantum groups; foliations, groupoids, stacks, gerbes.



ISSN print 1664-039X
ISSN online 1664-0403
2016. Vol. 6. 4 issues
Approx. 800 pages. 17.0 x 24.0 cm
Price of subscription:
238 € online only
298 € print+online

Editor-in-Chief:

Fritz Gesztesy (University of Missouri, Columbia, USA)

Deputy Chief Editor:

Ari Laptev (Imperial College, London, UK)

Aims and Scope

The *Journal of Spectral Theory* is devoted to the publication of research articles that focus on spectral theory and its many areas of application.



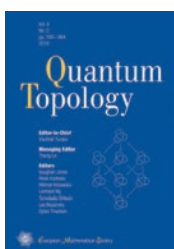
ISSN print 2308-1309
ISSN online 2308-1317
2016. Vol. 3. 4 issues
Approx. 400 pages. 17.0 x 24.0 cm
Price of subscription:
198 € online only
238 € print+online

Editor-in-Chief:

Michel L. Lapidus (University of California, Riverside, USA)

Aims and Scope

The *Journal of Fractal Geometry* is dedicated to publishing high quality contributions to fractal geometry and related subjects, or to mathematics in areas where fractal properties play an important role. The journal accepts submissions of original research articles and short communications, occasionally also research expository or survey articles, representing substantial advances in the field.



ISSN print 1663-487X
ISSN online 1664-073X
2016. Vol. 7. 4 issues
Approx. 600 pages. 17.0 x 24.0 cm
Price of subscription:
218 € online only
268 € print+online

Editor-in-Chief:

Vladimir Turaev (Indiana University, Bloomington, USA)

Aims and Scope

Quantum Topology is dedicated to publishing original research articles, short communications, and surveys in quantum topology and related areas of mathematics. Topics covered include: low-dimensional topology; knot theory; Jones polynomial and Khovanov homology; topological quantum field theory; quantum groups and hopf algebras; mapping class groups and Teichmüller space categorification; braid groups and braided categories; fusion categories; subfactors and planar algebras; contact and symplectic topology; topological methods in physics.

Editorial Team

Editor-in-Chief

Lucia Di Vizio

LMV, UVSQ
45 avenue des États-Unis
78035 Versailles cedex, France
e-mail: divizio@math.cnrs.fr

Copy Editor

Chris Nunn

119 St Michaels Road,
Aldershot, GU12 4JW, UK
e-mail: nunn2quick@gmail.com

Editors

Ramla Abdellatif

LAMFA – UPJV
80039 Amiens Cedex 1, France
e-mail: Ramla.Abdellatif@u-picardie.fr

Jean-Paul Allouche

(Book Reviews)
IMJ-PRG, UPMC
4, Place Jussieu, Case 247
75252 Paris Cedex 05, France
e-mail: jean-paul.allouche@imj-prg.fr

Jorge Buescu

(Societies)
Dep. Matemática, Faculdade
de Ciências, Edifício C6,
Piso 2 Campo Grande
1749-006 Lisboa, Portugal
e-mail: jbuescu@ptmat.fc.ul.pt

Jean-Luc Dorier

(Math. Education)
FPSE – Université de Genève
Bd du pont d'Arve, 40
1211 Genève 4, Switzerland
Jean-Luc.Dorier@unige.ch

Javier Fresán

(Young Mathematicians' Column)
Departement Mathematik
ETH Zürich
8092 Zürich, Switzerland
e-mail: javier.fresan@math.ethz.ch

Vladimir R. Kostic

(Social Media)
Department of Mathematics
and Informatics
University of Novi Sad
21000 Novi Sad, Serbia
e-mail: vladimir.slk@gmail.com



Scan the QR code to go to the
Newsletter web page:
<http://euro-math-soc.eu/newsletter>

Eva Miranda

(Research Centres)
Department of Mathematics
EPSEB, Edifici P
Universitat Politècnica
de Catalunya
Av. del Dr Marañón 44–50
08028 Barcelona, Spain
e-mail: eva.miranda@upc.edu

Vladimir L. Popov

Steklov Mathematical Institute
Russian Academy of Sciences
Gubkina 8
119991 Moscow, Russia
e-mail: popovvl@mi.ras.ru

Themistocles M. Rassias

(Problem Corner)
Department of Mathematics
National Technical University
of Athens, Zografou Campus
GR-15780 Athens, Greece
e-mail: trassias@math.ntua.gr

Volker R. Remmert

(History of Mathematics)
IZWT, Wuppertal University
D-42119 Wuppertal, Germany
e-mail: remmert@uni-wuppertal.de

Vladimir Salnikov

University of Luxembourg
Mathematics Research Unit
Campus Kirchberg
6, rue Richard Coudenhove-
Kalergi
L-1359 Luxembourg
vladimir.salnikov@uni.lu

Dierk Schleicher

Research I
Jacobs University Bremen
Postfach 750 561
28725 Bremen, Germany
dierk@jacobs-university.de

Olaf Teschke

(Zentralblatt Column)
FIZ Karlsruhe
Franklinstraße 11
10587 Berlin, Germany
e-mail: olaf.teschke@fiz-karlsruhe.de

Jaap Top

University of Groningen
Department of Mathematics
P.O. Box 407
9700 AK Groningen,
The Netherlands
e-mail: j.top@rug.nl

Valentin Zagrebnoy

Institut de Mathématiques de
Marseille (UMR 7373) – CMI
Technopôle Château-Gombert
39, rue F. Joliot Curie
13453 Marseille Cedex 13,
France
e-mail: Valentin.Zagrebnoy@univ-amu.fr

European Mathematical Society

Newsletter No. 100, June 2016

Editorial: Approaching a High Point in the Life of the EMS –

<i>P. Exner</i>	3
The EMS Ethics Committee: Work and Perspectives – <i>A. Quirós</i>	4
Encyclopedia of Mathematics – <i>U. Rehmann</i>	5
Sophie Germain on a French Stamp – <i>E. Strickland</i>	8
Twenty-Five Years: Looking Back and Ahead – <i>P. Exner</i>	10
Profinite Number Theory – <i>H. Lenstra</i>	14
Exchangeability, Chaos and Dissipation in Large Systems of Particles – <i>L. Saint-Raymond</i>	19
Panel: Challenges for Mathematicians	25
Bitcoin and Decentralised Trust Protocols – <i>R. Pérez-Marco</i>	31
A Tribute to Abbas Bahri – <i>M. Ahmedou et al.</i>	39
Beppo Levi's Mathematics Papers Return to Italy – <i>M. Mattaliano</i> ..	45
Historical Archive of the Istituto per le Applicazioni del Calcolo – <i>M. Mattaliano</i>	49
University Goes to School – <i>V. Salnikov</i>	51
The ETH Math Youth Academy – <i>K. Slavov</i>	51
Activities at the University of Geneva – <i>E. Raphael</i>	52
Nesin Mathematics Village – <i>S. Durhan</i>	54
ICMI Column – <i>G. Kaiser</i>	56
ERME Column – <i>T. Dooley & G. Gueudet</i>	57
Another Update on the Collaboration Graph – <i>M. Jost</i> , <i>N. D. Roy & O. Teschke</i>	58
Book Reviews	61
Letters to the Editor	64
Personal Column	64

The views expressed in this Newsletter are those of the authors and do not necessarily represent those of the EMS or the Editorial Team.

ISSN 1027-488X

© 2016 European Mathematical Society

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

President

Prof. Pavel Exner

(2015–2018)
Doppler Institute
Czech Technical University
Břehová 7
CZ-11519 Prague 1
Czech Republic
e-mail: ems@ujf.cas.cz

Vice-Presidents

Prof. Franco Brezzi

(2013–2016)
Istituto di Matematica Applicata
e Tecnologie Informatiche del
C.N.R.
via Ferrata 3
I-27100 Pavia
Italy
e-mail: brezzi@imati.cnr.it

Prof. Martin Raussen

(2013–2016)
Department of Mathematical
Sciences
Aalborg University
Fredrik Bajers Vej 7G
DK-9220 Aalborg Øst
Denmark
e-mail: raussen@math.aau.dk

Secretary

Prof. Sjoerd Verduyn Lunel

(2015–2018)
Department of Mathematics
Utrecht University
Budapestlaan 6
NL-3584 CD Utrecht
The Netherlands
e-mail: s.m.verduynlunel@uu.nl

Treasurer

Prof. Mats Gyllenberg

(2015–2018)
Department of Mathematics
and Statistics
University of Helsinki
P.O. Box 68
FIN-00014 University of Helsinki
Finland
e-mail: mats.gyllenberg@helsinki.fi

Ordinary Members

Prof. Alice Fialowski

(2013–2016)
Institute of Mathematics
Eötvös Loránd University
Pázmány Péter sétány 1/C
H-1117 Budapest
Hungary
e-mail: fialowsk@cs.elte.hu

Prof. Gert-Martin Greuel

(2013–2016)
Department of Mathematics
University of Kaiserslautern
Erwin-Schroedinger Str.
D-67663 Kaiserslautern
Germany
e-mail: greuel@mathematik.uni-kl.de

Prof. Laurence Halpern

(2013–2016)
Laboratoire Analyse, Géométrie
& Applications
UMR 7539 CNRS
Université Paris 13
F-93430 Villetaneuse
France
e-mail: halpern@math.univ-paris13.fr

Prof. Volker Mehrmann

(2011–2018)
Institut für Mathematik
TU Berlin MA 4–5
Strasse des 17. Juni 136
D-10623 Berlin
Germany
e-mail: mehrmann@math.TU-Berlin.DE

Prof. Armen Sergeev

(2013–2016)
Steklov Mathematical Institute
Russian Academy of Sciences
Gubkina str. 8
119991 Moscow
Russia
e-mail: sergeev@mi.ras.ru

EMS Secretariat

Ms Elvira Hyvönen and Ms Erica Runolinna

Department of Mathematics
and Statistics
P.O. Box 68
(Gustaf Hällströmin katu 2b)
FIN-00014 University of Helsinki
Finland
Tel: (+358)-9-191 51503
Fax: (+358)-9-191 51400
e-mail: ems-office@helsinki.fi
Web site: <http://www.euro-math-soc.eu>

EMS Publicity Officer

Dr. Richard H. Elwes

School of Mathematics
University of Leeds
Leeds, LS2 9JT
UK
e-mail: R.H.Elwes@leeds.ac.uk

EMS Agenda

2016

16–17 July

EMS Council, Humboldt University, Berlin, Germany

EMS Scientific Events

2016

4–9 July

Building Bridges: 3rd EU/US Summer School on Automorphic
Forms and Related Topics
Sarajevo, Bosnia and Herzegovina

11–15 July

EMS-IAMP Summer School in Mathematical Physics on
“Universality, Scaling Limits and Effective Theories”
Roma, Italy
<http://www.smp2016.cond-math.it/>

11–15 July

14th Workshop on Interactions between Dynamical Systems
and Partial Differential Equations (JISD 2016)
Universitat Politècnica de Catalunya, Spain

11–15 July

V Congreso Latinoamericano de Matemáticos
Barranquilla, Colombia
EMS speaker: Ulrike Tillmann

18–22 July

7th European Congress of Mathematics, Berlin, Germany
<http://www.7ecm.de/>

25–29 July

EMS-ESMTB Summer School “Mathematical Modelling of
Tissue Mechanics”
Leiden, The Netherlands

17–24 August

European Summer School in Multigraded Algebra and
Applications
Constanta, Romania

21–28 August

EMS-ESMTB Summer School “The Helsinki Summer School
on Mathematical Ecology and Evolution 2016: Structured
Populations”
Linnasmäki Congress Centre, Turku, Finland

25–26 August

Second Caucasian Mathematics Conference (CMC-II)
Lake Van, Turkey

25 September–1 October

50th Seminar Sophus Lie
Banach Conference Center, Bedlewo
Distinguished EMS Lecturer: Ernest Vinberg
<http://50sls.impan.pl>

2017

24–28 July

31st European Meeting of Statisticians
Helsinki
EMS-Bernoulli Society Joint Lecture: Alexander Holevo

Editorial: Approaching a High Point in the Life of the EMS

Pavel Exner (Czech Technical University, Prague, Czech Republic), President of the EMS

It seems that the founders of our society were fans of even numbers when they decided that its life would follow two- and four-year cycles. Now, we are again approaching the moment when the two periods meet and this is being marked by two important events: the European Mathematical Congress and the EMS Council, both of them convening in the days when this issue of the newsletter will reach your hands.

The congress is the opportunity to demonstrate recent achievements in Europe in all directions of mathematics and also to communicate with colleagues beyond our usual disciplinary borders, seeking inspirations for new endeavours. It is also traditionally the moment to distinguish those among us, especially the young, who have enriched mathematics with new remarkable results. The EMS Prizes have achieved significant renown, illustrated by the “one-in-six” rule: 10 out of the existing 60 prize winners have subsequently been awarded the Fields Medal. We can only hope that this trend will continue.

There is much more in the congress programme: Hirzebruch and Abel Lectures, panel discussions, a Women in Mathematics event and a lecture for high school students, to name just a few. One should also not forget lectures reflecting the *genius loci* of the congress site; there is no need to stress the important role Berlin has played many times in the history of mathematics.

As usual, the congress will be preceded by the meeting of the EMS Council, the society’s highest democratic authority. The council has to take some important decisions, including the approval of the EMS budget and the work of the EMS Executive Committee and its 11 committees, which deal with all the aspects of a mathematician’s life. The Executive Committee also has to be renewed, as some of its members will be finishing their terms; in particular, the council will have to elect two new vice-presidents. Another important decision concerns the site of the next congress in 2020. Two bids have been made by Portorož (Slovenia) and Sevilla (Spain). The Executive Committee is convinced that both are well prepared and the council delegates will have a difficult decision to make.

Let me return to the budget. While most of our revenue comes from member dues, we appreciate support from other sources. This year, we have received an extraordinarily generous one: the Simons Foundation has

decided to make an annual donation of \$50,000 to the EMS for a period of five years to support mathematics in Africa. We are extremely grateful for this noble deed and our Committee for Developing Countries is working out fellowship schemes to use the money in the most efficient way.

This is not the only good news from the fiscal arena. Thanks to the excellent work of our treasurer, we are running a budget surplus and this has allowed us to support a number of activities this year, including six Summer schools in various areas of mathematics, as well as the Summer school we organise biannually in collaboration with the International Association of Mathematical Physics, a European speaker at the Latin American Congress of Mathematics and other activities.

Let me next mention one more periodic event, this time related to the newsletter. The Editor-in-Chief of the newsletter changes every few years and such a moment has now arrived. Lucia Di Vizio, who has served in this role since 2012, is approaching the end of her term. I am afraid many might not have noticed the extent of her work; if things are running smoothly and you have your interesting reading every quarter of a year, you may not think of the effort that lies behind it. Lucia has led the newsletter Editorial Board with an exceptional commitment and passion and the EMS is deeply indebted to her for all her work in that role. This issue is her last one; from October, her successor Valentin Zagrebnoy from Université Aix-Marseille will take over. We are convinced that he will preserve the present quality and appeal of this journal.

To conclude, a few words about the newsletter itself. The issue you hold in your hands is No. 100. As mathematicians, we know that the exceptionality of the number is only due to the decadic system we use; nevertheless, it is an opportunity to look back at the history. This is now easy thanks to the efforts of Jiří Rákosník and the EMS Publishing House, which has ensured that all the issues are posted on the web at <http://www.euro-math-soc.eu/newsletter>. The panorama that this webpage offers illustrates the progress the newsletter has made under the leadership of Lucia and her predecessors since the first issue, which appeared in September 1991. Looking at it, we move into the second hundred with a well-justified optimism.

The EMS Ethics Committee: Work and Perspectives

Adolfo Quirós (Universidad Autónoma de Madrid, Spain), Chair of the EMS Ethics Committee

In 2010, the Executive Committee of the EMS decided to establish an Ethics Committee, which was to focus on unethical behaviour in mathematical publications. According to the remit prescribed for the committee, “this includes, for example, plagiarism, duplicate publication, inadequate citations, inflated self-citations, dishonest refereeing, and other violations of the professional code”. The first task assigned to the Ethics Committee was to prepare a Code of Practice (CoP). This task was completed in the Spring of 2012; the CoP was approved by the Executive Committee at the end of October and came into effect on 1 November 2012. It can be found on the committee’s webpage (<http://www.euro-math-soc.eu/committee/ethics>).

Many European mathematical societies have now formally adhered to the CoP and others have shown their support of its underlying principles. Likewise, several journals state on their webpages that they adhere to the EMS Code of Practice. We hope that publishers and editors of European journals and monographs in mathematics will conform to the CoP, even if they do not adopt it explicitly.

The Ethics Committee has used the CoP to decide on several cases that have been submitted following the approved procedure, and also to answer a number of questions and informal inquiries. Moreover, as was suggested in the remit received from the Executive Committee, the committee has taken up other relevant questions related to ethics in connection with its work. It should be noted that, beginning in 2014, the committee has gone through the renewal process common to all EMS committees. At this time, only four of the nine original committee members remain.

Since the committee’s first chair, Arne Jensen, has already reported on the preliminary work (EMS Newsletter 80, June 2011) and on the CoP itself (EMS Newsletter 87, March 2013), we will concentrate on reviewing some of the ethical problems we have addressed up to now and the new tasks we will have to confront.

Cases

The number of cases formally brought in front of the committee is not huge: three to four cases per year. This may be because of good reasons: unethical behaviour is rare in mathematics (we of course know most mathematicians behave properly) and/or when a potential problem appears, it is solved through direct interaction or by following the procedures set up by journals. But it may also be that the CoP, and the committee itself, are not sufficiently known or that people who might present a complaint think that the committee does not have the power to address it the way they would like. In this respect, it should be clear that the committee is certainly not a judiciary and we hope to

solve most of the cases through mediation. However, as stated in the CoP, the committee may make a formal submission to the President of the EMS in cases where it is convinced that unethical behaviour has occurred.

We are, in general, happy with the way cases have been resolved. As we expected, most of them concerned plagiarism. However, there have also been allegations of dishonest refereeing, improper handling of papers by editors and refusal to publish corrections.

Not all plagiarism is of the same sort and it is not always easy to distinguish between plagiarism, improper attribution and results that people doing research in a field can easily discover simultaneously. We ask for expert advice to elucidate such cases.

But then there is blatant plagiarism, where somebody copies verbatim other people’s work, sometimes even whole articles (except for the title). One may wonder how this can escape the referee’s and the editor’s scrutiny. In most of the cases we have seen, the explanation is simple: the paper had been published in so called “predatory journals”, where the only thing that matters is paying the publication fee. The offending “authors” have usually apologised but getting an answer from the “editors” has proven impossible.

Some general issues the committee has considered

The first ethical issue the committee addressed in some generality was precisely those predatory journals. Hopefully, most mathematicians will not take seriously alleged research published this way but it creates confusion and might be very damaging for those less experienced. The CoP states that any person listed as editor or editorial advisor should be aware of, and content with, the standards and editorial procedures and policies of the journal but we wonder if people always know that they “are” editors. We do not think the committee should ask such questions directly but if you find out that a colleague appears on the editorial board of a suspicious journal, maybe you could talk about this.

Another relevant issue is self-plagiarism, which is not always easy to spot because there is no “plagiarised author” who will complain. Besides the classical “recycling beyond reason” of previous results, the information we receive seems to indicate that the number of simultaneous submissions of the same research has increased and is taking bold new forms: one of the EMS member societies has recently told us of a paper already published in its journal being submitted to another journal and also (this is not a joke, although it is certainly ridiculous) of a rejected paper being submitted again, under a different title and with a

slightly different set of authors, to the same journal that rejected it! The offending authors have been banned from publishing in these journals in the future.

Plagiarising is of course much easier in this electronic age and creating lists of “suspicious” or “banned authors” is one of the tools used by journals and publishers to combat it. Enquiries have been made to the committee regarding how to use such lists. (Can they be shared? Is it reasonable to also create lists of “suspicious institutions”, i.e. those that fail to react when their employees misbehave?) Although we do not have all the answers, we think banning authors that have acted unethically helps uphold ethical standards but lists should be handled with extreme care.

Perspectives for future work

We believe ethics is not an abstract idea. In the future, we would like to work together with other EMS committees, such as Publications or Electronic Publishing, to address, for example, potential ethical issues in Open Access or problems arising from the misuse of bibliometric data.

In view of these new developments and of the experience gained by the committee, the CoP will at some point need to be revised. We think, however, that it would be premature to do it now. In the meantime, we have written some “Comments on the EMS Code of Practice”, which we expect will help in understanding the CoP objectives and how it is being applied. The document is available at the committee’s webpage and we welcome suggestions, both on the comments and on the CoP itself.

Last but not least, the committee has now taken up another relevant question related to ethics: conflicts of interest. The Executive Committee of the EMS is concerned about this issue, in particular in Scientific and Prize Committees, and has asked the Ethics Committee to prepare a document that will address conflicts of interest in the selection of people for prizes, grants, invited talks, etc. We expect to finish work on it in a reasonable amount of time.

EMS Ethics Committee Members for 2016

Adolfo Quirós (Universidad Autónoma de Madrid, Spain), *Chair*

Garth Dales (University of Lancaster, UK), *Vice-Chair*

Members:

Zbigniew Błocki (Uniwersytet Jagielloński w Krakowie, Poland)

Arne Jensen (Aalborg Universitet, Denmark)

Edita Pelantová (České vysoké učení technické v Praze, Czech Republic)

Norbert Schappacher (Université de Strasbourg, France)

Tatyana Shaposhnikova (Kungliga Tekniska Högskolan, Stockholm, Sweden)

Betül Tanbay (Boğaziçi Üniversitesi, Istanbul, Turkey)

Dirk Werner (Freie Universität Berlin, Germany)

Executive Committee representative:

Franco Brezzi (Istituto di Matematica Applicata e Tecnologie Informatiche del C.N.R., Pavia, Italy)



Adolfo Quirós has been the Chair of the EMS Ethics Committee since January 2016. He obtained his PhD from the University of Minnesota and is Profesor Titular at the Department of Mathematics of Universidad Autónoma de Madrid (Spain). His area of research is Arithmetic Algebraic Geometry and he is also involved in popularization activities, like the Mathematical Challenges run by the Spanish daily El País, which he coordinates and sometimes presents (on video). He has been Vice-president of Real Sociedad Matemática Española and is currently editor of its members’ journal, La Gaceta.

Encyclopedia of Mathematics – Now Enhanced by StatProb

Another Invitation for Cooperation

Ulf Rehmann (Universität Bielefeld, Germany), Editor-in-Chief of the Encyclopedia of Mathematics

A few years ago, a report was made on the Encyclopedia of Mathematics (EoM) (see https://www.encyclopediaofmath.org/index.php/Main_Page), which has now mutated, under EMS and Springer support, from a heavy, printed set of volumes into a Wikipedia-like endeavour, with more than 8,000 encyclopedic articles on all fields of mathematics, ready not only for free read access for the scientific and public community but also for further up-

dates and enhancements by knowledgeable authors, i.e. by you and your working group!

Recently, the EoM has been enlarged by the StatProb online collection, an interesting ensemble of encyclopedic articles collated by a collaboration of 10 international statistics and probability societies and called “StatProb – The Encyclopedia Sponsored by Statistics and Probability Societies” (formerly accessible at <http://statprob>).

com/encyclopedia/). These pages have been donated by their authors to the Encyclopedia of Mathematics and are now maintained within the framework of the EoM. This newly incorporated collection can now, as a whole, be found at <https://www.encyclopediaofmath.org/index.php/Category:Statprob>.

The EoM itself has a long history, as was noted in the previous newsletter article. The basis is the material from the classical *Encyclopaedia of Mathematics* (note the slight spelling difference!), which was published from 1985 to 2001 in print by Reidel and Kluwer Academic Publishers and since 2003 by Springer in a 10 volume set (together with three supplements). The *Encyclopaedia of Mathematics* itself was an updated and annotated translation of the five volume *Soviet Mathematical Encyclopaedia* (Matematicheskaya Entsiklopediya), which was edited by I.M. Vinogradov, V.I. Bitjuckov and Ju.V. Prohorov and published from 1977 to 1985. In 1997, an electronic version was produced and distributed on CDROM. Later, the CDROM material was also freely accessible on the web.

Some time ago, Springer approached the EMS and proposed a collaboration: under the condition that the EMS would organise the subsequent editions of the Encyclopedia, Springer would donate the content of the *Encyclopaedia* to the public as foundational material and provide and maintain a server equipped with “MediaWiki” software in order to allow its further dynamic development under the standard Wikipedia licence (the so-called “Creative Commons Attribution Share-Alike License”) or the alternative and essentially equivalent “GNU Free Documentation License”.

The EMS considers this encyclopedic corpus to be a rich mathematical heritage that deserves maintenance and further development and therefore established an editorial board to monitor any changes to articles, with full scientific authority over alterations and deletions. Of course, there are already a surprisingly large number of well written Wikipedia (WP) articles in mathematics, so one could ask why there should be another such attempt. However, the Encyclopedia of Mathematics is mainly aimed at professional mathematicians and includes pretty technical articles, whilst the Wikipedia articles are mainly aimed at the general public. The EoM and Wikipedia are also grounded on different editorial principles. While Wikipedia insists that its references are (kind of) original sources and therefore does not allow references to itself, the EoM, as a scientific publication endeavour, is an original source. There are many WP references to the EoM!

The EoM is also, in contrast to general WP pages, based on the MathJax software (see <http://www.mathjax.org/>), which allows content in arbitrary T_EX or L^AT_EX format and which makes the writing and editing of articles much easier for the professional mathematician. So, rather than, for example, encoding Euler’s formula using the less convenient WikiPedian tagged style $\langle \text{math} \rangle e^{2\pi i} - 1 = 0 \langle / \text{math} \rangle$, standard tex encoding can be used instead like $\$e^{2\pi i} - 1 = 0\$$, which allows the simple copying and pasting of formulas from T_EX manuscripts that already exist. The MathJax software allows smooth representation of even pretty complicated formulas and is therefore of great interest for the representation of mathematics on webpages. For example, the recently integrated StatProb articles consist of a set of T_EX files, which were smoothly converted to the EoM web format.

Another interesting piece of software used on the EoM pages is “Asymptote”, which allows the integration of well-formed graphics into the EoM pages. The EoM also has equipment to classify its material under 2010 MSC and to smoothly handle references, together with their links to MathSciNet and Zentralblatt.

If you are working in a field that you feel deserves more attention in the professional environment, because its development, for example, has been so substantial and rapid over the last 20–30 years, then you should consider either enlarging existing articles or even creating corresponding new ones about your field in the EoM, in order to make the important major achievements available to a broader community. In fact, if you are leading a research group, you could direct your students – under your guidance – to extend and write such articles in the framework of academic research seminars, for example, or as part of Master’s or PhD programmes.

You are cordially invited to have a look at this representative compendium of mathematics and consider contributing to its further development..



Ulf Rehmann is a retired professor of mathematics at Bielefeld University. He is an algebraist with an interest in linear algebraic groups and related structures like quadratic forms, Azumaya algebras, Brauer groups, etc. His editorial activities are in scientific electronic publishing and retro-digitisation.

He is a founding editor of Documenta Mathematica, Editor-in-Chief of the Encyclopedia of Mathematics and an editor of the retro-digitised versions of the ICM proceedings.

W. K. Clifford Prize 2017 – Call for Nominations

The W.K. Clifford Prize is an international scientific prize for young researchers, which intends to encourage them to compete for excellence in theoretical and applied Clifford algebras, their analysis and geometry. The award consists of a written certificate, one year of online access to Clifford algebra related journals, a book token worth €150 and a cash award of €1000. The laureate is also offered the opportunity to give the special *W.K. Clifford Prize Lecture* at University College London, where W.K. Clifford held the first Goldsmid Chair from 1871 until his untimely death in 1879.

The next W.K. Clifford Prize will be awarded at the *11th Conference on Clifford Algebras and Their Applications in Mathematical Physics (ICCA10)* in Ghent (Belgium) in 2017.

The deadline for nominations is 30 September 2016. Nominations should be sent to secretary@wkcliffordprize.org. For details, see <http://www.wkcliffordprize.org>.

Annales de l'Institut Fourier: Now Open Access

Hervé Pajot (Université Grenoble Alpes, St Martin d'Hères, France)

The *Annales de l'Institut Fourier* (AIF) were created in 1949. They form an academic, international journal of fundamental mathematics, managed by the Fourier Institute in Grenoble (France). Among the members of its editorial board are two recipients of the Fields Medal (Maryam Mirzakhani and Stanislav Smirnov).

Since 2015, the electronic version of the AIF has been open access (and there is no charge for authors!). This evolution was possible with the help of two national structures: Mathdoc and Mathrice (depending on the CNRS, the French centre for scientific activities). Like AIF, all French journals (if they want) can now benefit from the following services: installation and housing of the editorial software OJS (Mathrice), maintenance and skills with these tools, LaTeX typesetting, and production and distribution of the installations (Mathdoc, Cedram service). It is expected that most French academic journals will follow the lead of the AIF, in particular those that are now distributed by commercial publishing houses.

The Ferran Sunyer i Balaguer Prize 2016

The Ferran Sunyer i Balaguer Prize 2016 winners were:

Vladimir Turaev (Indiana University), and
Alexis Virelizier (Université de Lille 1), for the work

Monoidal Categories and Topological Field Theory

Abstract: The monograph consists of four parts. Part 1 offers an introduction to monoidal categories and to Penrose's graphical calculus. Part 2 is devoted to an algebraic description of the center of monoidal categories based on the theory of Hopf monads as developed by Virelizier with other coauthors. Part 3 explains topological quantum field theories, including fundamental earlier work of Reshetikhin-Turaev and Turaev-Viro. In part 4 the authors show how to present ribbon graphs by diagrams on skeletons of 3-manifolds and define graph topological quantum field theories by means of state sums on such skeletons. Their main result interprets such graph theories as surgery theories, thereby proving a conjecture stated by Turaev in 1995.

This monograph will be published by Springer Basel in their Birkhäuser series *Progress in Mathematics*.

fundació FERRAN SUNYER I BALAGUER
Institut d'Estudis Catalans



Call for the **Ferran Sunyer i Balaguer Prize 2017**

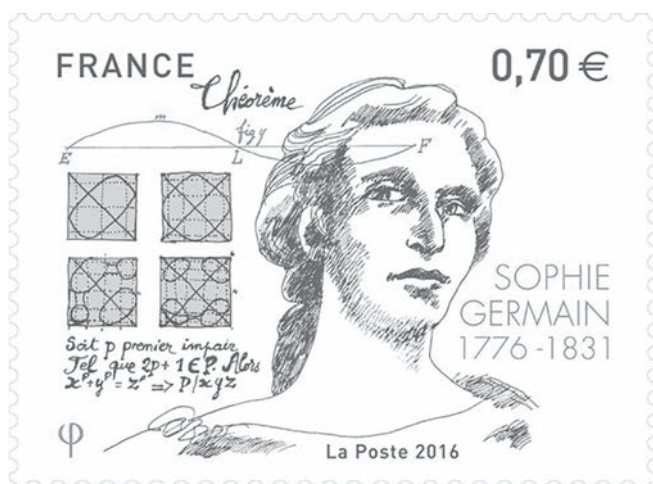
The prize will be awarded for a **mathematical monograph** of an expository nature presenting the latest developments in an active area of research in mathematics.

The prize consists of **15,000 Euros** and the winning monograph will be published in Springer Basel's **Birkhäuser** series "Progress in Mathematics".

**DEADLINE FOR SUBMISSION:
1 December 2016**
<http://ffsb.iec.cat>

Sophie Germain on a French Stamp

Elisabetta Strickland (University of Rome "Tor Vergata", Rome, Italy), EMS-WIM Committee



A stamp in honour of Sophie Germain has been available in France since 18 March and a ceremony was organised for the event by the Institut Henri Poincaré. Since her death in 1831, Sophie Germain has been honoured in several ways. A street, Rue Sophie Germain, has been named in her honour and a statue of her stands in the courtyard of the École Sophie Germain in Paris.

Germain was a revolutionary. She battled against the social prejudices of her era and a lack of formal training in order to become a celebrated mathematician. She was born in Paris on 1 April 1776, so she was 13 when the Bastille fell. As the turmoil in Paris made it impossible for her to spend time outside the house, she turned to her father's library. In a book of Jean-Étienne Montucla, *Histoire des Mathématiques*, she read an account of the death of Archimedes at the hands of a Roman soldier, while he was totally absorbed with a problem of geometry. Germain decided that if mathematics had held such fascination for Archimedes, it was a subject worthy of study. Her family didn't approve of her attraction to mathematics and, when night came, they would deny her warm clothes and proper lighting in her bedroom. She waited until they went to sleep and then took out candles, wrapped herself in blankets and worked until dawn. One morning, Germain was found asleep on her desk, the ink frozen in the inkwell; this made them realise that she had to be free to study mathematics.

In 1794, when she was 18, the École Polytechnique opened but, as a woman, Germain was not permitted to

attend. She managed to obtain the lecture notes of Lagrange, who was a faculty member, and started to send him her work using the pseudonym M. Le Blanc. Lagrange recognised the quality of her mathematics and was determined to meet M. Le Blanc so Germain was forced to disclose her true identity. Lagrange didn't mind that Germain was a woman and guided her research.

Initially, Germain had a deep interest in number theory and, again under the pseudonym of M. Le Blanc, she wrote to Carl Friedrich Gauss, presenting some of her considerations on *Fermat's Last Theorem*. Gauss thought well of Germain, even after he discovered that she was a woman, but he did not generally review her work, so the correspondence eventually ended without the two ever meeting.

In 1811, Germain participated in a competition sponsored by the Académie des Science in Paris concerning the experiments of the physicist Ernst Chladni on vibrating plates. She was the only entrant in the contest. The object of the competition was to give a mathematical theory for the vibrations of an elastic surface. She didn't succeed the first time because the jury said the equations were not established but she tried again and, at the third attempt, in 1816, she won the prize, allowing her to develop a reputation on a par with Cauchy, Ampere, Navier, Poisson and Fourier.

But Germain's best work was in number theory, where she made a significant contribution to *Fermat's Last Theorem*. She wrote again to Gauss to ask his opinion on her proof for a special case but Gauss again didn't answer. As we know, Andrew Wiles solved the problem in 1994 but Germain's work 200 years before is considered substantial.

Finally, Gauss did his best to convince the University of Göttingen to confer a doctor's degree *honoris causa* on Germain but she never had the chance to receive it because she died of breast cancer in 1831. When the state official who had to fill out her death certificate came to her house, he refused to write *mathematician* for her profession, writing *property owner* instead. Moreover, when the Eiffel Tower was erected and it was decided to inscribe on it the names of the 72 scientists whose work on elasticity had contributed to the enterprise, Germain's name was left out, perhaps because she was a woman. Today, however, Germain is considered one of the founders of mathematical physics.

EMS Monograph Award

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”.

The second EMS Monograph Award (2016) has been assigned jointly to

Yves de Cornulier (Université Paris-Sud, Orsay, France) and **Pierre de la Harpe** (Université de Genève, Switzerland) for their work

Metric Geometry of Locally Compact Groups

and

Vincent Guedj and **Ahmed Zeriahi** (both Université de Toulouse, France) for their work

Degenerate Complex Monge-Ampère equations

Scientific Committee

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

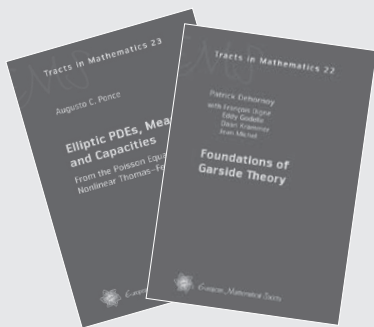
Submission

The third award will be announced in 2018, the deadline for submissions is 30 June 2017.

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. Monographs should preferably be typeset in TeX. Authors should send a pdf file of the manuscript by email to

info@ems-ph.org.

EMS Tracts in Mathematics



Editorial Board:

Carlos E. Kenig (University of Chicago, USA)
 Michael Farber (Queen Mary University of London, 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. 24 Hans Triebel: *Hybrid Function Spaces, Heat and Navier-Stokes Equations*
 978-3-03719-150-7. 2015. 196 pages. 48.00 Euro

Winner of the 2014 EMS Monograph Award:

Vol. 23 Augusto C. Ponce: *Elliptic PDEs, Measures and Capacities. From the Poisson Equation to Nonlinear Thomas–Fermi Problems*
 ISBN 978-3-03719-140-8. 2017. Approx. 350 pages. 58.00 Euro (to appear)

Winner of the 2014 EMS Monograph Award:

Vol. 22 Patrick Dehornoy with François Digne, Eddy Godelle, Daan Krammer and Jean Michel: *Foundations of Garside Theory*
 978-3-03719-139-2. 2015. 710 pages. 108.00 Euro

Vol. 21 Kaspar Nipp and Daniel Stoffer: *Invariant Manifolds in Discrete and Continuous Dynamical Systems*
 978-3-03719-124-8. 2013. 225 pages. 58.00 Euro

25th Anniversary of the EMS

To mark the 25th anniversary of the European Mathematical Society, a one day event with the title “Challenges for the next 25 years” was held at the Institut Henri Poincaré in Paris, 22 October 2015 (see the Editorial by Richard Elwes in Newsletter No. 99 for a report). The President Pavel Exner opened the meeting with a speech that is summarised below. Lectures with mathematical topics were given by Hendrik Lenstra (Leiden, the Netherlands), Laure Saint-Raymond (ENS Paris, France), László Lovász (Budapest, Hungary) and Andrew Stuart (Warwick, UK). A panel moderated by

the ERC President J.P. Bourguignon discussed specific challenges for the mathematical sciences. The panel consisted of ICIAM President Maria Esteban, Director of the Institut Mittag-Leffler and previous EMS President Ari Laptev, Peter Bühlmann (ETH Zürich, representing the Bernoulli Society) and Roberto Natalini (Istituto per le Applicazioni del Calcolo, Rome, and Chairman of the EMS Committee Raising the Public Awareness of Mathematics).

You will find below a written account of some of the talks and speeches that were given.

Twenty-Five Years: Looking Back and Ahead

Pavel Exner (Czech Technical University, Prague, Czech Republic), President of the EMS

This article summarises a presentation given at the opening of the October 2015 meeting at the Institut Henri Poincaré in Paris celebrating the 25th anniversary of the EMS.

Since last September, the newsletter has published a number of articles dedicated to the anniversary of the European Mathematical Society. The celebration culminated in a one-day meeting at the Institut Henri Poincaré in Paris on 22 October, almost 25 years to the day since the meeting in Mądralin where the foundations were laid. It was only natural to open the meeting with a ‘state of the union’ address and it was my duty and honour to present it. With pleasure, I accept the invitation of the newsletter to summarise the contents of that address for the readers of this issue.

The roots

A question about what brought the participants of the Paris meeting together is, of course, rhetorical only, but there is no harm in putting the gathering into the proper context, if not for any other reason than because the roots of the *European Mathematical Society* reach far into history. Mathematics has flourished in Europe for more than two millennia. In fact, with all due respect to other continents, the main body of the science we call mathematics today was formed in Europe. If this claim needs any proof, it is enough to start listing names: for instance, Pythagoras, Euclides, Archimedes, Diophantus, Fibonacci, Descartes, Newton, Leibnitz, Fermat, Pascal, Euler, Laplace, Lagrange, Gauss, Abel, Galois, Hamilton,

Riemann, Klein, Poincaré, Hilbert – each of you can keep on reciting scores of others.

Exchange of ideas is the soil on which science grows. Academies in which scientists meet have a long tradition that can be traced back to Ancient Greece. In Europe, they have started flourishing again since the Renaissance period. As the numbers of working mathematicians grew, they began to organise societies with purely or dominantly a mathematical focus. Among the early societies, one could mention:

- Amsterdam’s Koninklijk Wiskundig Genootschap (1778).
- Union of Czech Mathematicians and Physicists (1862).
- Moscow Mathematical Society (1864).
- London Mathematical Society (1865).

Then, the flood-gates opened and many others followed: through most of the 20th century, almost all European countries had mathematical societies, and some had two, three or even more.

Pains of childbearing

The growing sense of European identity inspired efforts to create a society representing all European mathematicians. The original impetus came in 1976 from the European Science Foundation and led to establishing, at the ICM in Helsinki in 1978, the *European Mathematical Council*, led by Sir Michael Atiyah, who can rightly be regarded as the ‘zeroth president’ of the EMS.

However, one should never expect fast solutions when mathematicians decide to solve a problem, to say nothing of the fact that the general situation in the European scene in the 1980s was far from simple. The next meeting at the ICM in Warsaw was delayed for well known political reasons and it was followed by meetings in Prague (1986) and Oberwolfach (1988), trying to draft the prospective society's statutes. After the political earthquake at the end of the 1980s, the feeling of urgency grew stronger and led finally to the decisive meeting in the Polish town of Mađralin, where representatives of 28 societies met in October 1990.

I am not going to include many pictures in this written version of my Paris presentation but the one which should not be missed shows participants of this founding meeting, with Sir Michael in the centre of the front row.



The Moirai at the EMS cradle.

What was agreed in Mađralin

The main dispute concerned the form of the society to be constituted. Two different concepts competed. Most participants wanted a federation of national societies, while a minority, headed by the French, advocated a society with individual membership. Complicated negotiations led finally to a compromise, because of which the European Mathematical Society has a combined architecture with both *individual* and *corporate members*, the latter being mostly national mathematical societies but also research institutes and other bodies. In a sense, the EMS is thus *a new building made of old bricks*.

The Mađralin meeting chose Helsinki as the legal seat of the EMS and we cannot be grateful enough to our Finnish colleagues, who provided us for a quarter of a century with a reliable administrative base. It also approved the statutes by which the society is governed by the *Council*. The council is elected by all the members and meets every two years, while the day-to-day work is steered by the *Executive Committee*. The meeting also elected *Friedrich Hirzebruch* as the first EMS President; he was followed by an array of prominent mathematicians:

- Friedrich Hirzebruch (1990–1994).
- Jean-Pierre Bourguignon (1995–1998).
- Rolf Jeltsch (1999–2002).
- John Kingman (2003–2006).

- Ari Laptev (2007–2010).
- Marta Sanz-Solé (2011–2014).

Many other distinguished mathematicians have served the society over the 25 years as officers, as committee members and in other roles.

Where we are now

Along the way from the modest beginnings in Mađralin, a lot has been achieved in the quarter of a century that has passed. It is not my aim here, however, to describe the EMS evolution from its birth; rather, I want to present the society's history from the point of view of its present state, as well as the challenges that lie ahead. An interested reader can follow the growth of the EMS step-by-step through the recollections of various important players that have been published in the newsletter recently.

As a brief summary, the European Mathematical Society currently represents:

- About *60 member societies* (55 are full members, two are associate members and three are reciprocal members, with one new application), up from 28 at the beginning, and *2459 individual members* (recall that by a Mađralin agreement we are bound to reconsider the society's architecture at 3000).
- *Twenty-six mathematical research centres* (more than any other continent) and 15 other institutional members, such as mathematics departments and other scientific organisations.
- Eleven permanent *committees* dealing with various aspects of a mathematician's life.
- Quadrennial *congresses* interlacing with the ICM.
- Coveted *EMS Prizes* regarded as a staple of quality.
- Journals and books from our *Publishing House*.

There are also numerous other activities of which we will speak more later.

Congresses and prizes

To have a *European Congress of Mathematics* every four years was one of the first decisions and today one can safely speak of an established tradition. They typically attract around 1000 people and so far they have taken place in:

- Paris, *1ECM*, 6–10 July 1992.
- Budapest, *2ECM*, 22–26 July 1996.
- Barcelona, *3ECM*, 10–14 July 2000.
- Stockholm, *4ECM*, 27 June–July 2004.
- Amsterdam, *5ECM*, 14–18 July 2008.
- Kraków, *6ECM*, 2–7 July 2012.

The forthcoming 7th congress convenes at *TU Berlin*, 18–22 July 2016 (see <http://www.7ecm.de/>) and we await it with great expectations. For the next congress in 2020, bids have been obtained from the universities of *Sevilla* (Spain) and *Primorska* (Slovenia). The decision will be taken at the council meeting prior to 7ECM.

Another initial decision was to award 10 *EMS Prizes* at each congress to the best mathematicians under the age of 35. The renown these prizes have achieved over a quarter of a century is seen from what one could call the *one-in-six rule*: of the 60 laureates so far, 10 subsequently received the Fields Medal, specifically:

- Richard Borcheres, 1992/1998.
- Maxim Kontsevich, 1992/1998.
- Tim Gowers, 1996/1998.
- Grigory Perelman, 1996/2006 (declined).
- Wendelin Werner, 2000/2006.
- Andrei Okounkov, 2004/2006.
- Elon Lindenstrauss, 2004/2010.
- Stanislav Smirnov, 2004/2010.
- Cédric Villani, 2008/2010.
- Artur Avila, 2008/2014.

We also have the brothers Lafforgue (one has the EMS Prize and one the Fields Medal) as well as combinations with other prestigious prizes. Hopefully, this trend will continue.

Later, other prizes were introduced: today, the EMS also awards the *Felix Klein Prize* for exceptional research in the area of applied mathematics and the *Otto Neugebauer Prize* for highly original and influential work in the field of history of mathematics.

EMS standing committees

We have 11 standing committees, the aim being to reflect most of the aspects of a mathematician's life. Let us mention the remit of each of them briefly.

- *Applied Mathematics*: one of the most active committees, reflecting the vital importance of mathematics in many fields of life and science. At the same time, we strongly believe in the unity of mathematics and we want pure and applied mathematicians to keep talking to each other under a single roof.
- *Developing Countries*: in collaboration with the corresponding IMU commission (CIMPA) and others, the aim of this committee is to help mathematicians in various ways in less fortunate countries. We only wish we had more money available for this noble goal.
- *Education*: there is no need to stress how important mathematical education is for the future of our discipline. At the same time, it is not always simple to find a common language between mathematics teachers and researchers.
- *Electronic Publishing*: the electronic ways of communicating mathematical results are steadily gaining importance, both concerning new literature and turning older results into digital forms (more on this later).
- *Ethics*: a relatively young committee dealing with issues of ever growing importance. Their task is to set rules such as the Code of Practice, which they formulated and which we recommend is followed by journals, as well as looking into concrete cases of scientific misbehaviour.
- *European Solidarity*: a quarter of a century after the European divide was removed, some significant differ-

ences persist and we are committed to help those who need it, especially young mathematicians suffering difficulties from the economic weakness of their country and region.

- *Meetings*: the task of this committee is to make recommendations on conferences, schools and other activities that the EMS should support financially (provided the budget allows it).
- *Publications*: this committee deals with various general publication issues, e.g. those concerning open access problems.
- *Raising Public Awareness*: there is no doubt that perception of mathematics among the general population is not exactly optimal and it is in our vital interest to do everything we can to improve this situation.

The two remaining committees will be mentioned separately.

ERCOM

This particular committee consists of leaders of the *European Research Centres in the Mathematical Sciences*. Europe has probably the densest network of such centres. They are very different to each other; some have a significant permanent staff and some are 'conference factories' but they all maintain a very high scientific level. In the words of Brian Davis about one of them, they are "... a mathematician's version of paradise". Let me explicitly mention at least a few:

- Stefan Banach International Mathematical Center.
- Centre International de Rencontres Mathématiques (CIRM).
- Erwin Schrödinger International Institute for Mathematical Physics.
- Euler International Mathematical Institute.
- The Abdus Salam International Centre for Theoretical Physics (ICTP).
- Institut des Hautes Études Scientifiques (IHÉS).
- Institut Mittag-Leffler.
- Isaac Newton Institute for Mathematical Sciences.
- Eighteen others.

Women in mathematics

The last committee (alphabetically) deals with female issues. We are well aware that the boundary conditions for the careers of men and women in mathematics are not the same and we are firmly committed to work against any biases.

It is important to say that women have often played vital roles throughout the history of the EMS. I cannot mention all of them so let me just recall a pair of names of particular significance. The first belongs to the lady who for about 15 years was the soul and memory of the society, *Tuulikki Mäkeläinen*. Furthermore, we not only have examples of participation but also of female leadership. I shall mention two names here. *Marta Sanz-Solé* served as the society's president, 2011–2014, and we all have fresh memories of the way she led the society: strong and diplomatic at the same time. One of the

most active members of the applied mathematics community, *Maria Jesús Esteban*, has been, since the beginning of 2016, the President of the ICIAM, an important organisation of which the EMS is a member. We wish her success in this role!



Tullikki Mäkeläinen

It is impossible to list all the women who have played a significant role in building the EMS. Let me just flash through a sample of names alphabetically: *Eva Bayer-Fluckiger*, *Bodil Branner*, *Mireille Chaleyat-Maurel*, *Doina Cioranescu*, *Mireille Martin-Deschamps*, *Lucia Di Vizio*, *Olga Gil-Medrano*, *Frances Kirwan*, *Sheung Tsun Tsou*, *Nina Uraltseva* and many, many others. And I should not forget three more names: a member of the current Executive Committee, *Laurence Halpern*, who did most of the work in preparing locally for the anniversary meeting, and the two young ladies, *Elvira Hyvönen* and *Erika Runolinna*, who currently run our secretariat in Helsinki.

Further activities

Congresses and committee work are by far not all that the EMS does. We support many sorts of mathematical activities, for example:

- *EMS Lecturers* once a year. The last was *Nicole Tomczak-Jägerman* at the EWM Conference in Cortona in September 2015.
- *EMS Distinguished Speakers* up to three per year, recently *Sylvia Serfaty* at the AMS-EMS-SPM Conference in Porto in June 2015.
- *EMS Joint Mathematical Weekends*. The ninth of this conference series was organised together with the LMS in September 2015 in Birmingham.
- *EMS Summer Schools* in pure and applied mathematics. In 2016, the society will provide financial support for six of them.
- *Activities with other societies*: joint lectures with the Bernoulli Society, in 2015 by *Gunnar Carlsson* at the European Statistical Congress and in 2016 by *Sara van de Geer* at the Nordic Mathematical Congress in Stockholm, March 2016. There is also the joint Summer school with the *International Association of Mathematical Physics*, in 2016 to be held in July in Rome.
- *Diderot Fora* devoted to relations of mathematics to other areas of human activity.

Applications for financial support can be made through the EMS webpage, before the end of September of the preceding year. They are collected and their scientific merits evaluated by our meetings committee. On our webpage, we also run a database of *jobs in mathematics*.

European Digital Mathematics Library Initiative

Mathematics literature is unusual in that it is, at least in principle, *eternally valid*. Europe is taking the lead in making this treasure trove digitally accessible, in particular through the digital library EuDML, accessible at <https://eudml.org/>.

- It provides a gateway to electronic publications and repositories of data providers.
- It has 12 founding members, among them the EMS, FIZ Karlsruhe, ICMCM Warsaw, University of Grenoble, Czech Academy of Sciences and UMI.
- Data, tools and services were assembled or created in the EU funded *EuDML Project* (2009–2013). After this source expired, the work continued being supported by its participants to the measure of their possibilities.
- The EuDML is estimated to cover some 6% of the mathematics literature in the world. There is a hope, albeit distant, that eventually it will become a part of the Global Digital Mathematics Library.

Another way in which we take care of the mathematical literature is the *Zentralblatt für Mathematik*, which we run together with Springer and FIZ Karlsruhe. Users may have noted significant innovations recently in the functioning of zbmATH. It is not an easy task but we invest effort in it because we believe it is important for the world to have two wells from which mathematical metadata can be drawn.

EU-MATHS-IN

A theorem may be the highest form of a mathematical result but it is by far not the only mode of mathematical achievement. In this connection, it is useful to mention another recent initiative:

- A network of mathematics for industry and innovation promoted by the EMS and ECMI (European Consortium for Mathematics in Industry). For more information, see <http://www.eu-maths-in.eu/>.
- Members are national networks in industrial mathematics: France, Germany, Austria, Italy, Spain, Netherlands, UK, Ireland, Hungary, Czech Republic, Poland, Sweden and Norway.
- It is a service unit for exchange of mathematical research and exploitation for innovation, industry, science and society.
- At the same time, it is a bridge between academic research groups and industry with European support.

The EMS Publishing House

At the dawn of the millennium, the EMS started its own publishing house. The main mover was *Rolf Jeltsch*, then the EMS President. The society owes its successful start to *Thomas Hintermann* and also to *Manfred Karbe* and others. After about 15 years of existence:

- The EMS-PH presently publishes *10–15 books* per year and *19 journals*.

- Among the journals, we have our ‘own’ *Journal of the EMS* (or JEMS), which has already built a high reputation.
- The EMS also publishes a *Newsletter* – which is no surprise to the readers of this article. I hope you all agree that it offers a lot of interesting reading and recall that its complete electronic version is freely available through the EMS webpage.
- As the publishing house has grown, we recently decided to form a *Scientific Advisory Board*, now headed by Jakob Yngvason. It is our intention to develop the enterprise further and make it stronger.

Outside Europe and outside mathematics

The above activity list could be continued, also mentioning that:

- We collaborate with the *International Mathematical Union* and with mathematical organisations around the world. In particular, we have reciprocity and cooperation agreements with partner societies in the U.S., Canada, Australia, Japan and Latin America.
- We are involved in high mathematical awards such as the *Abel Prize* and in various mathematical committees.

- As mentioned above, we are a part of *CIMPA*, an organisation that helps mathematicians in the developing countries around the world.
- We use our influence for *political lobbying* in various European institutions in the interests of mathematics and science in general.

What does this all tell us?

I think you would agree that the above survey documents that the EMS has not been idle in the first quarter of a century of its existence and that it has come a significant way from its modest origins in Mađralin. The purpose of my presentation, definitely, is not to boast about our achievements. We are well aware – paraphrasing the words of Isaac Newton – that we are standing on the shoulders of giants. It is our constituents, *our corporate and individual members*, from whom the EMS derives its strength and it is them who deserve our sincere thanks at this jubilee occasion.

At the same time, I hope that the survey I presented managed to convince everybody that the EMS, on its 25th birthday, is strong and self-confident, and is well prepared *to face the challenges in the years to come*.

Profinite Number Theory

Hendrik Lenstra (Universiteit Leiden, The Netherlands)

The ring of profinite integers, commonly named “Zee-hat”, is a familiar acquaintance of researchers in infinite Galois theory, algebraic number theory and arithmetic geometry. This article provides an elementary introduction to profinite numbers and their unconventional algebraic and analytic properties. It is based on a lecture and is intended to be a faithful write-up of the lecture text.

1 The factorial number system

Each $n \in \mathbf{Z}_{\geq 0}$ has a unique representation

$$n = \sum_{i=1}^{\infty} c_i i!, \quad \text{with } c_i \in \mathbf{Z},$$

$$0 \leq c_i \leq i, \quad \#\{i : c_i \neq 0\} < \infty.$$

In factorial notation:

$$n = (\dots c_3 c_2 c_1)_!$$

Examples: $25 = (1001)_!$, $1001 = (121221)_!$.

Note: $c_1 \equiv n \pmod 2$.

2 Arithmetic

For any k , the last k digits of $n + m$ depend only on the last k digits of n and of m , and likewise for $n \cdot m$.

Hence, one can also define the sum and the product of any two infinite sequences $(\dots c_3 c_2 c_1)_!$, with each $c_i \in \mathbf{Z}$, $0 \leq c_i \leq i$, and with the number of i with $c_i \neq 0$ now allowed to be infinite.

3 Profinite integers

Example: $(\dots 4321)_! + (\dots 0001)_! = (\dots 0000)_! = 0$. Hence, the sequence $(\dots 4321)_!$, with all $c_i = i$, may be called -1 .

The set of all sequences $(\dots c_3 c_2 c_1)_!$ as above is a ring with the operations as just defined: the *ring of profinite integers*, $\hat{\mathbf{Z}}$.

4 A formal definition

A more satisfactory definition of $\hat{\mathbf{Z}}$ is

$$\hat{\mathbf{Z}} = \left\{ (a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} (\mathbf{Z}/n\mathbf{Z}) : n|m \Rightarrow a_m \equiv a_n \pmod n \right\}.$$

This is a subring of $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$, with componentwise ring operations.

The group $\hat{\mathbf{Z}}^*$ consisting of the invertible elements of $\hat{\mathbf{Z}}$ is a subgroup of $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})^*$.

An equivalent definition is that $\hat{\mathbf{Z}}$ is the ring of endomorphisms of the group \mathbf{Q}/\mathbf{Z} and $\hat{\mathbf{Z}}^*$ is the automorphism group of \mathbf{Q}/\mathbf{Z} .

5 Three exercises

Exercise 1. Show that the ring $\hat{\mathbf{Z}}$ is commutative and that the unique ring homomorphism $\mathbf{Z} \rightarrow \hat{\mathbf{Z}}$ is injective but not surjective.

Exercise 2. Show that the ring $\hat{\mathbf{Z}}$ is uncountable.

Exercise 3. Let $m \in \mathbf{Z}_{>0}$. Show that the maps $\hat{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}}, a \mapsto ma$ and $\hat{\mathbf{Z}} \rightarrow \mathbf{Z}/m\mathbf{Z}, a = (a_n)_{n=1}^{\infty} \mapsto a_m$ combine into a short exact sequence

$$0 \rightarrow \hat{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}} \rightarrow \mathbf{Z}/m\mathbf{Z} \rightarrow 0.$$

In particular, show that m is not a zero-divisor in $\hat{\mathbf{Z}}$.

6 Profinite rationals

Let

$$\hat{\mathbf{Q}} = \left\{ (a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty}(\mathbf{Q}/n\mathbf{Z}) : n|m \Rightarrow a_m \equiv a_n \pmod{n\mathbf{Z}} \right\}.$$

Exercise 4. Show that the additive group $\hat{\mathbf{Q}}$ has exactly one ring multiplication extending the ring multiplication on $\hat{\mathbf{Z}}$.

Exercise 5. Show that the ring $\hat{\mathbf{Q}}$ is commutative, that it has \mathbf{Q} and $\hat{\mathbf{Z}}$ as subrings and that

$$\hat{\mathbf{Q}} = \mathbf{Q} + \hat{\mathbf{Z}} = \mathbf{Q} \cdot \hat{\mathbf{Z}} \cong \mathbf{Q} \otimes_{\mathbf{Z}} \hat{\mathbf{Z}} \quad (\text{as rings}).$$

7 Topological structure

If each $\mathbf{Z}/n\mathbf{Z}$ is given the discrete topology and $\prod_n(\mathbf{Z}/n\mathbf{Z})$ the product topology then $\hat{\mathbf{Z}}$ is closed in $\prod_n(\mathbf{Z}/n\mathbf{Z})$.

It is a compact, Hausdorff, totally disconnected topological ring. A neighbourhood base of 0 is $\mathcal{B} = \{m\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\}$.

The same neighbourhood base also makes $\hat{\mathbf{Q}}$ into a topological ring. It is locally compact, Hausdorff and totally disconnected.

Exercise 6: Show that $\mathbf{Q} \subset \hat{\mathbf{Q}}$ is dense and that $\hat{\mathbf{Z}} \subset \hat{\mathbf{Q}}$ is closed.

8 Amusing isomorphisms

$\hat{\mathbf{Z}}$ has been defined as a subring of $A = \prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$.

Exercise 7: Show that $A/\hat{\mathbf{Z}} \cong A$ as additive topological groups.

Exercise 8: Show that $A \cong A \times \hat{\mathbf{Z}}$ as groups but not as topological groups.

9 Profinite groups

In infinite Galois theory, the Galois groups that one encounters are *profinite groups*.

A profinite group is a topological group that is isomorphic to a closed subgroup of a product of finite discrete groups.

An equivalent definition is that it is a compact, Hausdorff, totally disconnected topological group.

Examples: The additive group of $\hat{\mathbf{Z}}$ and its group $\hat{\mathbf{Z}}^*$ of invertible elements are profinite groups.

10 $\hat{\mathbf{Z}}$ as the analogue of \mathbf{Z}

It is a well known fact that for each group G and each $\gamma \in G$, there is a unique group homomorphism $\mathbf{Z} \rightarrow G$ with $1 \mapsto \gamma$, namely $n \mapsto \gamma^n$.

An analogue for $\hat{\mathbf{Z}}$ is that, for each profinite group G and each $\gamma \in G$, there is a unique group homomorphism $\hat{\mathbf{Z}} \rightarrow G$ with $1 \mapsto \gamma$ and it is continuous, $a \mapsto \gamma^a$.

11 Examples of infinite Galois groups

The ring $\hat{\mathbf{Z}}$ is helpful in describing infinite Galois groups.

Write \bar{k} for an algebraic closure of a field k .

Example 1: With p prime and $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, one has

$$\begin{aligned} \hat{\mathbf{Z}} &\xrightarrow{\sim} \text{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p), \\ a &\mapsto \text{Frob}^a, \end{aligned}$$

where $\text{Frob}(\alpha) = \alpha^p$ for all $\alpha \in \bar{\mathbf{F}}_p$.

Example 2: With

$$\mu = \{\text{roots of unity in } \bar{\mathbf{Q}}^*\} \cong \mathbf{Q}/\mathbf{Z},$$

the map $\sigma \mapsto \sigma|_{\mu}$ induces an isomorphism

$$\text{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}) \xrightarrow{\sim} \text{Aut } \mu \cong \hat{\mathbf{Z}}^*$$

of topological groups.

12 Radical Galois groups

There are also non-abelian examples.

Example 3. For $r \in \mathbf{Q}, r \notin \{-1, 0, 1\}$, write

$$\sqrt[n]{r} = \{\alpha \in \bar{\mathbf{Q}} : \exists n \in \mathbf{Z}_{>0} : \alpha^n = r\}.$$

Theorem. Let G be a profinite group. Then, there exists $r \in \mathbf{Q} \setminus \{-1, 0, 1\}$ with $G \cong \text{Gal}(\mathbf{Q}(\sqrt[n]{r})/\mathbf{Q})$ (as topological groups) if and only if there is a non-split exact sequence

$$0 \rightarrow \hat{\mathbf{Z}} \xrightarrow{\iota} G \xrightarrow{\pi} \hat{\mathbf{Z}}^* \rightarrow 1$$

of profinite groups such that

$$\forall a \in \hat{\mathbf{Z}}, \gamma \in G : \gamma \cdot \iota(a) \cdot \gamma^{-1} = \iota(\pi(\gamma) \cdot a).$$

“Non-split” means the sequence does not arise from an isomorphism $G \cong \hat{\mathbf{Z}} \rtimes \hat{\mathbf{Z}}^*$. This condition is necessary because of the theorem of Kronecker–Weber.

13 Diophantine equations

One also encounters $\hat{\mathbf{Z}}$ in arithmetic algebraic geometry.

For $f_1, \dots, f_k \in \mathbf{Z}[X_1, \dots, X_n]$, one is interested in solutions $x = (x_1, \dots, x_n) \in \mathbf{Z}^n$ to the system $f_1(x) = \dots = f_k(x) = 0$.

Theorem.

- (a) The system has a solution $x \in \mathbf{Z}^n \Rightarrow$ for each $m \in \mathbf{Z}_{>0}$, it has a solution modulo $m \Leftrightarrow$ it has a solution $x \in \hat{\mathbf{Z}}^n$.
- (b) It is decidable whether a given system has a solution $x \in \hat{\mathbf{Z}}^n$.

14 p-adic numbers

Let p be prime. The ring of p -adic integers is

$$\mathbf{Z}_p = \{(b_i)_{i=0}^\infty \in \prod_{i=0}^\infty (\mathbf{Z}/p^i\mathbf{Z}) : i \leq j \Rightarrow b_j \equiv b_i \pmod{p^i}\}.$$

Like $\hat{\mathbf{Z}}$, it is a compact, Hausdorff, totally disconnected topological ring.

It is also a *principal ideal domain*, with $p\mathbf{Z}_p$ as its only non-zero prime ideal. Each ideal of \mathbf{Z}_p is *closed* and is of the form $p^h\mathbf{Z}_p$ with $h \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$, where $p^\infty\mathbf{Z}_p = \{0\}$.

15 The Chinese remainder theorem

For $n = \prod_{p \text{ prime}} p^{i(p)}$ (with $i(p) \in \mathbf{Z}_{\geq 0}$ and almost all $i(p) = 0$), one has a ring isomorphism

$$\mathbf{Z}/n\mathbf{Z} \cong \prod_{p \text{ prime}} (\mathbf{Z}/p^{i(p)}\mathbf{Z}).$$

In the limit,

$$\hat{\mathbf{Z}} \cong \prod_{p \text{ prime}} \mathbf{Z}_p \quad (\text{as topological rings}).$$

16 Profinite number theory

The isomorphism $\hat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p$ reduces most questions about $\hat{\mathbf{Z}}$ to similar questions about the much better behaved rings \mathbf{Z}_p . For this reason, $\hat{\mathbf{Z}}$ has received little attention in itself.

Profinite number theory in its proper sense studies those properties of $\hat{\mathbf{Z}}$ that involve interactions between different rings \mathbf{Z}_p , and those that are due to Euclid's discovery that $\prod_p \mathbf{Z}_p$ is an infinite product. It is to such properties that the remainder of this article is largely devoted.

While I believe that all statements I make are correct, I have not seen published or even written proofs of many of them. So, in a formal sense, much of what follows should be considered speculative.

17 Ideals of $\hat{\mathbf{Z}}$

For an ideal $\mathfrak{a} \subset \hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$, the following are equivalent:

- \mathfrak{a} is closed.
- \mathfrak{a} is finitely generated.
- \mathfrak{a} is principal.
- $\mathfrak{a} = \prod_p \mathfrak{a}_p$, where each $\mathfrak{a}_p \subset \mathbf{Z}_p$ is an ideal.

The set of closed ideals of $\hat{\mathbf{Z}}$ is in bijection with the set of *Steinitz numbers*. These are formal expressions $\prod_p p^{h(p)}$, with each $h(p) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$. The Steinitz number $\prod_p p^{h(p)}$ corresponds to the closed ideal $\prod_p p^{h(p)}\mathbf{Z}_p$.

Most ideals of $\hat{\mathbf{Z}}$ are not closed.

18 The spectrum of $\hat{\mathbf{Z}}$

The *spectrum* $\text{Spec } R$ of a commutative ring R is its set of prime ideals, an example being $\text{Spec } \mathbf{Z}_p = \{\{0\}, p\mathbf{Z}_p\}$.

For $S \subset \mathcal{P} = \{\text{prime numbers}\}$, let $e_S \in \hat{\mathbf{Z}} = \prod_{p \in \mathcal{P}} \mathbf{Z}_p$ have coordinate 0 at $p \in S$ and 1 at $p \notin S$.

For each $\mathfrak{p} \in \text{Spec } \hat{\mathbf{Z}}$, the set

$$\Upsilon(\mathfrak{p}) = \{S \subset \mathcal{P} : e_S \in \mathfrak{p}\}$$

is an *ultrafilter* on \mathcal{P} .

Example. Let $p \in \mathcal{P}$ and let $\mathfrak{p} \subset \hat{\mathbf{Z}}$ be the kernel either of the natural map $\hat{\mathbf{Z}} \rightarrow \mathbf{Z}/p\mathbf{Z}$ or of the natural projection $\hat{\mathbf{Z}} \rightarrow \mathbf{Z}_p$. Then, one has

$$S \in \Upsilon(\mathfrak{p}) \Leftrightarrow p \in S,$$

so $\Upsilon(\mathfrak{p})$ is a *principal* ultrafilter.

19 The spectrum and ultrafilters

One may study $\text{Spec } \hat{\mathbf{Z}}$ through the map

$$\Upsilon: \text{Spec } \hat{\mathbf{Z}} \rightarrow \{\text{ultrafilters on } \mathcal{P}\}.$$

Theorem.

- (a) \mathfrak{p} is closed in $\hat{\mathbf{Z}} \Leftrightarrow \Upsilon(\mathfrak{p})$ is principal.
- (b) $\Upsilon(\mathfrak{p}) = \Upsilon(\mathfrak{q}) \Leftrightarrow \mathfrak{p}$ and \mathfrak{q} have an inclusion relation.
- (c) Let U be an ultrafilter on \mathcal{P} . Then, the fibre $\Upsilon^{-1}U$ has size 2 if U is principal and is infinite if U is free.

Question: How does the order type of the totally ordered set $\Upsilon^{-1}U$ vary as U ranges over all ultrafilters on \mathcal{P} ?

20 The logarithm

For $u \in \mathbf{R}_{>0}$, one has $\frac{d}{dx}u^x = (\log u)u^x$, so

$$\log u = \left(\frac{d}{dx}u^x\right)_{x=0} = \lim_{\epsilon \rightarrow 0} \frac{u^\epsilon - 1}{\epsilon}.$$

Analogously, define $\log: \hat{\mathbf{Z}}^* \rightarrow \hat{\mathbf{Z}}$ by

$$\log u = \lim_{n \rightarrow \infty} \frac{u^{n!} - 1}{n!} \quad (\text{note: } \lim_{n \rightarrow \infty} n! = 0 \text{ in } \hat{\mathbf{Z}}).$$

This is a well-defined continuous group homomorphism, with

$$\begin{aligned} \ker \log &= \hat{\mathbf{Z}}_{\text{tor}}^* = \text{closure of } \{u \in \hat{\mathbf{Z}}^* : \exists n \in \mathbf{Z}_{>0} : u^n = 1\}, \\ \text{im } \log &= 2J = \{2x : x \in J\}, \end{aligned}$$

where $J = \bigcap_{p \text{ prime}} p\hat{\mathbf{Z}}$ is the Jacobson radical of $\hat{\mathbf{Z}}$.

21 Structure of $\hat{\mathbf{Z}}^*$

The logarithm fits in a commutative diagram

$$\begin{array}{ccccccc} 1 & \rightarrow & \hat{\mathbf{Z}}_{\text{tor}}^* & \rightarrow & \hat{\mathbf{Z}}^* & \xrightarrow{\log} & 2J & \rightarrow & 0 \\ & & \downarrow \wr & & \parallel & & \wr \uparrow & & \\ 1 & \leftarrow & (\hat{\mathbf{Z}}/2J)^* & \leftarrow & \hat{\mathbf{Z}}^* & \leftarrow & 1+2J & \leftarrow & 1 \end{array}$$

of profinite groups, where:

- The other horizontal maps are the natural ones.
- The rows are exact.
- The vertical maps make the diagram commutative.
- The vertical maps are *isomorphisms*.

As a consequence, one has a canonical isomorphism

$$\hat{\mathbf{Z}}^* \cong (\hat{\mathbf{Z}}/2J)^* \times 2J$$

of topological groups.

22 More on $\hat{\mathbf{Z}}^*$

Less canonically, one has isomorphisms

$$2\mathbf{J} \cong \hat{\mathbf{Z}},$$

$$(\hat{\mathbf{Z}}/2\mathbf{J})^* \cong (\mathbf{Z}/2\mathbf{Z}) \times \prod_p (\mathbf{Z}/(p-1)\mathbf{Z}) \cong \mathbf{A},$$

$$\hat{\mathbf{Z}}^* \cong \mathbf{A} \times \hat{\mathbf{Z}}$$

of topological groups, where $\mathbf{A} = \prod_{n \geq 1} (\mathbf{Z}/n\mathbf{Z})$ is as in Section 8, and a group isomorphism

$$\hat{\mathbf{Z}}^* \cong \mathbf{A}.$$

23 Power series expansions

The isomorphism

$$\log: 1 + 2\mathbf{J} \xrightarrow{\sim} 2\mathbf{J}$$

from Section 21 and its inverse

$$\exp: 2\mathbf{J} \xrightarrow{\sim} 1 + 2\mathbf{J}$$

are given by power series expansions

$$\log(1-x) = - \sum_{n=1}^{\infty} \frac{x^n}{n},$$

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

that converge for all $x \in 2\mathbf{J}$.

There is a weaker sense in which

$$\log: \hat{\mathbf{Z}}^* \rightarrow \hat{\mathbf{Z}}$$

is analytic on all of $\hat{\mathbf{Z}}^*$.

24 Two topologies on $\hat{\mathbf{Q}}$

In the topology that was defined on $\hat{\mathbf{Q}}$, the collection

$$\mathcal{B} = \{m\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\}$$

is a neighbourhood base of 0 that consists of $\hat{\mathbf{Z}}$ -ideals.

The set of closed maximal ideals of $\hat{\mathbf{Q}}$ is a subbase for the neighbourhoods of 0 in a second ring topology on $\hat{\mathbf{Q}}$ that is needed. An explicit neighbourhood base of 0 in that topology is given by

$$\mathcal{C} = \left\{ \mathbf{Q} \cdot \bigcap_{n=0}^{\infty} m^n \hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0} \right\}.$$

This collection consists of $\hat{\mathbf{Q}}$ -ideals.

25 Analyticity

Let $x_0 \in D \subset \hat{\mathbf{Q}}$.

Call $f: D \rightarrow \hat{\mathbf{Q}}$ analytic in x_0 if there exists a sequence $(a_n)_{n=0}^{\infty} \in \hat{\mathbf{Q}}^{\infty}$ such that the power series expansion

$$f(x) = \sum_{n=0}^{\infty} a_n \cdot (x - x_0)^n$$

is valid in the sense that

$$\forall U \in \mathcal{C} : \exists V \in \mathcal{B} : \forall x \in (x_0 + V) \cap D : \forall W \in \mathcal{B} :$$

$$\exists N_0 \in \mathbf{Z}_{\geq 0} : \forall N \geq N_0 : \sum_{n=0}^N a_n \cdot (x - x_0)^n \in f(x) + U + W.$$

To understand this formula, first omit “ $\forall U \in \mathcal{C} :$ ” and “ $+ U$ ” to see a more familiar notion of analyticity.

26 Examples of analytic functions

The map $\log: \hat{\mathbf{Z}}^* \rightarrow \hat{\mathbf{Z}} \subset \hat{\mathbf{Q}}$ is analytic in each $x_0 \in \hat{\mathbf{Z}}^*$, with expansion

$$\log x = \log x_0 - \sum_{n=1}^{\infty} \frac{(x_0 - x)^n}{n \cdot x_0^n}.$$

For each $u \in \hat{\mathbf{Z}}^*$, the map

$$\hat{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}}^* \subset \hat{\mathbf{Q}}, \quad x \mapsto u^x,$$

is analytic in each $x_0 \in \hat{\mathbf{Z}}$, with expansion

$$u^x = \sum_{n=0}^{\infty} \frac{(\log u)^n \cdot u^{x_0} \cdot (x - x_0)^n}{n!}.$$

Note that the power series expansions of the corresponding real functions look the same.

27 A Fibonacci example

Define $F: \mathbf{Z}_{\geq 0} \rightarrow \mathbf{Z}_{\geq 0}$ by

$$F(0) = 0, \quad F(1) = 1, \quad F(n+2) = F(n+1) + F(n).$$

Theorem. *The function F has a unique continuous extension $\hat{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}}$ and it is analytic in each $x_0 \in \hat{\mathbf{Z}}$.*

Notation: F .

For $n \in \mathbf{Z}$, one has

$$F(n) = n \Leftrightarrow n \in \{0, 1, 5\}.$$

28 Fibonacci fixed points

One has

$$\#\{x \in \hat{\mathbf{Z}} : F(x) = x\} = 11.$$

The only even fixed point of F in $\hat{\mathbf{Z}}$ is 0.

In addition, for each $a \in \{1, 5\}$, $b \in \{-5, -1, 0, 1, 5\}$, there is a unique $z_{a,b} \in \hat{\mathbf{Z}}$ with

$$z_{a,b} \equiv a \pmod{\bigcap_{n=0}^{\infty} 6^n \hat{\mathbf{Z}}},$$

$$z_{a,b} \equiv b \pmod{\bigcap_{n=0}^{\infty} 5^n \hat{\mathbf{Z}}},$$

$$F(z_{a,b}) = z_{a,b}.$$

This gives 10 odd fixed points and these are all there are.

Examples: $z_{1,1} = 1, z_{5,5} = 5$.

The number $z_{5,-5}^2$ has the striking property that it is very close to $5^2 = (-5)^2 = 25$ without being equal to it:

$$z_{5,-5}^2 \equiv 25 \pmod{201! \cdot \hat{\mathbf{Z}}}, \quad z_{5,-5}^2 \not\equiv 25 \pmod{202! \cdot \hat{\mathbf{Z}}}.$$

29 Larger cycles

Apparently, one has

$$\#\{x \in \hat{\mathbf{Z}} : F(F(x)) = x\} = 21,$$

$$\#\{x \in \hat{\mathbf{Z}} : F^n(x) = x\} < \infty, \quad \text{for each } n \in \mathbf{Z}_{>0}.$$

Here, F^n denotes the n -fold iterate of F .

Question: Does F have cycles of length greater than 2?

30 Other linear recurrences

Suppose that

$$E: \mathbf{Z}_{\geq 0} \rightarrow \mathbf{Z}, \quad t \in \mathbf{Z}_{>0}, \quad d_0, \dots, d_{t-1} \in \mathbf{Z}$$

are such that

$$\forall n \in \mathbf{Z}_{\geq 0} : E(n+t) = \sum_{i=0}^{t-1} d_i \cdot E(n+i),$$

$$d_0 \in \{1, -1\}.$$

Then, E has a unique continuous extension $\hat{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}}$, still denoted by E . That extension is analytic in each $x_0 \in \hat{\mathbf{Z}}$.

31 Finite cycles

Suppose, in addition,

$$X^t - \sum_{i=0}^{t-1} d_i X^i = \prod_{i=1}^t (X - \alpha_i),$$

where

$$\alpha_1, \dots, \alpha_t \in \mathbf{Q}(\sqrt{\mathbf{Q}}),$$

$$\alpha_j^{24} \neq \alpha_k^{24}, \quad (1 \leq j < k \leq t).$$

Example: $X^2 - X - 1 = (X - (1 + \sqrt{5})/2)(X - (1 - \sqrt{5})/2)$.

Tentative theorem. *If $n \in \mathbf{Z}_{>0}$ is such that the set*

$$S_n = \{x \in \hat{\mathbf{Z}} : E^n(x) = x\}$$

is infinite then $S_n \cap \mathbf{Z}_{\geq 0}$ contains an infinite arithmetic progression.

This theorem is tentative not just because of what was highlighted in Section 16 but also because it is not clear whether it is in its final form. Maybe the reader will see how the conditions on $\alpha_1, \dots, \alpha_t$ stated above come in. But to what extent are they necessary? Also, can the conclusion of the theorem be strengthened? Is there an example? The theorem would, at least, imply that $\{x \in \hat{\mathbf{Z}} : F^n(x) = x\}$ is indeed finite for each $n \in \mathbf{Z}_{>0}$.

32 Envoi

And that's the end.

Now carp at me. I don't intend

to justify this tale to you.

Why tell it? Well, I wanted to!

Alexander Pushkin (Translated by Ranjit Bolt)

33 Notes on the literature

The reader will have no difficulty locating references for profinite groups and infinite Galois theory. I especially recommend Gruenberg's contribution [5] to the classical volume by Cassels and Fröhlich [3]; other chapters in the same volume provide much arithmetic context. The proof of the theorem on radical Galois groups in Section 12 involves a fair bit of continuous cochain cohomology. This may be found in Abtien Javanpeykar's Leiden's Master's thesis [6]. For part (b) of the Diophantine theorem in Section 13, I do not know a reference but there is no doubt that it can be proved by techniques that

are commonly known to experts. Finding literature about p -adic numbers and ultrafilters may again be left to the reader. Steinitz numbers were introduced in 1910 by Steinitz [8, §16]. In my earlier paper on the subject [7], one will find, in addition to a graphical representation of several functions defined on profinite numbers, the power series expansion of the Fibonacci function, as well as information on its 11 fixed points. The definition of analyticity in Section 25 is inspired by the same paper. The tentative result stated in Section 31 is reminiscent of the theorem of Mahler (1935) and Lech (1954), for which the book by Cassels [2] is a fine reference. The Pushkin quotation in Section 32 is taken from a collection of modern translations of several of his poems [4].

Bibliography

- [1] Ranjit Bolt, *Tsar Nikita and his daughters*, pp. 32–38 in [4].
- [2] J. W. S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986.
- [3] J. W. S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Academic Press, London and New York, 1967.
- [4] Elaine Feinstein (ed.), *After Pushkin*, The Folio Society, London, 1999.
- [5] K. Gruenberg, *Profinite groups*, Chapter V, pp. 116–127 in [3].
- [6] Abtien Javanpeykar, *Radical Galois groups and cohomology*, Master's thesis, Mathematisch Instituut, Universiteit Leiden, 2013.
- [7] Hendrik Lenstra, *Profinite Fibonacci numbers*, *Nieuw Arch. Wiskd.* (5) **6** (2005), 297–300; reprinted in: *Eur. Math. Soc. Newsl.* **61** (September 2006), 15–19.
- [8] Ernst Steinitz, *Algebraische Theorie der Körper*, *J. Reine Angew. Math.* **137** (1910), 167–309.



Hendrik W. Lenstra, Jr. [hwl@math.leidenuniv.nl] received his PhD from the Universiteit van Amsterdam in 1977. He has worked at Amsterdam, at Berkeley and at Leiden, and he retired in 2014. He is best known for having introduced advanced techniques in the area of number theory algorithms, which have important applications in cryptography and computer security.

Exchangeability, Chaos and Dissipation in Large Systems of Particles

Laure Saint-Raymond (Université Pierre et Marie Curie & École Normale Supérieure, Paris, France)

The assumption of molecular chaos postulated by Boltzmann is the cornerstone of statistical theories of gas dynamics and of most fluid models. At equilibrium, probabilistic tools allow one to study the validity of such an assumption in the absence of phase transition. Out of equilibrium, the question remains essentially open.

In this note, some mathematical approaches to this problem will be presented, especially Kac's work in which chaos comes from infinitesimal noise and Lanford's work in which chaos is propagated asymptotically in the low density limit. In the vicinity of equilibrium, it will be shown that entropy production can be interpreted in terms of the growth of correlations.

The simplest possible dynamics of interacting particles to model gases at the level of atoms is hard sphere dynamics. Despite many efforts over the last 50 years, it still raises a lot of challenging open questions at the interface between dynamical systems, partial differential equations and probability. The answers to these questions are really important for physics because microscopic chaos is the cornerstone assumption of most macroscopic descriptions of gases, both at the kinetic level and at the fluid level. In other words, this is the very first step in the programme to solving Hilbert's sixth problem [18].

The system considered here consists of N identical balls of unit mass and diameter ϵ , say in the torus \mathbf{T}^d , with positions and velocities $(X_i(t), V_i(t))_{1 \leq i \leq N}$. It evolves under the combined effects of transport and collisions

$$\frac{dX_i}{dt} = V_i, \text{ as long as } |X_i - X_j| > \epsilon \text{ for all } j \neq i,$$

and specular reflection on the boundary $X_i - X_j = \epsilon n, n \in \mathbf{S}^{d-1}$,

$$V'_i = V_i - (V_i - V_j) \cdot nn, \quad V'_j = V_j + (V_i - V_j) \cdot nn.$$

These dynamics preserve the total linear momentum and the total kinetic energy

$$V'_i + V'_j = V_i + V_j, |V'_i|^2 + |V'_j|^2 = |V_i|^2 + |V_j|^2$$

and are globally well-defined for almost all initial configurations. Indeed, only a zero measure set of initial data leads to multiple collisions or an infinite number of collisions in a finite time [1].

However, in the vicinity of these pathological trajectories, the flow is not continuous with respect to the data. More generally, if the size of the particles is small, the system is expected to be highly unstable (as changing the position of one particle a little bit may completely change the trajectory). It therefore seems difficult to predict any deterministic behaviour of the system.

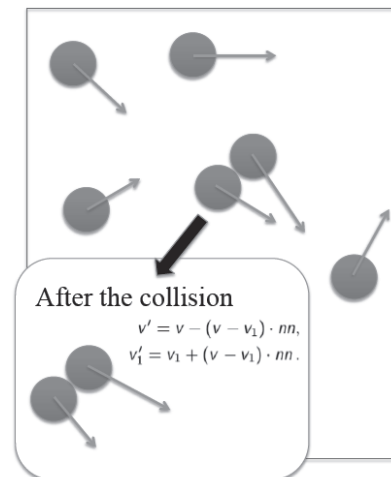


Figure 1. Hard sphere dynamics

The idea is then to take advantage of these mixing properties to capture some average behaviour. The disorder created by these mixing phenomena is usually referred to as “chaos” but this could actually correspond to different mechanisms:

- 1 Ergodicity is related to time averaging: roughly, it states that, for almost all initial data, the trajectory of the system will cover the whole energy level uniformly (up to the natural invariances of the system).
- 2 Uncorrelation is another measure of the disorder: if a system consists of a large number of particles that are not in a solid state, any two tagged particles are expected to evolve essentially independently of each other. This means, in particular, that there should be some preferred macroscopic configurations (because of the law of large numbers).

The goal here is to give a brief overview of the mathematical statements describing the foundations of statistical mechanics, both at thermodynamic equilibrium and out of equilibrium. It is not intended to be exhaustive but rather to point out some mathematical difficulties in making these well known theories rigorous.

1 Exchangeability and thermodynamic equilibrium

The heuristic argument to determining the statistical distribution of particles in a gas at thermal equilibrium is usually the following.

The first step is an assumption about uncorrelation.

In idealized gases, particles do not interact with one another except for very brief collisions in which they exchange energy and momentum. [...] This means that each particle's state can be considered independently from the other particles' state.

(From Wikipedia)

The second step then relies on a symmetry argument. As the particles are supposed to be identical, it is not important to keep track of their individual labels; only their statistical distribution is of interest. A computation due to Maxwell [24] shows that the average number of particles in a given single-particle microstate obeys the statistics

$$M_\beta(v) = \left(\frac{\beta}{2\pi}\right)^{d/2} \exp\left(-\frac{\beta}{2}|v|^2\right),$$

up to a translation in the velocity space (denoting by β the inverse temperature).

Clearly the statement in the first step needs to be more properly understood, as particles need to interact but still be independent.

Ergodicity and invariant measures

A first approach is to look at all possible equilibria for the system of N particles, i.e. at all invariant measures, and then to study the structures that are inherited on the distribution for any finite number of particles. In other words, take an average with respect to time and then possibly take limits as $N \rightarrow \infty$.

For the system of N hard spheres, the non-singular invariant measures are expected to depend only on the energy (up to a translation in velocity, due to the conservation of momentum). More precisely, the system is expected to be ergodic, meaning that on any energy surface, any subset that is invariant under the dynamics has to be either of zero measure or full measure.

However, this is a very challenging question and only partial results are currently known. They give either ergodicity in small dimension or ergodicity for almost all distributions of masses [8, 11, 20, 7, 29].

Theorem 1 (Simanyi). Consider a system of N hard spheres of radius ϵ and of masses $(m_i)_{1 \leq i \leq N}$ in \mathbf{T}^d . Then,

- if $N \leq \max(4, d)$, and $m_i = m$ for all i , the system is ergodic; and
- if $d = 2$, for all N , the system is ergodic for almost all distributions of masses $(m_i)_{1 \leq i \leq N}$.

In particular, it is not known whether or not the system of N identical hard spheres (with N large and ϵ small enough so that the system has no rigidity) is ergodic.

The different proofs are inductions on the number N of particles involved in the system and the induction step relies on the groundbreaking works for two particles by Bunimovitch-Sinai[8] and Chernov-Sinai[11]. They proved a strong result on local ergodicity: an open neighbourhood of every phase point with a hyperbolic trajectory (and with at most one singularity on its trajectory) belongs to a single ergodic component of the billiard flow, modulo the zero measure sets. The characterisation of the exceptional phase points then requires fine arguments of geometry and algebraic topology.

Concentration of measure in large dimension

From now on, the focus will be on invariant measures that only depend on the energy $H_N = \frac{1}{2} \sum_{i=1}^N |v_i|^2$. The next step is to understand the structure that is inherited by a given “single-particle microstate” and, more generally, by the joint distribution of s particles for any fixed s .

The central limit theorem [22, 6] shows that the velocities converge to independent normal variables. In low density regimes $N\epsilon^d \ll 1$, the non-overlapping condition $|x_i - x_j| > \epsilon$ disappears in the limit. Indeed, the partition function defined by

$$\mathcal{Z}_N = \int \prod_{1 \leq i < j \leq N} \mathbf{1}_{|x_i - x_j| > \epsilon} dX_N$$

satisfies

$$\log \frac{\mathcal{Z}_{N-s}}{\mathcal{Z}_N} \sim sN\epsilon^d \ll 1.$$

Theorem 2. Consider a system of N exchangeable hard spheres of radius ϵ with zero total linear momentum and uniformly distributed on the energy level corresponding to the inverse temperature β .

Then, in the limit $N \rightarrow \infty$, $\epsilon \rightarrow 0$, with $N\epsilon^d \rightarrow 0$, the law of s typical particles converges almost everywhere to M_β^{ss} .

Therefore, there is a precise scaling that defines the notion of “idealised gas”. In this setting, at thermal equilibrium, chaos is obtained asymptotically by a rather soft argument of concentration of measure.

Entropy and chaos

A good functional to express the concentration of measure is the entropy, which is defined for a random variable Z of density ρ by $S(Z) = - \int \rho \log \rho$. To get an entropic version of the central limit theorem, one can study, for instance, the evolution of the entropy along the process of block summation defined as follows. Let (Y_i) be a sequence of random variables (with zero expectation and the same finite variance). For any n , the sequel of random variables $Z_{n,i}$ is defined by recurrence

$$Z_{n,i} = Z_{n-1,2i} + Z_{n-1,2i+1},$$

with initialisation $Z_{0,i} = Y_i$.

One can then prove that the entropy increase is positive as long as the random variable $Z_{n,i}$ is not exactly Gaussian. A refinement of the Shannon-Stam inequality [32]

$$S\left(\sum_i \lambda_i Z_i\right) - \sum \lambda_i^2 S(Z_i) \geq 0, \text{ with } \sum \lambda_i^2 = 1,$$

provides the following estimate.

Theorem 3 (Carlen-Soffer). Denote by G a Gaussian variable with the same variance as Z_i . Then, under the Gaussian regularisation

$$\tilde{Z}_i = e^{-t} Z_i + (1 - e^{-2t})^{1/2} G,$$

the entropy difference decreases:

$$S\left(\sum_i \lambda_i Z_i\right) - \sum \lambda_i^2 S(Z_i) \geq S\left(\sum_i \lambda_i \tilde{Z}_i\right) - \sum \lambda_i^2 S(\tilde{Z}_i),$$

with equality when each Z_i has exactly the same Gaussian density.

Under an additional regularity condition expressed in terms of the Fisher information of the distribution ρ_i of Z_i

$$\int |\nabla \sqrt{\rho_i}|^2 < +\infty,$$

this quantity actually controls the relative entropy

$$S(Z_i|G) = - \int \left(\rho_i \log \frac{\rho_i}{M_\beta} - \rho_i + M_\beta \right).$$

Combining both results shows that $S(2^{-n/2} \sum_{i=1}^{2^n} Y_i)$ cannot converge towards a quantity which is strictly less than $S(G)$. Therefore, there is entropic convergence of the sum of independent variables towards the Gaussian [23, 2]:

$$S \left(2^{-n/2} \sum_{i=1}^{2^n} Y_i \middle| G \right) \rightarrow 0.$$

Moreover, in the case of weakly dependent variables, the entropy increase due to adding independent blocks may dominate the entropy loss due to local correlations. This leads to weak convergence of block summation and to an entropic central limit theorem even for dependent variables [9].

Boltzmann's approach

This result suggests that it is not necessary to have a very precise description of the joint law of variables $(Z_i)_{1 \leq i \leq N}$ to get a central limit theorem. In other words, there is no real need to understand the mixing properties for fixed N . Averaging only with respect to N with $N \gg 1$ should provide chaos.

Chaos in Boltzmann's kinetic theory [5] is actually not related to time averaging and does not require the system to be at thermodynamic equilibrium. Boltzmann's assumption (which needs to be proved to get a rigorous derivation of kinetic theory) is that the joint distribution of any two particles can be expressed in terms of the one-particle distribution

$$f_N^{(2)}(t, z_1, z_2) = f_N^{(1)}(t, z_1) f_N^{(1)}(t, z_2).$$

Note that this equality cannot be true for fixed N and ϵ since

- it does not account for the non-overlapping condition; and
- the product structure is not stable under the dynamics.

However, it is expected that an identity can be recovered asymptotically in the limit when $N \rightarrow \infty, \epsilon \rightarrow 0$.

One important issue is to understand in which sense the convergence holds. In particular, if the interactions between the particles are instantaneous, a natural question is whether the convergence to chaotic distributions is pointwise in time.

2 A stochastic model for the propagation of chaos

To start with, the focus will be on the mixing properties of the collision process, looking at simplified stochastic dynamics, referred to as Kac's model [19]. The idea here is to get rid of spatial variables and transport. Collisions are then not related to some boundary condition but defined as a stochastic jump process.

Randomness is therefore encoded in the dynamics:

- Collision times (t_k) are given by a Poisson process.
- Colliding pairs (i_k, j_k) are chosen randomly.
- The law of deflection angles n_k is given by the collision cross-section $b(V_{i_k} - V_{j_k}, n_k)$, where $b(w, n)$ depends only on $|w|$ and $|w \cdot n|$.

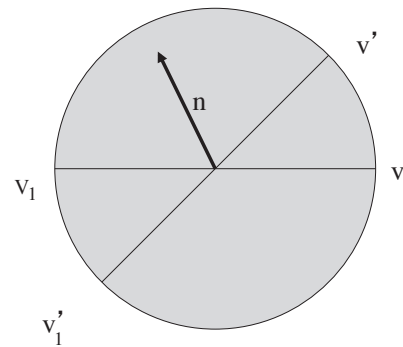


Figure 2. A jump process on the sphere

At each collision time, velocities are then updated according to the following formula:

$$V_i'(t^+) = V_i(t^-) - (V_i(t^-) - V_j(t^-)) \cdot nn,$$

$$V_j'(t^+) = V_j(t^-) + (V_i(t^-) - V_j(t^-)) \cdot nn,$$

where all subscripts k have been omitted for the sake of readability.

Because of the invariance of the collision cross-section b , Kac's process is microscopically reversible: the probability of having one specific collision is exactly the same as that of having the reverse collision. Kac's process is, however, much simpler than deterministic dynamics as it is a Markov chain, meaning that each jump is independent of the system's history.

The mean field limit

The mean field limit is the dynamics governing the average of the empirical measure

$$\mu_N(t, v) = \frac{1}{N} \sum_{i=1}^N \delta_{v=V_i(t)}$$

asymptotically in the limit $N \rightarrow \infty$.

In order that each particle exchanges a macroscopic quantity of energy (and momentum), the mean free time has to be of the order of $O(1)$. The transition probability for each pair of particles (i, j) therefore has to be of the order of $O(1/N)$.

Boltzmann's equation

$$\partial_t f = Q(f, f),$$

where the collision operator is defined for any $f = f(v)$ by

$$Q(f, f)(v) = \iint (f(v')f(v'_1) - f(v)f(v_1)) b(v - v_1, n) dv_1 dn,$$

then appears as a consequence of the law of large numbers.

Convergence to the Boltzmann equation

The work by Mischler and Mouhot [26] constitutes major progress in Kac's programme. Their results complete a series of works due to McKean [25], Snitzman [31], Graham and Méléard [14]. In particular, they obtain quantitative estimates for the convergence, with an explicit dependence with respect to the parameters of the problem, namely the number of particles N and the time t . These quantitative estimates are quite important given the fact that Kac's process is the underlying scheme in Monte-Carlo simulations of the Boltzmann equation.

The focus here will be on the case of the hard-sphere collision cross-section $b(v-v_1, n) = |(v-v_1) \cdot n|$ but the result can actually be extended to more general cross-sections, including those with a non-integrable singularity for grazing collisions.

Theorem 4 (Mischler & Mouhot). Consider N particles initially independent and identically distributed according to some compactly supported and centered $f_0 \in L^\infty(\mathbf{R}^d)$, and evolving according to Kac's process.

Then, in the mean field limit $N \rightarrow \infty$, the distribution of s typical particles $f_N^{(s)}$ converges to $f^{\otimes s}$ on any fixed time interval $[0, T]$:

$$\frac{1}{s} W_1(f_N^{(s)}(t), f^{\otimes s}(t)) \rightarrow 0 \text{ as } N \rightarrow \infty,$$

where W_1 denotes the 1-Wasserstein distance and f is the solution to the homogeneous Boltzmann equation

$$\partial_t f = Q(f, f).$$

Furthermore, the relaxation toward equilibrium as $t \rightarrow \infty$ is uniform with respect to the number N of particles:

$$\frac{1}{s} W_1(f_N^{(s)}(t), M^{\otimes s}) \rightarrow 0 \text{ as } t \rightarrow \infty,$$

where M is the Maxwellian with the same moments as f_0 .

The method of proof actually shares many similarities with a former work by Grünbaum [16]. Mouhot and Mischler have developed an abstract method that reduces the question of propagation of chaos to that of proving a purely functional estimate on generator operators (consistency estimates), along with differentiability estimates on the flow of the nonlinear limit equation (stability estimates). In particular, they have then been able to exploit dissipativity at the level of the mean-field limit equation rather than at the level of the particle system.

The rate of convergence is thus obtained as the sum of the initial errors due to both the lack of factorisation and the empirical sampling, and the error on the generators.

Propagation of chaos and dissipation

Assuming that the initial datum is entropically chaotic

$$\frac{1}{N} S(f_{N,0} | \gamma_N) \equiv -\frac{1}{N} \int \log(f_{N,0} / \gamma_N) d f_{N,0} \rightarrow S(f_0 | M_\beta),$$

where γ_N is the uniform probability measure on some energy surface and M_β is the Gaussian equilibrium with the same energy, one actually has the propagation of entropic chaos

$$\frac{1}{N} S(f_N | \gamma_N) \rightarrow S(f | M_\beta).$$

Since the functional $N^{-1} S(f_N | \gamma_N)(t)$ is monotonically increasing in time for the Markov process, one obtains directly a proof of Boltzmann's H-theorem in this context:

$S(f | \gamma)(t)$ is a non-decreasing function of t .

As for the block summation process studied by Carlen and Soffer (see Paragraph 1.3), this increase can be quantified if the Fisher information of the initial data is bounded

$$\int |\nabla_v \sqrt{f_0}|^2 dv < +\infty.$$

The propagation of chaos is therefore directly related to the dissipation mechanism, which has been forced by introducing randomness in the microscopic dynamics.

3 A deterministic result on the propagation of chaos

The situation is completely different for the deterministic dynamics of hard spheres because, although singular, this is an Hamiltonian system without any dissipation. Recall that, for fixed N and ϵ , all the collision parameters (time, pair of colliding particles and deflection angle) are prescribed by the pre-collision configuration. The randomness appears in the limit when the spatial micro-scale ϵ is squeezed. More precisely, the randomness of the initial data (which can be reinterpreted as some uncertainty on the initial state) is expected to be transferred to the dynamics.

The main assumption here is that the hard spheres are initially "independent" and identically distributed, meaning that

$$f_{N,0} = \frac{1}{Z_N} f_0^{\otimes N} \prod_{1 \leq i < j \leq N} \mathbf{1}_{|x_i - x_j| > \epsilon},$$

for some probability density f_0 such that

$$f_0(x, v) \leq \exp\left(-\mu - \beta \frac{|v|^2}{2}\right).$$

Because of the non-overlapping condition, independence is not satisfied for fixed radius ϵ . Depending on the scaling and on the dimension, it may even be that the distribution $f_{0,N}$ is highly concentrated on a very small subset of the phase space:

$$-\log Z_N = O(N^2 \epsilon^d).$$

Independence is only recovered in the limit $N \rightarrow \infty, N \epsilon^d \rightarrow 0$ for any fixed marginal (see Theorem 2):

$$f_{N,0}^{(s)} \rightarrow f_0^{\otimes s}.$$

The low density limit

In order for each particle to exchange a macroscopic quantity of energy (and momentum), the mean free time has to be of the order of $O(1)$. A computation due to Maxwell shows that if one has N spherical obstacles of diameter ϵ in a unit volume, the typical mean free time for a particle of energy E is $1/(N \epsilon^{d-1} \sqrt{E})$. The regime to observe some non-trivial dynamics, expressing a balance between the transport and the collision phenomena, is therefore Boltzmann-Grad scaling $N \epsilon^{d-1} = \alpha$ [15].

The starting point to analyse this low density limit is the Liouville equation relative to the dynamics of N hard spheres

$$\partial_t f_N + \sum_{i=1}^N v_i \cdot \nabla_{x_i} f_N = 0,$$

with the non-overlapping condition encoded in the domain

$$\mathcal{D}_N = \{(x_i, v_i)_{1 \leq i \leq N} / \forall i \neq j, |x_i - x_j| > \epsilon\}$$

and specular reflection on $\partial \mathcal{D}_N$

$$\begin{aligned} f_N(t, \dots, x_i, v_i, \dots, x_i + \epsilon n, v_j, \dots) \\ = f_N(t, \dots, x_i, v_i', \dots, x_i + \epsilon n, v_j', \dots). \end{aligned}$$

The classical strategy to obtain asymptotically a kinetic equation such as the Boltzmann equation is to write the evolution equation for the first marginal of the distribution function f_N . Using Green's formula,

$$\partial_t f_N^{(1)} + v \cdot \nabla_x f_N^{(1)} = (N-1) \epsilon^{d-1} C_{1,2} f_N^{(2)} \quad \text{in } \mathbf{R}_+ \times \mathbf{T}^d \times \mathbf{R}^d,$$

with

$$\begin{aligned} & (C_{1,2}f_N^{(2)})(t, z_1) \\ & := \iint n \cdot (v_1 - v) f_N^{(2)}(t, x, v, x + \epsilon n, v_1) dndv_1 \\ & = \iint (n \cdot (v_1 - v))_+ f_N^{(2)}(t, x, v', x + \epsilon n, v'_1) dndv_1 \\ & \quad - \iint (n \cdot (v_1 - v))_- f_N^{(2)}(t, x, v, x + \epsilon n, v_1) dndv_1, \end{aligned}$$

using the boundary condition to express the gain term in terms of pre-collision velocities.

This equation is very similar to the Boltzmann equation, except that it involves the second marginal, which is not known a priori, to satisfy the chaotic assumption

$$f_N^{(2)}(t, z_1, z_2) \sim f_N^{(1)}(t, z_1) f_N^{(1)}(t, z_2),$$

denoting $z_i = (x_i, v_i)$.

In order to obtain a closed system, a hierarchy of equations is needed, called the BBGKY hierarchy, involving all the marginals of f_N :

$$\begin{aligned} \partial_t f_N^{(s)} + \sum_{i=1}^s v_i \cdot \nabla_{x_i} f_N^{(s)} \\ = \alpha \left((N-s) \epsilon^{d-1} \alpha^{-1} \right) C_{s,s+1} f_N^{(s+1)} \quad \text{in } \mathbf{R}_+ \times \mathcal{D}_s, \end{aligned}$$

with specular reflection on \mathcal{D}_s .

It can be formally checked that, in the limit $N \rightarrow \infty$, $\epsilon \rightarrow 0$ with $N\epsilon^{d-1} = \alpha$, the limiting hierarchy

$$\partial_t f^{(s)} + \sum_{i=1}^s v_i \cdot \nabla_{x_i} f^{(s)} = \alpha \bar{C}_{s,s+1} f^{(s+1)} \quad \text{in } \mathbf{R}_+ \times (\mathbf{T}^d \times \mathbf{R}^d)^s,$$

referred to as the Boltzmann hierarchy, admits a particular solution $f^{(s)} = f^{\otimes s}$, provided that f is a solution to the nonlinear Boltzmann equation

$$\partial_t f + v \cdot \nabla_x f = \alpha Q(f, f).$$

The propagation of chaos will therefore result from a uniqueness argument for the Boltzmann hierarchy.

Convergence to the Boltzmann equation

This strategy has been successfully implemented by Lanford [21], who proved the convergence to the Boltzmann equation and consequently the propagation of chaos for short times.

Theorem 5 (Lanford). Consider N hard spheres on $\mathbb{T}^d \times \mathbb{R}^d$, initially distributed according to $f_{0,N}$.

Then, in the Boltzmann-Grad limit $N \rightarrow \infty$, $\epsilon \rightarrow 0$ with $N\epsilon^{d-1} = \alpha$, the distribution of s typical particles $f_N^{(s)}$ converges almost everywhere to $f^{\otimes s}$, where f is the solution to the Boltzmann equation

$$\partial_t f + v \cdot \nabla_x f = \alpha Q(f, f)$$

on a short time interval $[0, T^*(\beta, \mu)/\alpha]$.

The main drawback of this result is the time of validity of the approximation, which happens to be a fraction of the mean free time. In particular, on this time scale, one cannot observe any relaxation to thermodynamic equilibrium, so that no fluid description may be relevant. This restriction on the time of convergence is not only technical; it also corresponds to the time on which the limiting equation is expected to be well-posed in weighted L^∞ spaces. In such spaces, no advantage

can be taken of the cancellations between the gain and loss terms in the collision operator. The lifespan is therefore more or less the same as for the equation $\dot{F} = \alpha F^2$.

The proof of Lanford relies on a priori estimates that are obtained following the very same lines, except that the fixed point argument holds in a much more complicated functional space, since all marginals $(f_N^{(s)})_{s \leq N}$ have to be controlled simultaneously. Once these uniform bounds have been established, the idea is to use some generalised Taylor expansion to express the solution to the BBGKY hierarchy as a series of operators acting on the initial data. For short times, this series is uniformly convergent and it is therefore enough to study the convergence as $\epsilon \rightarrow 0$, $N \rightarrow \infty$ of each elementary term.

Small errors are introduced by the prefactors $(N-s)\epsilon^{d-1}\alpha^{-1}$ and by the micro translations ϵn in the collision integrals but the main difficulty comes from the fact that the transport in \mathcal{D}_s does not coincide with free transport. Solutions of the Boltzmann equation will therefore provide a good approximation of the deterministic dynamics as long as there is no recollision (i.e. no collision between two particles that belong to the same collision tree). The probability of these recollisions can be estimated by a geometric argument and is proved to vanish in the limit $\epsilon \rightarrow 0$. This part of the argument does not provide any restriction on the time interval.

Note that, in this strategy, chaos is prescribed initially and collisions, because they induce some very weak correlations between the particles, seem to destroy it (at least partially). This means that the mixing effects of collisions are completely neglected.

Correlations and dissipation

So far, the only way to see the cancellations between the gain and loss terms in the collision operator is the existence of invariant measures. A natural idea is then to look at small fluctuations around such an equilibrium and try to extend the time of convergence. More precisely, in [4], the global bound is used on some ‘‘linearised’’ relative entropy to get a quasi-global convergence result:

Theorem 6 (Bodineau, Gallagher & Saint-Raymond). Consider N hard spheres on $\mathbb{T}^2 \times \mathbb{R}^2$, initially close to equilibrium $M_{N,\beta} = \frac{1}{Z_N} \mathbf{1}_{\mathcal{D}_N} M_\beta^{\otimes N}$ with fluctuation

$$\delta f_{N,0}(x, v) = M_{N,\beta} \sum_{i=1}^N g_0(z_i),$$

with g_0 a Lipschitz function such that $\int M g_0(z) dz = 0$.

Then, in the Boltzmann-Grad limit $N \rightarrow \infty$, $\epsilon \rightarrow 0$ with $N\epsilon^{d-1} = \alpha$, the fluctuation $\delta f_N^{(s)}$ converges almost everywhere to $M_\beta^{\otimes s} \sum_{i=1}^s g(t, z_i)$, where g is the solution to the linearised Boltzmann equation

$$\partial_t g + v \cdot \nabla_x g = -\alpha \mathcal{L}_M g, \quad \text{with } \mathcal{L}_M g = -\frac{2}{M} Q(M, M g),$$

uniformly on a time interval of the type $[0, C \log \log \log N/\alpha]$.

The main idea is to introduce a sampling procedure to control the growth of collision trees.

The linearised entropy bound (which is uniform in both N and t)

$$\frac{1}{N} \int \frac{f_N^2}{M_{N,\beta}} dZ_N \leq C_0$$

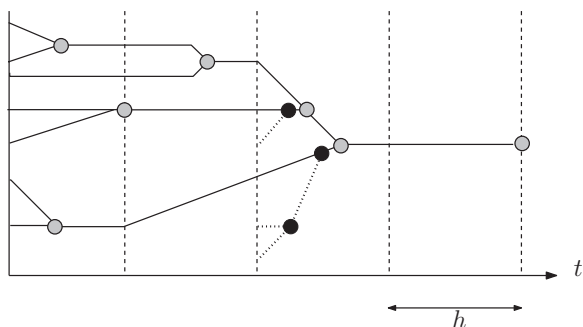


Figure 3. Superexponential collision trees

is then used to kill the contribution of superexponential collision trees, i.e. collision trees with more than 2^k collisions in the k -th time interval. In other words, the expansion is iterated back to the initial time only if it does not involve too many collision operators.

The main technical difficulty in applying this strategy is that the uniform bounds typically involve L^2 spaces, for which the collision integrals are not well defined. Exchangeability is therefore needed to more precisely describe the structure of the cumulants:

$$g_N^m(Z_m) := \sum_{k=1}^m (-1)^{m-k} \sum_{\sigma_k \in \mathfrak{S}_m^k} \frac{f_N^{(k)}(Z_{\sigma_k})}{M_{\beta}^{\otimes k}},$$

where \mathfrak{S}_m^k is the set of all parts of $\{1, \dots, m\}$ with k elements. Its cardinal is denoted by C_m^k .

The crucial inequality is

$$\|g_N^{(1)}(t)\|_{L^2(Mdz)}^2 + \sum_{m=2}^N \frac{C_m^m}{N} \|g_N^{(m)}(t)\|_{L^2(M^{\otimes m}dZ_m)}^2 \leq C \|g_0\|_{L^2(Mdz)}^2.$$

It is very reminiscent of the entropy inequality for the linearised Boltzmann equation

$$\|g(t)\|_{L^2(Mdz)}^2 + 2\alpha \int_0^t \int M g \mathcal{L}_M g(s, z) dz ds \leq \|g_0\|_{L^2(Mdz)}^2.$$

In particular, the cumulants seem to play a similar role to the dissipation in the limiting equation.

This is consistent with the fact that deterministic dynamics is not dissipative. The dissipation comes from the description given to this dynamics and not from the dynamics itself: at each collision, part of the information is lost since the correlations are just forgotten. This seems to indicate a very strong link with information theory.

4 Chaos and turbulence

However, the case of fluctuations around equilibrium is somehow specific, as it is characterised by the fact that the entropy is very close to its maximum. In particular, it implies that the correlations have a very fast decay, typically as powers of $1/\sqrt{N}$. This is one of the key arguments to control the singular integrals.

In the general case of chaotic data, the entropy inequality will also provide a control on the cumulants (with a suitable definition), but without any decay, and in some $L \log L$ functional spaces. As for the limiting equation, a renormalisation process would be needed to define the collision integrals $\bar{C}_{s,s+1}$ (which involve traces on manifolds of codimension d).

The kind of renormalisation that should be convenient here does not appear clearly but it should express the interplay between the different spatial scales.

To conclude, a global picture of what is expected by physicists will now be given (even though it is quite far from the present mathematical understanding of the situation!):

- Transport should introduce some mixing at small spatial scales. More precisely, the distribution of hard spheres is expected to be locally Poisson at scale $\epsilon^{(d-1)/d}$ (which is the typical distance between particles).
- Because of this spatial randomness, the collision process should behave as a stochastic process mixing the velocities (like Kac's process).
- At large spatial scales, transport is then responsible for dispersion. This should prevent spatial concentrations, which are the main obstacle to chaos. This property is also known as hypocoercivity.

Understanding the interactions of these different scales seems to be a challenging programme for the future.

Bibliography

- [1] R. Alexander, *The Infinite Hard Sphere System*, PhD dissertation, Dept. Mathematics, Univ. California, Berkeley, 1975.
- [2] A. R. Barron, *Entropy and the central limit theorem*. Ann. Prob. **14** (1986), 336–342.
- [3] T. Bodineau, I. Gallagher and L. Saint-Raymond. *The Brownian motion as the limit of a deterministic system of hard-spheres*, to appear in *Inventiones* (2015), arXiv:1305.3397.
- [4] T. Bodineau, I. Gallagher and L. Saint-Raymond. *From hard sphere dynamics to the Stokes-Fourier equations: an L^2 analysis of the Boltzmann-Grad limit*, submitted (2015), arXiv:1511.03057.
- [5] L. Boltzmann, *Lectures on gas theory*. University of California Press, Berkeley, 1964. Translated by Stephen G. Brush. Reprint of the 1898 Edition. Reprinted by Dover Publications, 1995.
- [6] E. Borel, *Introduction géométrique à quelques théories physiques*, Gauthiers-Villars, Paris, 1914.
- [7] P. Bálint, N. Chernov, D. Szász and I. P. Tóth, *Multidimensional semidispersing billiards: singularities and the fundamental theorem*, Ann. Henri Poincaré **3**, 451–482.
- [8] L. A. Bunimovich and Ya. G. Sinai, *The fundamental theorem of the theory of scattering billiards*, Math. USSR-Sb. **19**, 407–423.
- [9] E. Carlen and A. Soffer, *Entropy production by block variable summation and central limit theorems*. Comm. Math. Phys. **140** (1991), 339–371.
- [10] C. Cercignani, R. Illner and M. Pulvirenti, *The Mathematical Theory of Dilute Gases*, Springer Verlag, New York NY, 1994.
- [11] N. I. Chernov and Ya. G. Sinai, *Ergodic properties of certain systems of 2D discs and 3D balls*, Russian Math. Surveys **42**, 181–207.
- [12] P. Diaconis and D. Freedman, *A dozen de Finetti-style results in search of a theory*. Ann. Inst. H. Poincaré Probab. Statist. **23** (1987), 397–423.
- [13] I. Gallagher, L. Saint-Raymond and B. Texier. *From Newton to Boltzmann: the case of hard-spheres and short-range potentials*, Zürich Lectures in Advanced Mathematics, EMS Publishing House, 2014.
- [14] C. Graham and S. Méléard, *Stochastic particle approximations for generalized Boltzmann models and convergence estimates*. The Annals of Probability **25** (1997), 115–132.
- [15] H. Grad, *On the kinetic theory of rarefied gases*. Comm. Pure Appl. Math. **2** (1949), 331–407.

- [16] F. A. Grünbaum, *Propagation of chaos for the Boltzmann equation*. Arch. Rational Mech. Anal. **42** (1971), 323–345.
- [17] E. Hewitt and L. Savage, *Symmetric measures on Cartesian products*. Trans. Amer. Math. Soc. **80** (1955), 470–501.
- [18] D. Hilbert. *Begründung der kinetischen Gastheorie* Math. Ann. **72** (1912), 562–577.
- [19] M. Kac, *Foundations of kinetic theory*. In Proceedings of the Third Berkeley Symposium on Mathematical Statistics and Probability, 1954–1955, vol. III (Berkeley and Los Angeles, 1956), University of California Press, 171–197.
- [20] A. Krámli, N. Simányi and D. Szász, *The K-Property of Four Billiard Balls*, Commun. Math. Phys. **144**, 107–148.
- [21] O. E. Lanford, *Time evolution of large classical systems*, Lect. Notes in Physics **38**, J. Moser ed., 1–111, Springer Verlag, 1975.
- [22] P. S. Laplace, *Mémoire sur les approximations des formules qui sont fonctions de très-grands nombres, et sur leur application aux probabilités*, Mémoires de la Classe des sciences mathématiques et physiques de l’Institut de France (1809), 353–415.
- [23] J. V. Linnik, *An information theoretic proof of the central limit theorem with Lindeberg conditions*. Theory Probab. Appl. **4** (1959), 288–299.
- [24] J. C. Maxwell, *On the dynamical theory of gases*. Philos. Trans. Roy. Soc. London Ser. A **157** (1867), 49–88.
- [25] H. P. McKean, *Fluctuations in the kinetic theory of gases*. Comm. Pure Appl. Math. **28** (1975), 435–455.
- [26] S. Mischler and C. Mouhot. *Kac’s program in kinetic theory*. Inventiones **193** (2013), 1–147.
- [27] M. Pulvirenti, C. Saffirio and S. Simonella, *On the validity of the Boltzmann equation for short range potentials*, arXiv:1301.2514.
- [28] D. Ruelle, *Thermodynamic formalism*, Addison Wesley, Reading, Mass., 1978.
- [29] N. Simányi, *Proof of the Boltzmann-Sinai Ergodic Hypothesis for Typical Hard Disk Systems*, Inventiones **154** (2003), 123–178.
- [30] H. Spohn, *Large scale dynamics of interacting particles*, Springer-Verlag **174** (1991).
- [31] A.-S. Sznitman, *Topics in propagation of chaos*. In Ecole d’été de probabilités de Saint-Flour XIX 1989, vol. 1464 of Lecture Notes in Math. Springer, Berlin, 1991, 165–251.
- [32] A. J. Stam, *Some inequalities satisfied by the quantities of information of Fisher and Shannon*. Info. Contr. **2** (1959), 101–112.



Laure Saint-Raymond [laure.saint-raymond@ens.fr] is a professor at UPMC and ENS in Paris. Her research is focused on the asymptotic analysis of problems from fluid mechanics, gas and plasma models. Her main contributions are concerned with the Boltzmann-Grad limit of deterministic systems of particles (with T. Bodineau and I. Gallagher) and hydrodynamic limits of the Boltzmann equation (with F. Golse).

Panel: Challenges for Mathematicians

To conclude the day of celebration of its 25th anniversary, the Executive Board of the European Mathematical Society decided to set up a roundtable to address the current issues that mathematicians face. I was given the task of moderating it. Four broad issues were identified:

1. How mathematicians learn and teach.
2. How mathematicians do mathematics, communicate it and publish it.
3. How mathematicians interact with the ‘outer world’ about their discipline.
4. How mathematicians deal with new trends like big data, etc.

In order to take advantage of the particular expertise of the panel members, while allowing the distinguished and engaged audience to contribute to the debate, it was decided that the time should be equally divided between the four topics, with an initial presentation by a panel member, comments by the others and time left at the end of each exchange for contributions by the audience.

The four issues were covered in order by Ari Laptev, Roberto Natalini, Maria Esteban and Peter Bühlmann, who, later in this article, report on the discussions that took place on each topic.

The overall format chosen for the roundtable allowed an appropriate level of interactivity.

With the contributions from the audience, it was clear that the importance of the issues discussed was unani-

mously recognised but there were diverse opinions on whether the mathematical community was dealing with them properly. Attention to teaching and care taken with research articles were values shared by the mathematicians attending. Efforts to achieve more visibility and understanding in the wider public were more diversely addressed, some pointing to the considerable amount of material already gathered in recent years and the need to make it widely available and others to the considerable gap that still exists with scientists from other disciplines.

The final words were spoken by François Tisseyre, a film director who has made several movies on mathematics by mathematicians over the last 30 years, in particular one on the First European Congress of Mathematics under the title “Mathématiques, mon village”. His view is that, in spite of very valuable efforts by a significant number of mathematicians, the community at large has not yet fully understood what it takes to position itself in the media environment. Nevertheless, he underlined the considerable progress made in the quality of oral presentations at conferences and seminars. He also highlighted the fact that now, in many institutions, technical facilities are available to record lectures, offering the possibility to access them at leisure from repositories and creating a fantastic new resource.

Jean-Pierre Bourguignon
(IHÉS, Bures-sur-Yvette, France)
EMS President 1995–1998



From left to right: Ari Laptev, Maria J. Esteban, Jean-Pierre Bourguignon, Peter Bühlmann, Roberto Natalini

How mathematicians learn and teach

This subject is very complex and it is impossible to cover it completely within the timeframe we have for this roundtable. We have two big problems here: teaching at school and teaching at university level.

The main problem regarding teaching in schools is that it is extremely political. In many countries, teaching is regulated by the government and those who are responsible for it are not always competent enough. Many officials are directly involved in how we are supposed to teach mathematics in schools.

One may compare the results of the education of mathematics in schools with the Pisa study. This relatively recent study was carried out in 2014 and 43 countries were involved. The best results were in countries like Hong-Kong, Singapore and Finland. For example, Finland was placed 12th. Sweden, in contrast, which is culturally very similar to Finland, was placed 6th from bottom.

I remember at one of the meetings of the Royal Swedish Academy of Sciences, the Swedish Minister of School Education making a joke when criticising the previous Swedish government. He mentioned his conversation with the Minister of Education from Finland, who claimed that, in Finland, they did not have any ambition to be the best in Europe or the best in the world. They just wanted to be better than Sweden. The Finnish Government certainly succeeded!

Concerning university level of mathematics education, I have had my own subjective experience by teaching in three different countries: Russia, Sweden and now England. The education in each of these countries is extremely different, not only in terms of the organisation of courses (which is not surprising) but also often in terms of the mathematical content of the courses. For example, in the UK, university professors teach much less than in Sweden and definitely less than in Russia.

At Imperial College London, we have two terms of 10–11 weeks, where we give three hours a week of lectures for undergraduate students, with the result that the students have very little time to meet their professors. To a large extent, the education is reduced to self-education

outlined by the lectures. Of course, there are tutorials where each student is assigned a professor, meeting them every week. However, I am not sure how effective this system is. After all, our knowledge of mathematics is based on what we manage to learn at university. I must say that I am not especially impressed by the current standard of analysis courses in the UK because we simply do not have enough time for them. Other mathematical disciplines probably do not suffer as much as classical analysis.

I am also sure that the organisation of teaching in France, Germany, Italy and other countries is different. I do not want to say which one is better but I think that it would be good if, for example, the EMS would focus on this so that we could try to compare the different experiences. Maybe this could be an idea for the EMS Education Committee.

In recent years, European countries have had to adapt to the Bologna designed programme, in order to ensure comparability in the standards and quality of higher education qualifications. In many countries, there have been numerous protests but, finally, it has been agreed to have three years of undergraduate education. Luckily, some engineering universities have been able to keep a four-year undergraduate programme in order to maintain their own excellent local traditions.

Everybody complains that the quality of university study is deteriorating. This is, of course, partially related to how well students are prepared for university education at high school. However, the level of school education varies depending on the country. There are still some countries where school education is better than in other countries. It would be good to have a study of this area of education too.

In countries with better basic school education, university professors have better syllabuses for their university courses. I believe that mathematics engineering education in Germany, Switzerland and France is still at a higher level compared with some other European countries.

*Ari Laptev
(Imperial College London, UK)
EMS President 2007–2010*

How mathematicians do mathematics, communicate it and publish it

For all these issues, the situation has considerably changed over the last 15 to 20 years. It has now become natural for mathematicians to use various skills and be motivated by problems from other domains. This has considerably blurred the frontier, if there is one, between fundamental and applied mathematicians.

Still, in my opinion, mathematicians are not as present as physicists and biologists in the media and social networking. A survey has shown that, of the general public who are interested in science (already a minority of the whole population), those who show interest in medicine and the environment dominate massively while mathematics remains invisible. This is a sign that the success of mathematics is not considered at the level of society.

What are the causes of this situation? Firstly, there is the fact that mathematics is considered a difficult subject by many people and there is also the absence of a tradition of communicating mathematics to the general public. From the results of a study showing the evolution of media used to access information on science (with very significant improvements over the internet), it is clear that mathematics is still not so present in this media development.

It is a commonly held view that mathematicians have higher publication standards than many other disciplines. Generally, articles are written clearly, with fair representation of the research that has been conducted. This view was challenged by someone in the audience, who mentioned the increasing pressure to publish more, leading to an inflation of publications and a lowering of standards. The disproportionate weight that some publishers have gained was criticised by another person in the audience. Many still felt that the publication situation was much sounder in mathematics than in other disciplines, where bibliometric data strongly drives publication strategies because of the role played in decisions about grants and promotions. The success of repositories such as arXiv and its transformative effect have been mentioned in this area.

Several people in the audience recognised that communication was an important issue, with significant efforts made to have generalist journals regularly publishing articles focusing on mathematics. The community needs to share good practices. It tends to underestimate both the level of effort needed to produce a professional movie and that there is a public out there eager to be confronted with the passion of mathematicians in action (as shown by the success of some recent movies about mathematicians that have had success well beyond what the professionals expected).

The challenge of adapting communication to the public was underlined, beginning for example with the need to propose challenging but 'cool' things for young children at primary school. As there have already been a lot of attempts in this area, people should be encouraged to use what is already available. An excellent example has been set by the interactive exhibit *Imaginary*, which uses free software and allows visitors to take the initiative.

It is clear that some progress is still in order. Several studies showing the high level of impact of mathematics in the economy have recently been published but mathematicians have not been very good at making this known to the general public. Currently, students trained with a good knowledge of mathematics also have the shortest waiting time to become employed. This is also not so well known.

In summary, a change has occurred for the mathematical community since there are now many more interactions with other disciplines and some very successful initiatives in communication to the wider public. However, considerable progress still needs to be made to get to the level of other disciplines.

Roberto Natalini

(Consiglio Nazionale per la Ricerca, Rome, Italy)

Chair of the committee for Raising Public Awareness of Mathematics of the EMS

About the relation of mathematicians with the world-at-large

The organisers of the round table put together for the celebration of the 25th anniversary of the EMS have expressed their wish to briefly discuss the relationship between mathematicians (maybe more precisely European mathematicians) and the world-at-large, i.e. our society and economy. In other words, the question to address is how mathematicians contribute to the general wellbeing and development of our society.

Many centuries ago, mathematics had the goal of solving problems that arose in people's lives. Until the end of the 19th century, practically all important developments in mathematics were linked to the search for solutions to concrete problems. However, with the advent of the 20th century, a large segment of mathematics began to follow its own internal logic and to focus on internal needs. This shift caused parts of mathematics to be removed from practical needs or applications.

Nevertheless, as several recent studies on the socio-economic impact of mathematics in the UK, the Netherlands and France have shown, an important part of the economy depends on high-level mathematics (though not necessarily and directly on mathematicians). In the most recent study, focusing on France, it was shown that 15% of the GDP and 9% of existing jobs rely on high-level mathematics. Similar percentages are mentioned in the British and Dutch studies, despite the fact that these three countries differ considerably in the size and make-up of their economic and industrial sectors.

How do mathematicians contribute to this big success? And how could they contribute more or better? Another recent study carried out in France estimates that approximately 10% of mathematicians work for companies or work to address society's problems. This percentage seems difficult to beat. As companies continue to appreciate more and more the importance and ben-

efits of mathematics, one major concern is what will happen when there are not enough mathematicians ready to answer their questions? It has been estimated that over the next 10 years, twice as many mathematicians will be needed – that is 20% – than are currently involved in this kind of activity. This number relates to France. In other countries the discrepancy could be even worse. So, what are the main difficulties that we face in meeting future demands?

One very important obstacle is the lack of recognition that this kind of mathematical activity receives within our community. Discussions in important committees focus on issues of excellence and, specifically, on what and where to publish. These are very appropriate issues, of course, but the utility of the research or work that is performed should also be recognised by funding and legislative institutions and by the mathematical community at large. This is currently far from being the case! A mathematician's performance and excellence should not be linked solely to publications. The evaluation of research and mathematical work should be based on a variety of criteria. The quality of publications is important; however, in some cases, the extent to which the work contributes to the resolution of important industrial or societal problems should also be considered and valued. One only has to sit on a committee comprised of mathematicians with the task of deciding whom to hire, or on whom to bestow an important award or grant, and it quickly becomes clear how little recognition there is for very applied mathematical work! Therefore, working in industrial mathematics is a risky choice because it may not advance your career. A well established mathematician can devote time to this kind of work or activity, since there is little risk to their career; however, they should think carefully before pushing students into applied fields, unless their main aim is to work for a company.

Another obstacle is that many mathematicians may, in principle, be open to working on applied problems but do not realise that the mathematical tools they know and are familiar with could be relevant to these problems. Testimonials, examples and success stories could be of great help here. It seems more and more clear that most, if not all, fields of mathematics can contribute to solving concrete problems. Unfortunately, this is not common knowledge among mathematicians.

Well-adapted solutions to these issues may be underway. In many European countries (14 at the moment, and the number is growing), new groups affiliated with the European network EU-MATHS-IN (www.eu-maths-in.org) are trying to build bridges between academic mathematicians and companies (especially small and medium-sized enterprises). Some of these national branches have been lucky to be funded and thus are able to count on employees and collaborators to assist in the main tasks of the network. The national networks of EU-MATHS-IN differ in their organisational structures but their aims are the same: to increase and improve the interface between academic mathematics and the world of large, medium and (especially) small enterprises. The final aim of EU-MATHS-IN is to become a European infrastructure at

the service of companies and academic mathematicians, to become a one-stop-shop for companies looking for mathematicians to provide specific services or to become their employees, consultants or collaborators. The EMS was one of the promoting members of EU-MATHS-IN; the other was the ECMI, the European Council for Mathematics in Industry. The mathematical community as a whole should be interested in the development of these institutions as they are working to increase the impact and visibility of mathematics in society. This effort will be good for our societies and economies; it will also be important for the scientific community, since it will help to attract more funding, justify the creation of more academic jobs and open new opportunities for our students in their search for jobs.

Maria J. Esteban
(CNRS and Université Paris-Dauphine, France)
*President of the International Council for
Industrial and Applied Mathematics (ICIAM)*

Mathematics, Statistics and Data Science

The process of extracting information from data has a long history (see, for example, [1]) stretching back over centuries. Because of the proliferation of data over the last few decades, and projections for its continued proliferation over coming decades, the term *Data Science* has emerged to describe the substantial current intellectual effort around research with the same overall goal, namely that of extracting information. The type of data currently available in all sorts of application domains is often massive in size, very heterogeneous and far from being collected under designed or controlled experimental conditions. Nonetheless, it contains information, often *substantial* information, and data science requires new interdisciplinary approaches to make maximal use of this information. Data alone is typically not that informative and (machine) learning from data needs conceptual frameworks. Mathematics and statistics are crucial for providing such conceptual frameworks. The frameworks enhance the understanding of fundamental phenomena, highlight limitations and provide a formalism for properly founded data analysis, information extraction and quantification of uncertainty, as well as for the analysis and development of algorithms that carry out these key tasks. In this personal commentary on data science and its relations to mathematics and statistics, we highlight three important aspects of the emerging field: Models, High-Dimensionality and Heterogeneity, and then conclude with a brief discussion of where the field is now and implications for the mathematical sciences.

Models

Mathematical models provide a conceptual framework within which to interpret data. A well-established connection between models and data is provided by the statistical approach in which the primary task is the inductive inference from data to draw conclusions about

unknown model parameters or structures. This is the process of blending models with data. The manner in which the model and the data are linked, and the relative belief in the accuracy of the model and the data, play important roles in this blending process. One class of examples are the complex models arising from Newton's laws, such as those governing the Earth's atmosphere for use in weather prediction. This field (at current levels of computer resolution) involves models with billions of state variables, which are confronted with datasets of millions of measurements at regular intervals several times each day – this is the process of data assimilation [2]. These problems, although increasingly data rich, are very model-driven, with a belief in Newton's laws providing a very strong constraint on the task of interpreting the data. At the other extreme are problems that are primarily data-driven and in which the model arises from the data rather than being a constraint – for example deep learning in image classification [3]. Matrix completion for the Netflix problem [4] is another example of a primarily data-driven application in which the model is not based on any fundamental modelling principles. Between these two extremes of data-driven and model-driven inference are numerous applications in biology and the social sciences in which cartoon models are used, such as the SIR models [5] describing the transmission of infectious diseases or continuum flow models for crowds [6]; in these disciplines, the models are significant constraints on the data but do not have the pivotal position that Newton's laws play in some application areas. In this discussion of model-driven versus data-driven procedures, and the spectrum in between, it is important to appreciate that whilst purely data-driven procedures might be appropriate for the task of forecasting or prediction, they do not provide the additional “mechanistic” or “causal” insights that arise when incorporating data into Newton's laws, for example. Indeed, in fields that are currently data-driven, it can be expected that mechanistic models will emerge as the data provides information about the fundamental mechanisms at play. In particular, this suggests that whilst the mathematical models of the last few centuries are “pencil and paper” models, the next few decades may open up new paradigms for mathematical modelling based around “machine-learned” models that reside in computer memory and are organised around fundamental principles that emerge from the data.

High-Dimensionality

The topic of “high-dimensionality” arises in two important ways: through the size of the dataset and through the size of the model, as indicated in the examples described above. For high dimensional models, important questions relate to the ability of algorithms to scale to arbitrarily high, even infinite dimensional, formulations [7, 8] of the statistical inference problem. Another key development in high dimensional statistics is based on the concept of sparsity, which has proven to be remarkably successful in many applications, including the highly celebrated compressed sensing methodology [9, 10] and its noisy version, in which stochastic error terms are su-

perimposed on the observed signal. The mathematical underpinning and understanding of high-dimensional statistical inference (see [11] and [12]) has evolved almost simultaneously with practical applications.

Early examples of high-dimensional problems arose in genomics in the late 1990s when relating disease status to the genetic profile of a person [13]. When measuring many biomarkers (expressions of many genes in the genome), for example around ten thousand in the early times of such applications, a model would typically involve (at least) one unknown parameter for every measured variable, encoding an unknown effect of the biomarker to the disease status. And thus, there is immediately an inference problem with ten thousand unknown parameters to be estimated from about one hundred people participating in a well-designed study. Successful models, classification and even causal inference techniques have been built in statistics and bioinformatics at the interface between molecular and computational biology. Nowadays, genetic profiles are measured with millions of biomarkers and, instead of a well-defined single study, there are huge health databases containing information from very many people. New problems that arise include privacy issues and heterogeneity; the latter is discussed in the following paragraph.

Heterogeneity

With growing data volume, one might reasonably expect an increased sample size. But these large datasets that are now routinely available are usually not collected from well-designed experiments and they are often rather heterogeneous. They might exhibit unwanted time trends, variation or sub-population structures or arise from different sources like satellites, aircraft and weather balloons for weather prediction. When partitioning the massive data into fairly homogeneous groups (which, without further information, is a difficult task in statistical mixture or change point modelling), this often leads to severe high-dimensional problems in which the sample size within a homogeneous group is rather small in comparison to the dimensionality of the unknown model parameters. New avenues of investigation are required to tackle fundamental problems relating to heterogeneity in large-scale data. This is an area where new input is needed from mathematics and statistics because naive design and use of standard algorithms does not lead to accurate information extraction.

Where Are We Now?

Data science is clearly emerging as an identifiable research area of enormous importance, dealing with large-scale data problems in many application areas such as biology and medicine (epidemics, genetics and genomics, neuroscience), engineering (imaging, signal processing), geophysical sciences (climate, weather, the Earth's subsurface and numerous energy applications), the social sciences (economics, ranking and voting, crowd sourcing) and commerce (Amazon, Google, Netflix), to name just a few. Whether data science will become a distinct academic discipline in the way that computer

science did in the 1950s remains to be seen. But, clearly, the subjects of mathematics and statistics have very close relations to data science, whatever form it takes. Statistics has a longstanding tradition and an established framework for quantifying uncertainties and this in turn helps to address substantial problems of replicability in data-driven science. Mathematics has a unique position to contribute to the foundations in information and data science. Whilst avoiding claims that mathematics and/or statistics should “own large parts” of data science, it is clear that we should embrace others who participate in the endeavour and the intellectual challenges that stem from doing so. Data science is certainly stimulating new and exciting mathematics and statistics. As a consequence, education in the mathematical sciences should incorporate more in-depth training in computing, mathematical modelling and statistical thinking, in the context of data-rich applications and theoretical paradigms.

References

- [1] S.M. Stigler. *The History of Statistics: The Measurement of Uncertainty before 1900*. Belknap Press/Harvard University, 1986.
- [2] S. Reich and C. Cotter. *Probabilistic Forecasting and Bayesian Data Assimilation*. Cambridge University Press, 2015.
- [3] J. Schmidhuber. Deep learning in neural networks: an overview. *Neural Networks*, 61: 85–117, 2015.
- [4] E.J. Candes and B. Recht. Exact matrix completion via convex optimization. *Foundations of Computational Mathematics*, 9: 717–722, 2009.
- [5] W.O. Kermack and A. G. McKendrick. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London A*, 115: 700–721, 1927.
- [6] R.L. Hughes. A continuum theory for the flow of pedestrians. *Transportation Research Part B*, 36: 507–535, 2002.
- [7] M. Dashti and A. M. Stuart. The Bayesian Approach to Inverse Problems. Springer Handbook on Uncertainty Quantification, to appear. arxiv:1302.6989.
- [8] S.L. Cotter, G.O. Roberts, A.M. Stuart and D. White. MCMC methods for functions: modifying old algorithms to make them faster. *Statistical Science*, 28: 424–446, 2013.
- [9] D.L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, 52: 1289–1306, 2006.
- [10] E.J. Candes and T. Tao. Near-optimal signal recovery from random projections: Universal encoding strategies? *IEEE Transactions on Information Theory*, 52: 5406–5425, 2006.
- [11] P. Bühlmann and S. van de Geer. *Statistics for High-Dimensional Data. Methods, Theory and Applications*. Springer Verlag, Series in Statistics, 2011.
- [12] T. Hastie, R. Tibshirani and M. J. Wainwright. *Statistical Learning with Sparsity: the Lasso and Generalizations*. Chapman and Hall/CRC Press, Series in Statistics and Applied Probability, 2015.
- [13] T.R. Golub et al. Molecular Classification of Cancer: Class Discovery and Class Prediction by Gene Expression Monitoring. *Science*, 286: 531–537, 1999.

*Peter Bühlmann
(ETH Zürich, Switzerland) and
Andrew M. Stuart
(Warwick University, Coventry, UK)*

A.M. Stuart is grateful to DARPA, EPSRC, ERC and ONR for financial support that led to some of the research underpinning this article.



New journal published by the
European Mathematical Society

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



ISSN print 2415-6302
ISSN online 2415-6310
2017. Vol. 1, 4 issues
Approx. 400 pages
17.0 cm x 24.0 cm
Price of subscription:
198 € online only
238 € print+online

Editor-in-Chief
Mark Sapir (Vanderbilt
University, Nashville, USA)

Editors

Goulnara Arzhantseva (University of Vienna, Austria)
Frédéric Chapoton (CNRS and Université de Strasbourg, France)
Pavel Etingof (Massachusetts Institute of Technology, Cambridge, USA)
Harald Andrés Helfgott (Georg-August Universität Göttingen, Germany and Centre National de la Recherche Scientifique (Paris VI/VII), France)
Ivan Losev (Northeastern University, Boston, USA)
Volodymyr Nekrashevych (Texas A&M University, College Station, USA)
Henry K. Schenck (University of Illinois, Urbana, USA)
Efim Zelmanov (University of California, San Diego, USA)

Aims and Scope

The *Journal of Combinatorial Algebra* is devoted to publication of research articles of the highest level. Its domain is the rich and deep area of interplay between combinatorics and algebra. Its scope includes combinatorial aspects of group, semigroup and ring theory, representation theory, commutative algebra, algebraic geometry and dynamical systems. Exceptionally strong research papers from all parts of mathematics related to these fields are also welcome.

Bitcoin and Decentralised Trust Protocols

Ricardo Pérez-Marco (CNRS, Université Paris 13, France)

Bitcoin is the first decentralised peer-to-peer (P2P) electronic currency. It was created in November 2008 by Satoshi Nakamoto, the pseudonym of the anonymous author or group of authors of the associated groundbreaking article [1]. Nakamoto released the first implementation of the protocol in open source client software [2], bringing about the genesis of bitcoins on 9 January 2009. The bitcoin protocol is based on clever ideas that solve a form of the Byzantine Generals Problem and sets the foundation for Decentralised Trust Protocols. Still in its infancy, the currency and the protocol have the potential to disrupt the international financial system and other sectors, where business is based on trusted third parties. The security of the bitcoin protocol relies on strong cryptography and one-way hashing algorithms.

1 Electronic decentralised money

Progress in cryptography has made possible secure communications and electronic payments over the internet. The use of a credit card is a form of electronic cash that relies on a trusted third party, preventing overspending or double spending. The remarkable main contribution of the bitcoin protocol is to get rid of trusted third parties and establish a pure peer-to-peer (P2P) decentralised currency.

Our national currencies rely on the central banks, which have the power to regulate the monetary mass. These central authorities are not always public institutions like the Federal Reserve. In the last decade, the European Central Bank (ECB) has taken over national central banks in the European Union. The ECB claims its independence from national governments in order to set monetary policy. Unfortunately, the role of the ECB is not politically neutral, as seen in the recent Greek crisis. The elected Greek government came under pressure from the ECB when it deprived Greek banks of liquidity. Whoever owns the key to the printing press has tremendous economic and political power.

A decentralised form of money has existed for several thousand years. Precious metals like gold and silver are decentralised. Value is widely acknowledged because of scarcity and physical properties. The “barbarous relic” (quoted from J. M. Keynes’, making reference to the gold standard) has been the “canonical” form of money since ancient times. From cuneiform clay tablets [3], we know that precious metals were already used in Mesopotamia circa 2600 B.C. There was an evolution in Europe during the 18th century when bank notes were introduced by John Law (paper and leather money appeared even earlier in China [4]). These were backed by gold and silver (and land). Prior to modern times, there was a world monetary bimetalism (during the Roman Empire, Aureus and Denarius coins were used). This generated monetary tensions

due to the fluctuations of one metal with respect to the other but it produced a subtle monetary equilibrium (see [5]) that could be disrupted by fixing the wrong exchange rate. This happened in 1717 when Isaac Newton, then Master of the British Royal Mint, set an incorrect gold/silver ratio, imposing a de facto gold standard. After 1870, with the withdrawal of the stabilising role of the Banque de France (which was unable to sustain the gold/silver ratio at 15.5. A 20 French Franc gold Napoleon coin contains 5.81 grams of pure gold whilst the 5 French Franc silver coin contains 22.5 grams of pure silver), there was an emergence of a world gold standard and gold became the world currency. National currencies were then backed by gold reserves and the dynamics between competing currencies obeyed the *Copernicus-Gresham Law* (stated by Copernicus [6] and earlier by Oresme [7]).

Copernicus-Gresham Law. *Bad money drives out the good.*

This means that if two kinds of money are available, people prefer to use or spend “bad” money and hoard “good” money.

Historically, the gold standard was gradually abandoned during the 20th century, until 1971 when the convertibility of the American dollar into gold was withdrawn (Nixon shock) in favour of a floating currency system. Then, national currencies became “fiat” money, backed only by faith in the issuing central banks and governments.

The motivation behind bitcoin creators is to create a form of “electronic gold”, whose integrity and non-falsifiability relies on mathematical properties, instead of physical properties for gold or faith in central banks for fiat money. But how is this even possible when a digital token can be replicated exactly, infinitely and at no cost? It would be like being able to produce gold easily, jeopardising the scarcity and non-falsifiability properties that make it valuable. On the other hand, the electronic nature makes it perfect for storage and transportation. The main obstacle is to prevent the possibility of “double spending”, i.e., the simultaneous use of the same token for different payments. At first, “decentralisation” and “electronic” seem to be incompatible goals. The “double



Figure 1. Old and new decentralised money blended together into a one ounce silver coin

spending problem” is the main difficulty in the inception of decentralised electronic money.

The only way to prevent double spending is to have a ledger accounting for all transactions, so that the recipient can check that the transaction is legitimate. If we don’t want this ledger to be centralised under the control of a third party then it must be public. This argument shows that all transactions must be publicly recorded (maybe in an obfuscated form).

Transparency Theorem. *Electronic decentralised money must rely on a public ledger.*

Once this is accepted, the major problem is how to construct a trusted public ledger, that is, how to build a reliable, non-falsifiable public database of approved transactions. This is not a simple task. For bitcoin, this public ledger is a file or a set of files called “the blockchain”, which contains a chronological sequence of blocks cryptographically bundled together with all bitcoin transactions.

2 Byzantine Generals and Sybil attacks.

The core of the problem is to establish a decentralised mechanism for trust consensus. A centralised “trust” stamp is only as good as the confidence put in the third party who validates that trust. Therefore, decentralised trust consensus, if possible, is stronger and more resilient. This is a good example of “Taleb antifragile structure” [8], since it benefits from the erosion of centralised systems. It is an intricate (Byzantine!) problem to devise such a mechanism of validation. This “Trust Machine” (as presented on the cover page of a recent issue of “The Economist” [9]) is the core of the bitcoin protocol.

It cannot be ignored that some agents may act maliciously, it cannot be assumed that the communications are secure and it cannot be controlled who participates in the open community.

This type of problem was first systematically studied in 1982 [10]. Lamport named it “The Byzantine Generals Problem” in the context of computer systems. The goal is to handle malfunctioning or malicious components that give conflicting information to different parts of the system.

The Byzantine Generals Problem

The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

The problem of reaching a consensus in an open network is similar but more complex: the number of generals is not fixed. In this more general “Nakamoto Byzantine Generals Problem”, there must be prevention of pseudospoofing or Sybil attacks, which consist of the creation of multiple fake identities in order to subvert the reputation of the system. The safeguard against this form of attack is to request that the participation or share of influence in the system has a cost. Thus, a malicious attacker would need important resources. Nakamoto’s proposal is to make the influence of each participant propor-

tional to the share of computer power that he contributes to secure the system. The idea of “Proof of Work” (PoW) was used by Adam Back with *Hashcash* (1997) to fight spam. The first implemented cryptocurrency using a PoW was Hal Finney’s RPOW. Other earlier proposals were from Wei Dai with *b-money* (1998) and Nick Szabo with *Bit Gold* (1998). According to Nakamoto (bitcointalk 2010): “*Bitcoin is an implementation of Wei Dai’s b-money proposal on Cypherpunks in 1998 and Nick Szabo’s Bitgold proposal.*”

The network is secure as long as the majority of the computer power comes from honest players.

3 Nakamoto decentralised consensus

The process of validating bitcoin transactions safeguards against double spending and it works as follows. The bitcoin net consists of nodes that connect P2P to each other and propagate the transactions (as in Figure 2). The typical client connects to at least eight other peers. Each node checks that the transactions are valid and respect the rules of the protocol (the code is public [11]). Some of these nodes are “miners” or validators of transactions. They collect transactions into a block of transactions. A hashing algorithm digests any file into a fixed length string of bits (more on hashing algorithms below). Miners add the hash of the header of the previously validated block and some other data (timestamp, number of transactions, etc.) in order to build the new block header. Varying a nonce, they try to find a hash of the block header starting with a certain number of zero bits. This number sets the difficulty of the problem and is adjusted every 2016 blocks in a function of the total hashing power so that a solution is found in about 10 minutes on average. This procedure is a sort of “decentralised lottery” that designates the miner that validates the blocks. The “winner” earns a reward in newly created bitcoins. The winning probability is proportional to the computer power provided. The validated block is propagated through the network, which checks that the solution is correct and that the block does not contain double spends.

The miners hash the header of the block but not the whole block. To ensure incorruptibility of the transactions, the root of a Merkle hash tree (more on Merkle trees below) of the transactions is added to the header.

A race starts when two or more blocks are validated simultaneously in different parts of the net. Then, some miners accept one and some accept the other one as the next valid block. In further validations, one of the two groups will be faster. Then, all miners switch to the longest blockchain and



Figure 2. Worldwide propagation of a bitcoin transaction

the race stops. This creates what are called “orphan blocks”, which are off the blockchain and invalid.

The miner validating the block gets a reward in bitcoins. This was first set to be 50 bitcoins and the reward is halving about every four years (or, more precisely, after 210,000 blocks). At the time of writing, the reward is 25 bitcoins and by July 2016, after block number 420,000, the reward will drop to 12.5 bitcoins.

Apart from this mining reward, miners can get fees from each transaction. Fees are voluntary and up to the user, and are typically zero or very low. But a higher fee incentivises the miners to include the transaction with priority in the next block. Thus, a higher fee ensures that a transaction is processed faster.

The production of bitcoins slows down in a geometric way. At the time of writing, the total number of bitcoins in existence is over 15 million. By 2140, a total of 21 million bitcoins will exist and no more will be produced. The growth of the monetary mass is programmed into the algorithm. Each bitcoin can be divided into 100 million units called “satoshis”, i.e., eight digits can be used. This makes the currency extremely divisible and well suited for micropayments. The model of production and the scarcity imposed is inspired from mining gold.

Hashing algorithms

A hashing algorithm digests any file into a fixed length string of bits. The slightest modification of the original file produces a completely different output. The bits of the output appear with random frequency and it is computationally hard to find collisions (different inputs yielding the same output). Hashing algorithms are used, for example, to check the integrity and non-tampering of files.

The two main hashing algorithms used in the bitcoin protocol are RIPEMD-160 and SHA-256, which produce outputs of 160 and 256 bits respectively. The mining algorithm consists of performing the double SHA-256 of the block header (doubled to prevent “padding attacks”). The Merkle tree of transactions in a block consists of pairing the transactions and hashing them together (repeating one in order to get a power of 2), then pairing the resulting hashes, etc., in order to build a dyadic tree of hashes. The root of the tree is the Merkle root and is included in the header of the block. So, neither the transactions nor their ordering can be changed once the block is validated.

4 Pseudoanonymity and structure of bitcoin addresses

Since transactions must be made public, it seems that all privacy is lost. However, this is not the case because bitcoin addresses can be created without any personal data from the owner.

Each bitcoin address is composed of a pair of public and private keys. The private key is used to sign transactions that allow one to spend the bitcoins in the balance of the address. Technically speaking, the owner of the bitcoins at that address is whoever has control of the associated private key. The public key has a shorter hashed version, which is the one made public in order to receive funds. A bitcoin public ad-

dress looks like

14xuSZXtfGw5XqfYxEjp4crwYGYQDWmZ12.

This one is under the control of the author (and you are welcome to try your hand at bitcoin transactions by sending many bitcoins!). With a QR code encoding an address, it can be scanned with a smartphone.

Bitcoin addresses are generated using elliptic curve cryptography. To generate a private key, 256 bits are randomly picked (by tossing a coin 256 times, for example) and this binary number gives a secret key k . The associated public key is computed using elliptic curve multiplication $k.g$ of a base point g in the *secp256k1* elliptic curve

$$y^2 = x^3 + 7,$$

where the arithmetic is done in the prime field \mathbb{F}_p with the prime number p slightly less than 2^{256} ,

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1,$$

and the base point given by

$$g_x = 55066263022277343669578718895168534326250603453777594175500187360389116729240$$

$$g_y = 32670510020758816978083085130507043184471273380659243275938904335757337482424$$

This choice of elliptic curve and base point follows cryptographic standards (which is the subject of some controversy for the unexplained choice of parameters). The public key is a 520 bit number obtained as $K = 04xy$ by concatenating the hexadecimal 04 to x and y , where $k.g = (x, y)$, picking $x, y \in [0, p - 1]$ and writing them as 256 digit binary numbers. Usually, a compressed form is used for public keys by hashing K using SHA-256 and then RIPEMD-160. This result is usually written in a special base called *Base58Check*.

Since the public key and its compressed version are generated by applying one-way cryptographic functions, one cannot recover the private key from them. Therefore, they can be safely shared without compromising the private key. This is what is done when a payment is requested to an address.

The space of private keys is huge. Thus, if a proper random choice is made, there is no need to check that anyone else holds the same private key. This allows a decentralised generation of bitcoin addresses offline with no link to the identity of the owner.

This pseudonymity, plus the convenience of electronic payments, has made bitcoin the currency of choice for payments made in the “deep web”, for example in Silk Road, the online market for drugs that was dismantled by the FBI.

This structure of bitcoin addresses raises many legal questions. The most basic one is how to prove ownership of bitcoins. If someone wishes, they can prove that they are in control of a certain address by signing a transaction (or any message) using their private key. On the other hand, it is difficult to prove ownership of a private key with no collaboration.



Figure 3. QR code of a bitcoin address

5 Why is bitcoin money? What is money?

Bitcoin does not fit the standard definitions of money that can be found in most economy or finance books. Even some reputed economists have denied that bitcoin could be money. Before explaining why bitcoin is indeed good money, the essence of money needs to be understood. Some abstract reasoning is necessary.

The key to understanding what money is relies on the fact that abstract objects exist *only* in their properties. In other words, their existence does not depend on any representation. Something that is familiar to mathematicians is often difficult to grasp for non-mathematical minds that are used to relying on representations of abstract objects. In simple terms, *something with all the good properties of money is money!*

In layman's terms, if an animal looks like a duck, walks like a duck, swims like a duck and quacks like a duck then ... it is a duck!

Now, what are these "good properties" of money? Since prehistory, all civilisations have noticed that bartering is inefficient for trading, for the simple reason that, most often, the buyer has nothing of interest to offer to the seller in exchange for his goods, who may need other goods produced by a third individual. The solution to this game theory problem is to use an "exchange token" that has the consensus of the community in exchange for goods or services. Since ancient times, all kinds of tokens have been used for that purpose: shells, salt, seeds, metals, cigarettes, etc.

Obviously, one accepts the token only if one is confident that it will be accepted in the future in exchange for goods or services preserving its value. Anything can be money but *good money is confidence*. This monetary property makes good money valuable, a type of value that transcends the physical representation it may have. Once this is understood, a natural list of properties of good money follows easily. No form of money has all these properties and there is no universal notion of "best money", which depends on the context.

1. *Good money is not easy to falsify or produce.* Otherwise, whoever has this capability could produce arbitrarily large quantities of money at minimal cost with the subsequent disruption of the monetary mass. In the case of gold, its chemical nature as an inert fundamental element in Mendeleev's Table makes it impossible to produce in the way that the medieval alchemists dreamed (excluding residual decay of heavier elements from nuclear fission, which is not cost efficient). Shells could be used as money far away from the coast. Cash, coins and bills are protected by security measures. Bitcoins are not forgeable because they are attached to unique bitcoin addresses that are linked cryptographically in the unalterable blockchain to the original *coinbase transaction* where they were created.
2. *Good money is easily authenticatable.* The success of gold is partly due to its properties (weight, colour, texture), which makes it easily identifiable. In the case of bitcoins, the blockchain data is used.
3. *Good money is easily divisible.* Cheaper items might be needed and the payment received should be divisible. Gold is easily divisible up to gram fractions. Euros are divisible into 100 cents and bitcoins into 100 million satoshis.

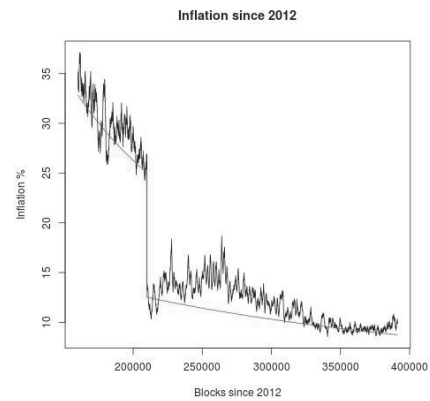


Figure 4. Bitcoin price inflation since 2012

4. *Good money is easily transportable.* It may need to be used far away from where it was acquired, through migration, for example, or through international trade. Electronic money has the best transportation properties. Gold is easy to transport only in small quantities but silver is worse due to the higher mass/price ratio.
5. *Good money enables fast payment settlements.* It takes about 10 minutes to validate a bitcoin transaction and about 24 hours for a European banking SEPA.
6. *Good money is scarce.* There is no absolute measure of "scarcity". There must be some cost to its production or extraction. Otherwise, its monetary value cannot exceed its production cost. This explains why water cannot be good money. Gold is scarce because of the limited amount that can be extracted from the Earth and the energy cost required to extract it (mountains have literally been moved, as testified by the landscape of Las Medulas in Spain). Fiat money scarcity depends only on the will of the central banks (Quantitative Easing (QE) policies by the Federal Reserve have made the dollar abundant but only to the financial sector). Bitcoin scarcity is encoded in the protocol: it costs energy to produce by the PoW and only 21 million bitcoins will ever exist. Paradoxically, scarcity is not in opposition to global use if divisibility is good. No more than 21 million people can have more than one bitcoin but there are more than 200,000 satoshis for each citizen of the world.
7. *Good money is international.* Otherwise, when travelling abroad, exchange fees are incurred. Also, the value of money attached to countries suffers from that country's economic situation. Gold is international and universally accepted. The US dollar is the most international national fiat currency. Bitcoin is transnational by design and not linked to any country or central bank.
8. *Good money preserves or increases its value over time.* Money may need to be saved for years to make big purchases. Any sort of money suffers fluctuations over time. Gold has passed the test of time: one ounce of gold is worth an elegant suit both today and during the Roman empire. Historically, fiat money is debased through inflation, in a way that "no one man in a million will detect" (Keynes). Bitcoin has yet to pass the test of time. In 2011, 2012, 2013 and 2015, it was the best performing currency and in 2014 the worst one.

9. *Good money is not volatile.* Since it might not be known when savings are to be spent, a stable value is desired. All financial assets are volatile but the free market exchange rate of bitcoin is highly volatile, which is not desirable. This volatility is related to its increase of value, which occurs through a concatenation of bubbles. Because of fundamental reasons, volatility is decreasing over time. This will be discussed later.
10. *Good money is fungible.* This means that every dollar is like any other one or any gold atom is like any other one. Fungibility is not always perfect. For instance, money has a memory, which will make it less fungible (for example, fiat money from illicit activities needs to be laundered in order to be fungible). Bitcoin is not perfectly fungible since the blockchain keeps a trace of its past. For instance, one can follow stolen bitcoins, which are sold at a discount. Gold coins are not always fungible, since their preservation state determines part of their price, even for bullion coins.
11. *Good money does not decay over time.* Gold, being chemically more neutral, is better than silver. Treasures from wreckages are a good example: gold coins can be in mint state but silver coins are always badly damaged.
12. *Good money has a large base of users.* You only need one person to accept your money but the larger the community, the more efficient the free market.
13. *Good money is liquid.* It should be well accepted and easily exchangeable for other forms of money.
14. *Good money is easy to store securely.* Since it might need to be saved before it is spent, it must be stored and protected from thieves. Bitcoin has some of the best storage properties.
15. *Good money is anonymous.* Historically, there is a right to privacy in commercial transactions and, for security reasons, anonymity is suitable for large transactions. Bitcoin is only pseudoanonymous.
16. *Good money is decentralised.* Otherwise, its value depends on a third party. If faith on this third party weakens then confidence disappears and the monetary value is lost. This can happen suddenly. It represents an inherent instability of fiat currency and derivatives markets. Centralised money can be blocked or confiscated by the central authority (for example, in a bank freeze). Gold is decentralised, as is bitcoin by design.
17. *Good money is useless!* This is a major property that has been traditionally overlooked. “Useless” here means of non-monetary use, i.e., it does not have any other significant use, in particular no industrial use. Why must it be useless? Because, otherwise, part of its value will depend on the economic activity in the sector where it is employed. But, according to Point 8, its value must be preserved and, in particular, be resilient to economic downturns. In those cases, good money should act as a refuge for wealth. When it has some other use, it also has the positive effect that its value cannot collapse to absolute zero, something which can happen to bitcoin and which happens too often with fiat money. When money has no other use, its value is purely monetary. This property is the reason why silver, platinum and palladium have worse monetary value than gold. Platinum and palladium are used in the au-

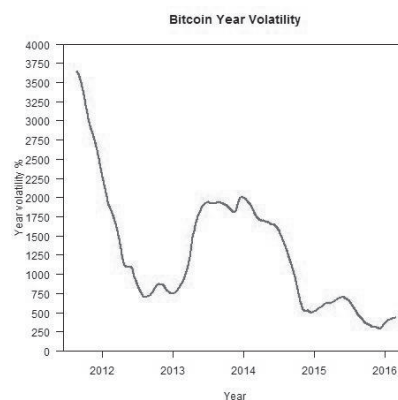


Figure 5. Bitcoin volatility

tomobile industry in catalytic converters. Silver has been used in photography since the 19th century and today is an essential element in the manufacturing of photovoltaic panels.

Corollary. *The more abstract money is the better it is.*

18. *Good money is antifragile.* According to Taleb’s definition [8], something is antifragile if it gains from disorder and unexpected changes. Good money is resilient to economic downturns and also benefits from them as one of the best forms to preserve value. Bitcoin benefits from the inherent instability of other centralised forms of money.
19. *Good money can be used over insecure channels.* Raw bitcoin transactions are designed to travel through insecure communication channels, which is not the case for other digital payment methods, which need an additional layer of encryption.
20. And last but not least, a bonus property that is new to bitcoin. *Good money is programmable!* This is a new property of bitcoin transactions. They come with a “script field”, with instructions on how and when the transaction is to be performed. The most common script is to request that the funds can only be spent with a signature with the secret key of the destination address. But one can also specify things such as to request that the transaction only be effective at a later date, for example 52,560 blocks later (which is about one year later). Also, the scripting allows $n - m$ multisignature addresses, where n signatures among $m \geq n$ are necessary to spend the funds.

This last property is unique to bitcoin, which is the first form of “programmable money”. Bitcoin is reinventing money. The conclusion is that bitcoin has many of the good properties of money and therefore it is money!

However, it is not “perfect money”. Good properties of money depend on its use and context. John Nash gave a thought to what “ideal money” would be [12].

Nowadays, its main weak points are the small user base and the high volatility. The reasons for high volatility are deep and fundamental. The distribution of bitcoins, concentrated with miners and early adopters, is heavily non-Paretian. As observed by Pareto at the end of the 19th century, all wealth distributions have a power law decay and these distributions are universal and stable (see [13] for a simple model explain-

ing Pareto's distribution and stability, motivated by the study of bitcoin volatility). Therefore, bitcoin wealth distribution must converge to a Pareto distribution and this induces an important volume in the market. High volume is correlated with high volatility. From this, it can be inferred that volatility must be high but also that it must decrease over time, which is what is being observed.

6 New economic theory

Bitcoin is also a fascinating academic experiment: for the first time in history, the emergence of a new, decentralised monetary system can be studied. This will be a new chapter in future textbooks on monetary theory.

Moreover, it is destroying some economic beliefs that were previously carved in stone. Some economists have serious doubts about the viability of a deflationary currency. In simple terms, their argument runs as follows. Why would anyone be willing to purchase anything if sometime later they can buy more with the same money? Their conclusions are that the consumption will vanish and the economy will perish. But, historically, gold was a mildly inflationary and viable form of money. The only way to drive out gold from the monetary system was by brute force, through massive hoarding by the central banks.

Actually, this scenario does not occur with bitcoin. Things do not work that way. With a deflationary currency, there is no incentive to make superfluous expenses. People will purchase what they need and save the rest for the future. In practice, what happens, as in the bimetallism dynamics, is that people will spend the bad money and hoard the good money, and will also spend bitcoins when its exchange rate is favourable.

What does not work (in its traditional form) with a deflationary currency is the credit system at large. First, there is no incentive to place savings in a bank. One of the main reasons why people do so is to mitigate the debasement of the currency with the interest paid by the bank. Loans are difficult to repay since on top of the deflation one has to pay interest. Only credits to very productive businesses make sense. Mortgages are not. The banking foundations are at risk with a deflationary currency. This, together with the fact that bitcoins allow anyone to be their own bank, points to a profound disruption of the banking system, similar to what happened with the postal services during the general adoption of email.

Some economists believe that a currency without government sponsorship is hardly viable. This is the opinion of Yannis Varoufakis [14], a lucid contemporary economist, game theorist and one of the few that understands the technical aspects of bitcoin. Varoufakis had a brilliant plan to issue a Greek national cryptocurrency linked to the growth of the Greek GDP.

7 Regulation and the legal status of bitcoin

Regulators are struggling to give bitcoin a proper legal status. One of the main questions is to decide if it should be considered a currency or a commodity. If it is the latter, it would be subject to VAT; if it is the former, it would be exempt like other currencies (including gold bullion). The regulation is not uniform. Only recently, the EU authorities have decided

to consider bitcoin a currency. It should probably not be considered either of the options, since it doesn't fit into the existing legal framework. In the USA, FinCen, which supervises financial companies and enforces AML (Anti Money Laundering) regulations, is requiring bitcoin exchanges to be regulated like financial service companies. A too strict regulation forces bitcoin businesses to migrate to more friendly jurisdictions. Fiscal regulation problems are also Byzantine. What should the taxation of miners be? How can the fiscal rules be enforced with a pseudoanonymous currency? The uneasiness of regulators with technical aspects makes the task even more difficult. There have been some considered reports by the ECB on virtual currencies [15]. It is interesting to note how even the ECB recognises an uneasiness with current definitions of money in the economic literature, which do not seem to apply to bitcoin. From the introduction of the 2015 report:

The ECB does not regard virtual currencies, such as bitcoin, as full forms of money as defined in economic literature. Virtual currency is also not money or currency from a legal perspective.

They even try their hand at giving a definition of virtual currency (on p. 25):

A virtual currency can therefore be defined as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.

This is an odd definition, which defines as "virtual currency" anything not fitting the usual definition of money, missing the essence of what money really is: *confidence*!

8 The Trust Machine

Being an unfalsifiable ledger, the blockchain has other unexpected applications. It has been rightly labelled as "The Trust Machine", which is a very accurate description.

The first non-monetary application is to provide a decentralised trustable clock ... by just counting blocks! It is not a highly precise clock because block validation occurs only about every 10 minutes. Another example of a new application is to provide notary services without a notary! The existence of a legal document can be validated directly inside the blockchain, without the need for a third party. One can scan the document, hash it and insert the hash in the transaction scripting space, which will be embedded in the blockchain and will remain there forever, providing mathematical proof that the document existed at the time of the block validation. Similarly, the blockchain can be used as a decentralised and universal system to certify proof of ownership. Non-erasable messages can be included in the blockchain like the one Satoshi inserted in the genesis block: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

The blockchain technology can be used in order to build decentralised and anonymous market places. Different projects are being developed. One can build other blockchains for this type of application or one can build what have been called "side-chains". This is a new idea that grafts a new service onto the bitcoin blockchain, taking advantage of the security already in place for the bitcoin net. Also, new platforms built

from scratch like Ethereum are being proposed with the goal of offering all sorts of decentralised services.

Since bitcoin offers the possibility of cheap and secure international transactions, it has attracted the attention of the banking system as a way to reduce their operational costs. There has recently been much talk about “private” blockchains, without the understanding that blockchain technology is about an open, decentralised system and is more than a shared database. Some of these speculations fail to realise that a protocol of blockchain type is non-trivially linked to a currency token, which incentivises security by the decentralised mining power.

9 Bitcoin curiosities

Who is Satoshi Nakamoto?

Little is known about the true identity of Satoshi Nakamoto, apart from his participation in the Cryptography Mailing List, a meeting place for the Cypherpunk group, and in the forum *bitcointalk* that he created. There has been much speculation. Even the name of the late John Nash was put forward because of his writings on “Ideal Money” [12]. This is unlikely in view of the last mathematical section of the founding article but his work could have had an influence. Nakamoto is an individual or a group of people with a background in cryptography, mathematics and coding, leading the project up to their last post on December 2010. The diversity of expertise needed to devise and implement the protocol, and the earlier precursor work, points to a collaborative project by members of the cypherpunk community. This could also explain why early mined coins by Nakamoto (estimated to be over a million) haven’t moved. But why did the Nakamoto group choose to stay anonymous? When a project transcends individuals, it makes sense to develop it anonymously. There is a close example in the Bourbaki group (who may have inspired them). The right to privacy is the most fundamental part of the Cypherpunk philosophy, as described in the Cypherpunk manifesto (Erik Hughes, 1993). As for mathematical theorems, the identity of the authors is irrelevant for the ongoing project. The community can only be grateful to them.

The millionaire pizza

The first bitcoin transaction was made in block 170, on 12 January 2009, between Nakamoto and the late Hal Finney, who was the first one to realise the potential of Nakamoto’s creation. The first purchase using bitcoin was only made much later on 22 May 2010 [16]. The *bitcointalk* forum is a meeting place for bitcoin developers and users, where general and technical discussions take place. L. Hanyecz, the first GPU miner, offered to trade 10,000 bitcoins for two pizzas (which was worth about \$40 at the time) to be delivered to him. Another participant accepted the deal and earned what is now worth several million dollars. This gives a good illustration of the workings of a deflationary currency.

Is bitcoin a Ponzi scheme?

Detractors of bitcoin argue that the currency has nothing backing it, hence it has no value. They fail to grasp that bitcoin is backed and secured by the full computer power of the val-

idating network, currently at more than 9.4 million petaflops, which, at present, surpasses by hundreds of times the power of the 500 fastest computers in the world combined. Then, they claim that bitcoin is a mere Ponzi scheme, confusing its exponential viral development with a Ponzi scam. Viral development is common in the world of new technologies. The adoption rate is a sigmoid curve, with an exponential rate in the first phase (in which we are now). A main difference between bitcoin and a Ponzi scheme is the open source code. Anyone can check that the bitcoin network functions as it is supposed to by inspecting and analysing the bitcoin code. Thus, there is full and transparent information. This is quite different from the opaque operation of Ponzi schemes (or the central banking system, by the way).

On bitcoin bubbles

The price of bitcoin is fixed by the free market. It is a non-regulated international market. Anyone can exchange other currencies or other goods for bitcoins if they find a counterpart willing to accept bitcoins. The actual exchange rate is determined by the largest exchanges, which have the largest volume. The price evolution has not been peaceful. The bitcoin exchange rate suffers from high volatility. So far, there have been six major bubbles and many others of a smaller scale:

- From \$0.003 to a peak of \$0.0875, from 1 May to 18 July 2010, a 2,816 % increase in less than three months.
- From \$0.06 to a peak of \$0.50, from 6 October to 6 November 2010, a 733 % increase in one month.
- From \$0.40 to a peak of \$1.10, from 26 January to 9 February 2011, a 175 % increase in two weeks.
- From \$0.58 to a peak of \$32.00, from 4 April to 8 June 2011, a 5,417 % increase in two months.
- From \$9.75 to a peak of \$260, from 26 October 2012 to 10 April 2013, a 2,566 % increase in about five months.
- From \$110 to a peak of \$1,245, from 2 October to 5 December 2013, a 1,032 % increase in two months.

These are partly speculative bubbles. Usually, when these bubbles burst, the price does not drop significantly lower than the previous peak, which is an indicator that a fundamental upper trend is at work. Someone holding \$1 in bitcoin in April 2010 could turn it today into \$150,000. The current annual monetary inflation is about 8 % (the real one, due to the increase of computing power is currently around 9 %) but the user growth is now higher. In 2016, after the next halving, inflation will drop to around 4 %.

What is the target capitalisation of bitcoin?

Currently, there are about 15.5 million bitcoins (the 15 millionth bitcoin was mined during Christmas Day 2015). At the current market price of 400 euros, this gives a capitalisation of the bitcoin at about 6 billion euros. To put this number into perspective, a company enters onto the list of the 50 largest publicly traded companies with a market capitalisation of over 93 billion euros. Some small countries have a GDP smaller than bitcoin capitalisation. The current monetary mass M1 of the euro (currency in circulation + overnight deposits) is 6,500 billion euros.

One can speculate about the target capitalisation of bitcoin. This depends on its growth and use. If only a small frac-

tion of the total underground economy goes into bitcoin, its price will be quite large (\$ 10,000 is not unreasonable) but some authors speculate that it may reach \$ 100,000 in a few years and even over 1 million dollars per bitcoin if bitcoin becomes the reference international currency.

What can I buy with bitcoins?

There are all sorts of companies and small business accepting bitcoins. It is likely that somewhere near you, there is some cafe or restaurant that accepts bitcoin. There is a useful site, coinmap.org, which plots on a map the places that accept bitcoin. One of the largest companies that sells goods over the internet, Overstock, has been accepting bitcoin. Bitcoin is particularly well adapted to payments over the internet. One does not need to worry about someone stealing your credit card data. When you make a bitcoin payment you don't give away any personal information nor any information that could be useful to a hacker. There are also companies, like Xapo, offering a bitcoin wallet linked to a regular credit card that can be refilled using bitcoins.

Can bitcoin be a solution for the unbanked?

A major proportion of the population in the world has no access to banking services. In Kenya, a particular form of electronic money developed in 2007. It is called *mPesa* and the currency is based on mobile phone minutes that can be exchanged and used to pay for goods or services. About a third of the Kenyan population uses mPesa. Recently, there have been efforts to integrate bitcoin with mPesa, which will bring bitcoin to the users of mPesa that can be used with their regular mobile phone.

Getting started

A final few lines on how to get started. The first question anyone asks is how to buy or earn bitcoins. First, one needs to set up a wallet in order to manage bitcoins. The fastest way is to sign up for a free online wallet at sites like blockchain.info, which also has an app for your Android smartphone (you only need a working email). A better way is to download the official client at bitcoin.org or a free wallet program like Armory or Electrum. The official client downloads the full blockchain. It can take several days (now the blockchain is about 70 Gb). Electrum avoids this by using "trusted sites", which is faster but not decentralised. Finally, for those wanting the highest level of security, the best solution is to purchase a Trezor or Ledger device, which is like a flash drive securely holding the private keys, which never go online. Then, one can purchase or sell bitcoins by registering at an exchange site like bitstamp.net or bitfinex.com (the two largest in the West) or carry out a personal transaction through the site localbitcoins.com.

10 Conclusions

Monetary questions have historically attracted some of the most brilliant thinkers: Oresme, Copernicus, Newton, Keynes, Nash, Nakamoto, etc. The new form of money that the bitcoin protocol brings to us forces a redefinition of basic notions. It represents an escalation in the ladder of abstraction of the concept of money. As for mathematical theories, abstraction

comes hand-in-hand with more pure, more general, more universal and more effective properties. From the perspective of economic dynamics, this is a unique event that deserves close attention from the academic community. From a social and political point of view, bitcoin brings back to the citizen the ownership of money. It is a "technology coup" to the centralised, outdated financial system ruled by banks. The wide implementation of "The Mathematical Trust Machine" will have a profound social, economic and political impact, and mathematics is at the root of this coming revolution.

Acknowledgements.

I am grateful to L. Blanco, R. K. Englund, A. Marti and N. Szabo for their remarks and comments.

Bibliography

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", www.bitcoin.org/bitcoin.pdf, released on 1 November 2008 on the USENET Cryptography Mailing List "Bitcoin P2P e-cash paper".
- [2] S. Nakamoto, "Bitcoin v0.1", released on 9 January 2009 on the USENET Cryptography Mailing List "Bitcoin v0.1 released".
- [3] "Cuneiform digital library initiative", www.cdli.ucla.edu.
- [4] J.-F. Serval and J.-P. Tranié, *The Monetary System: Analysis and New Approaches to Regulation*. Wiley & Sons, 2014.
- [5] M. Flandreau, *The glitter of gold*. Oxford University Press, 2004.
- [6] N. Copernicus, *Monete cudende ratio*. 1526.
- [7] N. Oresme, *De origine, natura, jure et mutationibus monetarum*. 1360.
- [8] N. Taleb, *Antifragile: Things that Gain from Disorder*. Random House, 2012.
- [9] *The Economist*, vol. 417, 8962, 31 October – 6 November 2015.
- [10] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem", *ACM Trans. Prog. Lang. Syst.*, vol. 4, pp. 382–401, July 1982.
- [11] "Bitcoin code", www.github.com/bitcoin.
- [12] J. F. Nash, "Ideal money", *Southern Econ. J.*, vol. 69, 1, 2002.
- [13] R. Perez-Marco, "A simple dynamical model leading to Pareto wealth distribution and stability", *arXiv:1409.4857*, 2014.
- [14] Y. Varoufakis, "Bitcoin and the dangerous fantasy of apolitical money", www.yanisvaroufakis.eu.
- [15] ECB, "Virtual currency schemes", www.ecb.europa.eu, 2012, 2015.
- [16] L. Hanyecz, "Pizza for bitcoins!", www.bitcointalk.org.



Ricardo Pérez-Marco [ricardo.perez.marco@gmail.com] grew up in Barcelona, studied at ENS Paris and received a PhD from University Paris-Sud in 1990. He won the Prize of the EMS in 1996, was a professor at UCLA and is now Directeur de Recherches at CNRS (Paris). His focus is on geometry and complex analysis, with widespread interests including small divisors, holomorphic dynamics, zeta functions and economic dynamics. His hobbies include being a chess player, a poker player, a speculator and a bitcoiner, as well as challenging the establishment.

A Tribute to Abbas Bahri (1955–2016)

Mohameden Ahmedou (Universität Giessen, Germany), Mohamed Ben Ayed (Université de Sfax, Tunisia), Ali Maalaoui (American University of Ras Al Khaimah, UAE) and Vittorio Martino (Università di Bologna, Italy)



The eminent mathematician Abbas Bahri passed away on 10 January 2016 at the age of 61 years. He was a leading figure in nonlinear analysis and conformal geometry. Indeed, he played a fundamental role in the understanding of the lack of compactness arising in certain variational problems. For example, his book *Critical Points at Infinity in Some Variational Problems* exerted

a tremendous influence on researchers working in the field of nonlinear partial differential equations involving critical Sobolev exponents. In particular, the book included finite dimensional reduction for Yamabe-type problems and the related shadow flow for an appropriate pseudogradient, as well as the accurate expansion of the Euler-Lagrange functional and its gradient, which later became tools widely used in this field.

Abbas Bahri was born and grew up in Tunisia where he attended elementary school and high school. At the age of 16, he moved to Paris, where he was admitted to the prestigious *Ecole Normale Supérieure, Rue d'Ulm* at the age of 19. He later defended a *Thèse d'Etat* under the direction of Professor Haim Brezis in 1981 at the age of 26.

Abbas' remarkable achievements have been widely recognised. He was awarded the Langevin and Fermat prizes¹ in 1989 for "introducing new tools in the calculus of variation" and in 1990 he received the Board of Trustees Award for Excellence, the Rutgers University highest honour for outstanding research.

Abbas Bahri's mathematical interests were very broad, ranging from nonlinear partial differential equations arising from geometry and physics to systems of differential equations of celestial mechanics. However, his research focus was mainly on fundamental problems in contact form and conformal geometry. The aim of this short note is to outline some of the milestones of Abbas' mathematical legacy.

1 The critical points at infinity approach to non-compact variational problems

Many partial differential equations (PDEs) enjoy a variational structure, that is, one can see their solutions as critical points of functionals. The space where the functionals are defined depends on the PDEs. For example, to study the following nonlinear PDE:

$$-\Delta u = |u|^{q-2}u \text{ in } \Omega; \quad u = 0 \text{ on } \partial\Omega \quad (\text{with } q > 2), \quad (1)$$

where Ω is a bounded subset of \mathbb{R}^n , $n \geq 3$, one can define

$$I(u) = \frac{1}{2} \int_{\Omega} |\nabla u|^2 - \frac{1}{q} \int_{\Omega} |u|^q, \quad u \in H_0^1(\Omega),$$

where $H_0^1(\Omega)$ denotes the Sobolev space (the space of the functions $u \in L^2(\Omega)$ with $\nabla u \in (L^2(\Omega))^n$ and $u = 0$ on $\partial\Omega$). It is clear that the solutions of (1) are in a one-to-one correspondence with the critical points of I .

Recall that the embedding of $H_0^1(\Omega)$ into $L^q(\Omega)$ is compact for $q < \frac{2n}{n-2}$ and it is only continuous if $q = \frac{2n}{n-2}$. Hence, the exponent $q - 1 = \frac{n+2}{n-2}$ is said to be a *critical exponent* for equations of type (1). Note that, for $1 < q - 1 < \frac{n+2}{n-2}$, using the compactness of the embedding, one can show that I has at least one critical point by maximising I on the space $\Sigma := \{u \in H_0^1(\Omega) : \|u\| = 1\}$.

PDEs with critical nonlinearities exhibit exceptional features such as blowups, loss of compactness, energy quantisation and formation of singularities, emerging from the critical balance between the model linear PDE and strongly nonlinear terms. At the frontier of stability, these behaviours present great challenges to mathematical analysis and examples of such phenomena may be found in geometry (prescribed curvature problems, conformal deformation laws), physics (mean field equations, Chern-Simons-Higgs models, electroweak theory, Yang-Mills equation) and general relativity (quasi-local mass, static metrics). The understanding of the nonlinear features of these equations (bubbling off phenomena, existence mechanisms) is one of the main concerns of nonlinear geometric analysis and occupied a central position in Abbas' research. In a recent interview (Fifth Saudi Science Conference, An Interview with Professor Abbas Bahri, 1 Dec 2011) when asked the question: "What are the most fascinating discoveries scientists have made in your area during the last 20 years?" he answered laconically: "The understanding of non-compact phenomena." Indeed, Abbas became fascinated by variational problems arising in contact geometry at the beginning of his career and kept working on that topic all his life. He was, in particular, motivated by the Weinstein conjecture about the existence of periodic orbits of the Reeb vector field of a contact form. Although this problem features a variational structure, its corresponding variational form is neither compact nor Fredholm. It is in this framework that Abbas developed the concept of *critical points at infinity* [3]. These are accumulating points of non-compact orbits of the gradient flow. In fact, he discovered that the ω -limit set of non-compact orbits of the gradient flow behaves like a *usual critical point* once a Morse reduction in the neighbourhood of such geometric objects is performed. In particular, one can associate to such *asymptotes* a Morse index (counting the number of decreasing directions in the normal form given by the Morse reduction) as well as a stable and an unstable

¹ Prix Fermat 1989, Annales de la faculté des sciences de Toulouse, vol. XI, no. 2, 1990, pp. 7–8.

manifold. This strategy turns out to be very useful in handling non-compactness in other variational problems (such as Yamabe-type equations, prescribed scalar curvature equations, the n -body problem in celestial mechanics and mean field equations).

The following short sections highlight some of Abbas Bahri's main contributions in this field.

The Yamabe-type problem and the Bahri-Coron topological argument

In [13], Abbas Bahri and Jean-Michel Coron studied the following Yamabe-type equation on domains $\Omega \subset \mathbb{R}^n$, $n \geq 3$:

$$-\Delta u = u^{\frac{n-2}{n-2}}, u > 0 \text{ in } \Omega, \quad u = 0 \text{ on } \partial\Omega. \quad (2)$$

This nonlinear PDE involving a critical Sobolev exponent does not have a solution when the domain is star-shaped but it has a radial solution on annular domains. Such behaviour suggests that the topology of the domain should play a crucial role in the condition that ensures the existence of solutions. Indeed, by exploring the impact of the topology of the domain, Bahri and Coron proved that if the group homology $H_d(\Omega, \mathbb{Z}_2)$ is not trivial for some $d \geq 1$ then the equation (2) always has at least one solution. In proving such a result, they discovered a topological argument, which turns out to be very useful in the study of some other Yamabe-type problems (such as Yamabe-type problems on manifolds with or without boundaries [4, 12, 1], the CR–Yamabe problem [26, 27], and mean field-type equations on unbounded domains [15]).

To explain the strategy of the proof, we need to set up the variational framework and recall some preliminaries.

Equation (2) has a very nice variational structure. Indeed, its solutions are in a one-to-one correspondence with the critical points of the functional

$$J(u) := \frac{1}{\int_{\Omega} |u|^{\frac{2n}{n-2}}},$$

defined on $\Sigma_+ := \{u \in H_0^1(\Omega); \|u\| = 1; u \geq 0\}$, where $H_0^1(\Omega)$ stands for the Sobolev space and $\|\cdot\|$ its norm.

Note that the Palais-Smale (PS) condition is a crucial property to extend the standard tools of the calculus of variation. A function f is said to satisfy the PS condition in $[a, b]$ if each sequence (x_n) such that $a \leq f(x_n) \leq b$ and $\nabla f(x_n)$ tends to 0 possesses a convergent subsequence.

Although J does not satisfy the PS condition, the flow lines of the gradient violating this condition are well understood (see [30], [20]). Namely, such flow lines should enter an ε -neighbourhood $V(p, \varepsilon)$ of some highly concentrated bubbles. Moreover, the limit energy levels of non-compact ones are given by $p^{2/(n-2)}S$, where p denotes the number of bubbles and S the Sobolev constant.

By setting

$$W_p := \{u \in \Sigma_+; J(u) < (p+1)^{2/(n-2)}S\}$$

from a classical deformation lemma, it follows, under the assumption that there are no critical points between the levels $p^{2/(n-2)}S$ and $(p+1)^{2/(n-2)}S$, that the sublevel W_p retracts by deformation onto $W_{p-1} \cup A$, where $A \subset V(p, \varepsilon)$.

To study the equation above, Bahri and Coron argued as follows. Firstly, they observed, under the assumption that $H_d(\Omega, \mathbb{Z}_2) \neq 0$, that it follows from a well known result of R.

Thom [31] that this nontrivial homology class can be realised by a d -dimensional compact manifold without boundary V . That is, denoting by $\iota : V \rightarrow \Omega$ the related embedding and by ω the orientation class of the manifold V , we have that $0 \neq \iota_*(\omega) \in H_d(\Omega, \mathbb{Z}_2)$.

Next, let

$$B_p(V) := \left\{ \sum_{i=1}^p \alpha_i \delta_{a_i}; \quad a_i \in V, \quad \alpha_i \geq 0; \quad \sum_{i=1}^p \alpha_i = 1 \right\}$$

denote the p -set of formal barycentres of V endowed with the weak topology of measures. These are stratified sets of top dimension $dp + p - 1$. Let $\omega_p \in H_{dp+p-1}(B_p(V), B_{p-1}(V))$ denote the top homology class of the pair $(B_p(V), B_{p-1}(V))$.

To perform their topological argument, Bahri and Coron constructed, for a large real parameter λ , a continuous sequence of functions

$$f_p(\lambda) : (B_p(V), B_{p-1}(V)) \rightarrow (W_p, W_{p-1}).$$

These functions induce homeomorphisms in the homology

$$(f_p(\lambda))_* : H_*(B_p(V), B_{p-1}(V)) \rightarrow H_*(W_p, W_{p-1}).$$

Moreover, under the assumption that the functional J does not have any critical point under the level $2^{2/(n-2)}S$, we have that

$$(f_1(\lambda))_* : H_d(V) \rightarrow H_d(W_1)$$

is a homotopy equivalence. On the other hand, for large p , all $(f_p(\lambda))_*$ are trivial in homology. Indeed, through a careful expansion of J using the interaction terms, one can prove that $f_p(\lambda)$ is homotopic to a map with its values in W_{p-1} .

Next, for a small number $\varepsilon > 0$, let $q \in \mathbb{N}$ be the smallest integer such that

$$(f_q(\lambda))_*(\omega_q) = 0 \text{ in } H_{dq+q-1}(W_q, W_{q-1})$$

$$\text{and } (f_q(\lambda))_*(\omega_q) \neq 0 \text{ in } H_{dq+q-1}(J^{qS+\varepsilon}, W_{q-1}).$$

It then follows, from an exact sequence argument in homology of the triple $(W_p, J^{pS+\varepsilon}, W_{p-1})$, that

$$H_{dq+q}(J^{(q+1)^{2/(n-2)}S}, J^{q^{2/(n-2)}S+\varepsilon}) \neq 0.$$

Since the PS condition is satisfied in the range

$$(q^{2/(n-2)}S + \varepsilon, (q+1)^{2/(n-2)}S) \text{ for } \varepsilon \text{ small,}$$

one can derive the existence of a critical point of generalised Morse index $qd + q$.

We point out that the topological argument above is of an abstract nature; in fact, it is based on the following dynamical features of the gradient in the neighbourhood at infinity $V(p, \varepsilon)$. Indeed, one can use the following two properties in a crucial way.

- The unstable manifold $W_u(V(p, \varepsilon))$ of $V(p, \varepsilon)$ does not intersect $V(m, \varepsilon)$ with $m > p$.
- The flow lines leaving $V(p, \varepsilon)$ through the unstable manifold of a *critical point at infinity* do not re-enter $V(p, \varepsilon)$ through the stable manifold of another *critical point at infinity*.

Finally, we point out that a necessary and sufficient condition for the existence of solutions to equation (2) is still missing. Moreover, the geometry of the domain should play an important role in such a condition. Indeed, Wei Yue Ding [23] constructed solutions for (2) on a contractible domain. In order to investigate the role of geometry, Abbas conjectured (private communication) that the following result would be true.

Denoting by G the Green's function of the Laplace operator under Dirichlet boundary conditions and by H its regular part, and setting $\varrho_p(x) := \varrho_p(x_1, \dots, x_p)$ to be the least eigenvalue of the matrix $M := (a_{ij})$ given by $a_{ii} := H(x_i, x_i)$ and $a_{ij} := -G(x_i, x_j)$ for $i \neq j$, one can define the set:

$$I_p := \{x = (x_1, \dots, x_p) \in \Omega^p; \varrho(x_1, \dots, x_p) < 0\}.$$

Then, the following should hold true.

If Ω is contractible but for some $p \geq 2$ the set I_p is not contractible then equation (2) has at least one solution.

The reason behind the above conjecture is that the contribution of critical points at infinity to the topology of the pair

$$(J^{p^2/(n-2)S+\varepsilon}, J^{p^2/(n-2)S-\varepsilon})$$

is described by the pair (Ω^p, I_p) (see [19]).

The prescribed scalar curvature problem

A natural extension of the Yamabe problem is to ask the following question. Given a compact closed Riemannian manifold (M, g) and a smooth function $K \in C^\infty(M)$, does there exist a conformal metric \tilde{g} such that the scalar curvature with respect to \tilde{g} is given by the function K ?

Note that \tilde{g} is a conformal metric to g if there exists a function f such that $\tilde{g} = e^f g$. Setting $\tilde{g} := u^{\frac{4}{n-2}} g$, this problem amounts to solving the following nonlinear PDE involving a critical Sobolev exponent:

$$L_g u = K u^{\frac{n+2}{n-2}}, u > 0 \text{ in } M, \tag{3}$$

where L_g stands for the conformal Laplacian.

Just as in the Yamabe case, problem (3) has a variational formulation. However, the associated Euler-Lagrange functional does not satisfy the PS condition. Moreover, there are some obstructions to the existence of solutions (see [25] and [21]).

Using the positive mass theorem of Schoen and Yau [28], [29], Escobar and Schoen [24] proved, for a three-dimensional closed Riemannian manifold, that as long as the manifold is not conformally equivalent to the three round sphere \mathbb{S}^3 , problem (3) is always solvable under the assumption that K is a positive function.

In [14], Bahri and Coron, inspired by earlier work of Abbas on contact form geometry [3], developed a *critical points at infinity* approach for the scalar curvature problem on \mathbb{S}^3 under the non-degeneracy assumption that at a critical point a of K we have $\Delta K(a) \neq 0$. Their strategy consists of studying the ω -limit set of non-compact orbits of the gradient flow. Following the work of Michael Struwe [30], we know that such non-compact orbits will be trapped in an ε -neighbourhood $V(p, \varepsilon)$ of highly concentrated p -bubbles δ_{a_i, λ_i} . The strategy adopted by Bahri and Coron consists of tracking down such flow lines that remain indefinitely in $V(p, \varepsilon)$ by showing that they decompose into an infinite part, which will vanish as time tends to infinity, and a *shadow flow*, which is a finite dimensional part and which splits in a canonical way into an ordinary differential equation, whose variables are: matching parameters $\alpha_i(t)$, concentration points $a_i(t) \in \mathbb{S}^3$ and concentration rates

$\lambda_i(t)$. Namely, we have that, as $t \rightarrow +\infty$,

$$\begin{aligned} -\frac{\dot{\lambda}_i}{\lambda_i} &= A_1 \frac{\Delta K(a_i)}{\lambda_i^2 K(a_i)^{\frac{5}{4}}} - A_2 \sum_{j \neq i} \lambda_j \frac{\partial \varepsilon_{ij}}{\partial \lambda_i} + \text{l.o.t.}, \\ \dot{a}_i &= B_1 \frac{\nabla K(a_i)}{\lambda_i^2 K(a_i)^{\frac{5}{4}}} + B_2 \sum_{j \neq i} \frac{\partial \varepsilon_{ij}}{\partial a_i} + \text{l.o.t.}, \end{aligned} \tag{4}$$

where A_i, B_i are positive constants and $\varepsilon_{ij} := \langle \delta_i, \delta_j \rangle$, which behaves like $\frac{G(a_i, a_j)}{(\lambda_i \lambda_j)^{1/2}}$, denotes the interactions of two bubbles.

It then follows from the system of equations above that such a flow line will exit any set $V(p, \varepsilon)$ for $p \geq 2$ since the interaction terms ε_{ij} , which are the leading ones, would bring the flow lines down. Hence, the only possible non-compact flow lines are those that concentrate at single points. Moreover, analysing the above ordinary differential equation in the set $V(1, \varepsilon)$, one can derive that the only possibility for a flow line to build a *critical point at infinity* is that $a_i(t)$ converges to a critical point a_i of K such that $\Delta K(a_i) < 0$. Conversely, any gradient flow line, starting from a bubble $\delta_{b, \lambda}$ where $b \in \mathbb{S}^3$ is a critical point of K such that $\Delta K(b) < 0$, would remain forever in $V(1, \varepsilon)$ for $\varepsilon \rightarrow 0$. Hence, the only singularities of the gradient flows are those of the above type. The index of such a critical point at infinity is defined as the coindex of K at the concentration point a . It follows then, from an Euler-Poincaré-type argument, that:

$$\sum_{a \in \mathbb{S}^3; \nabla K(a)=0, \Delta K(a)<0} (-1)^{3-\text{Morse}(K,a)} = 1.$$

Hence, any function violating such an equality can be realised as a scalar curvature of a Riemannian metric conformally equivalent to the standard metric on \mathbb{S}^3 .

To study the non-compactness in the case of spheres of dimension $n \geq 4$, Abbas introduced a family of bounded *pseudogradients* in the neighbourhood at infinity. A vector field W is said to be a pseudogradient for J if it satisfies the following condition: there exists a positive constant c such that

$$\langle \nabla J(u), W(u) \rangle \geq c \|\nabla J(u)\|^2, \quad \forall u.$$

This family allowed him to determine the end-points of the flow lines and he proved that they are in a one-to-one correspondence with the *critical points at infinity*. He then associated to this family a topological invariant $\mathcal{I}(V)$ (see [11]), a kind of degree that has to be non-zero, to ensure the existence of solutions. Such an invariant has been extended by Ben Ayed, Chtioui and Hammami [18] and has been used to investigate the problem of prescribed scalar curvature on high dimensional spheres.

2 The lack of compactness and Fredholm structure in contact form geometry

Bahri has made many contributions in the field of contact geometry, which is in some sense the counterpart of symplectic geometry for the odd dimensional case. One can see this duality as follows. Let us consider a particle q moving on the plane under a force field $-\nabla V$. Then, Newton's equation reads as

$$m\ddot{q} = -\nabla V(q).$$

If we assume for simplicity that $m = 1$ and we set $p = \dot{q}$ then we have the system

$$\begin{cases} \dot{q} = p \\ \dot{p} = -\nabla V(q). \end{cases}$$

So, if we denote by $H(p, q) = \frac{1}{2}|p|^2 + V(q)$ the total energy (kinetic and potential), the previous system reads as

$$\begin{cases} \dot{q} = \frac{\partial H}{\partial p} \\ \dot{p} = -\frac{\partial H}{\partial q}. \end{cases}$$

Such a system is called Hamiltonian. Now, let us suppose that we are looking for periodic solutions of such a system, namely periodic orbits of the vector field $(\frac{\partial H}{\partial p}, -\frac{\partial H}{\partial q})$. We have two choices. Either we fix the period T , therefore working on a manifold of dimension four and meeting the theory of symplectic manifolds and the Arnold conjecture, or we fix the energy level H , therefore being constrained on a manifold of dimension three and meeting the theory of contact manifolds and the Weinstein conjecture. The study of such problems is variational, i.e. there exists a functional J on a suitable space such that the critical points of J are solutions to our system. Clearly, since we are looking for periodic orbits, the space of variations should be in the space of loops.

This approach can be formalised for the general setting of a compact three-dimensional manifold (M, α) , where α is a 1-form on M such that $\alpha \wedge d\alpha$ is a volume form (never vanishing). Such a form has a very intrinsic vector field associated to it, called the Reeb vector field, which we denote by ξ and which satisfies

$$\begin{cases} d\alpha(\xi, \cdot) = 0 \\ \alpha(\xi) = 1. \end{cases}$$

Now, the problem turns to looking for periodic orbits of the vector field ξ . This is equivalent to studying the critical points of the functional $J : H^1(S^1; M) \rightarrow \mathbb{R}$ defined by

$$J(x) = \int_{S^1} \alpha(\dot{x}).$$

Here, we denote by $H^1(S^1; M)$ the H^1 -loops space on M , that is, the space of the curves $x : [0, 1] \rightarrow M$, $x(0) = x(1)$, that have the regularity of the Sobolev space H^1 . This functional basically measures the contribution of ξ along \dot{x} . Indeed, if we assume that the manifold has a global frame of the form (ξ, v, w) , where v and w are in $\ker(\alpha)$, then for a loop x we have $\dot{x} = a\xi + bv + cw$ for some functions a, b, c , and thus $J(x) = \int_0^1 a(t)dt$. It is important to notice that this functional defined on $H^1(S^1; M)$ is unbounded from below and above, since a can take any form; moreover, it is not Morse.

Bahri first focused on finding a better space of variations for the functional J . In order to restrict the functional on a smaller space and avoid the degeneracy, he introduced a sort of Legendre transform similar to the classical one. Indeed, the standard contact form α_0 on S^3 is a pull-back from the standard contact form on $P(\mathbb{R}^3)$, i.e. the unit sphere cotangent bundle of S^2 . Therefore, it is equipped with its Liouville form: the Legendre duality can be completed for this Liouville form. This transform can be viewed as the data of a vector field v in $\ker(\alpha_0)$ such that $\beta_0(\cdot) := d\alpha_0(v, \cdot)$ is a contact form with the same orientation as α_0 . This Legendre transform allows one to move from a Hamiltonian problem on the cotangent sphere of S^2 to a Lagrangian problem.

This duality was then extended by Bahri-Bennequin in [10] to the more general framework of a contact form α on a three-dimensional compact orientable manifold without boundary M , leading to a variational problem on a space of curves. In fact, assuming that v is a non-vanishing vector field

in $\ker(\alpha)$, we say that the Legendre transform of α with respect to v can be completed if the dual non-singular one-form $\beta(\cdot) := d\alpha(v, \cdot)$ is again a contact form on M with the same orientation as α . In this situation, by restricting the functional J on the subspace of the H^1 -loops on M :

$$C_\beta = \{x \in H^1(S^1; M) \text{ s.t. } \beta(\dot{x}) = 0; \alpha(\dot{x}) = a\},$$

where a is a positive constant, the following result by Bahri-Bennequin holds [10]:

J is a C^2 functional on C_β whose critical points are periodic orbits of ξ and they are of finite Morse index.

We notice that the curves in C_β can be expressed in a simple way, that is, if $x \in C_\beta$ then $\dot{x} = a\xi + bv$, where a is now just a constant (eventually depending on x) and therefore $J(x) = a > 0$. The understanding of this variational problem, such as the study of the existence and the multiplicity of critical points of J , is closely related to problems such as the Weinstein conjecture and the definition and well-posedness of a contact homology. However, this variational formulation has two main difficulties: the lack of compactness and the Fredholm assumption.

Non-compactness. The functional J defined on C_β is non-compact, in the sense that it does not satisfy the PS condition. In fact, one can see this fact directly from the functional: if we have a curve $x \in C_\beta$ with $\dot{x} = a\xi + bv$ then, as was mentioned above, the functional just controls the value a of the curve but the b -component along v is free. Therefore, it can have any behaviour along a PS sequence.

In his works [10, 6], Bahri constructed a flow in order to give a precise description of the violation of the PS assumption. Moreover, the introduced flow has many important topological properties on the curves, such as the decreasingness of the linking number, and it has asymptotes going to critical points at infinity. The description of the PS sequences is made by means of curves that lie on a stratified space and that are made of pieces of ξ and pieces of $\pm v$ (since the functional does not catch the variation along v), in terms of *conjugate points* and *characteristic pieces*. In order to describe this fact, let x be a curve belonging to C_β . Then, $\dot{x} = a\xi + bv$ for some function b and positive constant a . Then, one defines the set

$$\Gamma_{2k} = \{\gamma \in C_\beta, \quad ab = 0\},$$

where the curve γ in C_β is made by k pieces along ξ and k jumps on $\pm v$ (see Figure 1 for a typical element of Γ_{10}). This set will be the limiting set of the flow and we can again consider the functional J on it (after passing to the limiting process). The set of variations at infinity is defined as $\bigcup_{k \geq 0} \Gamma_{2k}$ and on this set the functional at infinity reads as

$$J_\infty(\gamma) = \sum_{k=0}^{k=\infty} a_k.$$

The critical points of this functional are what Bahri called critical points at infinity. Next, he gave an exact geometric definition of these critical points by introducing the following definitions. First, let ϕ_s be the transport map of v , namely the one parameter group of diffeomorphisms generated by the flow

$$\frac{d}{ds}(\phi_s(x)) = v_{\phi_s(x)}, \quad \phi_0(x) = x.$$

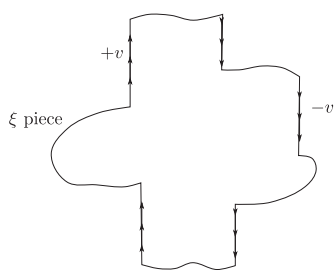


Figure 1. Typical element of Γ_{10}

Then, one says that a v -jump between two points x_0 and $x_1 = x(s_1)$, $s_1 \neq 0$, is a v -jump between *conjugate points* if the following holds:

$$(\phi_{s_1}^* \alpha)_{x_1} = \alpha_{x_0}.$$

In other words, conjugate points are points on the same v -orbit such that the form α is transported onto itself by the transport map along v .

Also, a ξ -piece $[x_0; x_1]$ of an orbit is *characteristic* if v completes an exact number $k \in \mathbb{Z}$ of half revolutions from x_0 to x_1 .

Now, Bahri gave the following characterisation for critical points at infinity.

A curve in $\bigcup_{k \geq 0} \Gamma_{2k}$ is a critical point at infinity if it satisfies one of the following assertions:

- (1) The v -jumps are between conjugate points. These critical points are called *true* critical points at infinity.
- (2) The ξ -pieces have characteristic length and, in addition, the v -jumps send $\ker(\alpha)$ to itself.

The main result of Bahri, in this setting, is the understanding of how these critical points at infinity contribute to the change of topology in the variational problem.

A major difference to the Yamabe-type problems is that, in this situation, there can be characteristic pieces where a single curve can behave as many superposed critical points at infinity, with different indices, and they can interact [7].

Violation of Fredholm. The second difficulty that Bahri tackled in this variational problem was the violation of the Fredholm assumption [7, 17]. Let us briefly recall the definition of a Fredholm operator and a basic example. Let X and Y be two Banach spaces and $F : X \rightarrow Y$ be a bounded linear operator. F is called Fredholm if its kernel and co-kernel are of finite dimension and, in that case, the Fredholm index is the difference between these two dimensions. Fredholm operators are close cousins of invertible operators, in the sense that the non-invertibility of F is mild. As an example, if we take $X = Y$ separable Hilbert spaces and $F = Id + K$, where Id is the identity and K is a compact operator (in this case F has index 0), then the *Fredholm alternative* says that the problem $F(x) = y$ is solvable if and only if y is orthogonal to the kernel of F , that is, y satisfies a finite number of orthogonality conditions. This allows, in many cases, the reduction from an infinite dimensional problem to a finite dimensional one: first solving orthogonally to the kernel (since we have invertibility) and then solving in the kernel, which is a finite dimensional space. Now, we say that a nonlinear operator F is Fredholm if its differential dF is Fredholm at every point. For these operators, one has a version of the implicit function theorem, which is needed in order to apply a Morse theory ap-

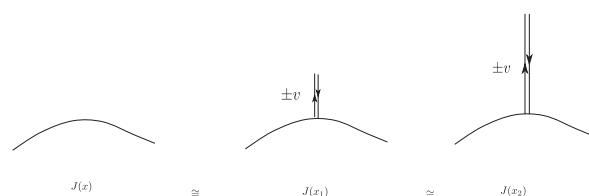


Figure 2. The functional and the v -jumps

proach to variational problems and make use of transversality, gluing and perturbations.

In his work, Bahri found simple a criterion to check if violation of the Fredholm property occurs or not based on some properties of the transport map ϕ . The main idea comes from the fact that the functional does not control b properly. Therefore, it might be an infinite space of perturbations that are *invisible* to the linearised operator. In fact, by looking at the functional J in the larger space

$$C_\beta^+ = \{x \in H^1(S^1; M) \text{ s.t. } \beta(\dot{x}) = 0; \alpha(\dot{x}) \geq 0\},$$

one can see that it remains insensitive to the introduction of a $\pm v$ piece (see Figure 2). Moreover, the modified functional is Fredholm in the following way:

$$\tilde{J}(x) = \int_0^1 \alpha(\dot{x})(t)dt + \delta \log(1 + \int_0^1 |b(t)|dt),$$

since one has control of b , as shown in [7]. Now, let x be a curve that is transverse to v and, at a point $x(t_0)$, one introduces a “back and forth” v piece of length s . Let x_ϵ be the curve obtained by introducing a small “opening” piece of length ϵ between the two v pieces. Then, one has

$$J(x_\epsilon) = J(x) - \epsilon(\alpha_{x(t_0)}(d\phi_{-s}(\xi)) - 1) + o(\epsilon).$$

Thus, if there exists $s > 0$ such that $\alpha(\phi_{-s}(\xi)) > 1$ then one would have a decreasing direction from the level $J(x)$ and one would be able to bypass a critical point without changing the topology, even though it has a finite Morse index, and this is due exactly to the violation of the Fredholm condition. Therefore, the criterion is the following.

If $\phi_{-s}^(\alpha)(\xi) < 1$, for every $s \neq 0$, then J satisfies the Fredholm condition.*

For instance, the Fredholm assumption is violated for the standard contact structure α_0 and the first exotic structure of Gonzalo and Varela defined on S^3 and for a family of tight contact structures on the torus T^3 .

In particular, Bahri pointed out the *point to circle* relations, where a circle of critical points, under the S^1 -action, can have Morse relations with a single point. The fact is that, during the perturbation procedure, the S^1 -action could be lost. In order to explain and give some applications of these phenomena, Bahri made explicit computations on two main examples: the sphere equipped with its standard contact form and with the first overtwisted contact form of Gonzalo-Varela. In his works [5], he showed how it is possible to overcome the Fredholm violation by carefully studying the Fadell-Rabinowitz index of different sets bounding the critical points. In particular, it led to another proof of the Weinstein conjecture on the sphere.

Co-authors of Abbas Bahri

Haim Brezis (1980, 1988, 1996), Henri Berestycki (1980, 1981, 1981, 1984, 1984), Luis Sanchez (1981), Jean Michel Coron (1985, 1985, 1985, 1986,

1988, 1991), Pierre-Louis Lions (1985, 1988, 1992, 1997), Paul H Rabinowitz (1989, 1989, 1990, 1990, 1990, 1991), Yanyan Li (1990, 1995), Biancamaria D’Onofrio (1992), Olivier Rey (1995), Thierry Aubin (1997, 1997, 1999), Iskander A. Taimanov (1998), Sagun Chanillo (2001), Yongzhong Xu (2007, 2008).

PhD Students of Abbas Bahri

Hasna Riahi (Rutgers University, New Jersey, 1993), Yansong Chen (Rutgers University, New Jersey, 1995), Mohameden Ahmedou (ENIT, Tunisia, 1998), Khalil El Mehdi (ENIT, Tunisia, 1998), Hichem Chtioui (ENIT, Tunisia, 1998), Hammami Mokhless (ENIT, Tunisia, 1998), Mohamed Ben Ayed (ENIT, Tunisia, 1998), Abdellaziz Harrabi (ENIT, Tunisia, 2000), Abdelbaki Selmi (ENIT, Tunisia, 2000), Salem Rebhi (ENIT, Tunisia, 2000), Ridha Yacoub (ENIT, Tunisia, 2002), Yongzhong Xu (Rutgers University, New Jersey, 2005), Ali Maalaoui (Rutgers University, New Jersey, 2013).

Acknowledgment

We are grateful to Diana and Salima Bahri for their valuable help and to Lucia di Vizio, Philippe Souplet and Hatem Zaag for the suggestion to publish this paper in the EMS Newsletter.

Bibliography

[1] Ahmedou M. O., Conformal deformations of Riemannian metrics via “critical point theory at infinity”: the conformally flat case with umbilic boundary. (English summary) Non-compact problems at the intersection of geometry, analysis, and topology, 1–17, Contemp. Math., 350, Amer. Math. Soc., Providence, RI, 2004.

[2] Aubin T. and Bahri A., *A topological hypothesis for the problem of prescribed scalar curvature*. J. Math. Pures Appl. (9) 76 (1997), no. 10, 843–850.

[3] Bahri A., *Un problème variationnel sans compacité dans la géométrie de contact (French) [A variational problem without compactness in contact geometry]*, C. R. Acad. Sci. Paris Sér. I Math. 299 (1984), no. 15, 757–760.

[4] Bahri A., *Another proof of the Yamabe conjecture for locally conformally flat manifolds*, Nonlinear Anal. 20 (1993), no. 10, 1261–1278.

[5] Bahri A., *A Linking/ S^1 -equivariant Variational Argument in the Space of Dual Legendrian Curves and the Proof of the Weinstein Conjecture on S^3 “in the Large”*, Advanced Nonlinear Studies 15 (2015), no. 3, 497–526.

[6] Bahri A., *Classical and quantum periodic motions of multiply polarized spin particles*, Pitman Research Notes in Mathematics Series, 378. Longman, Harlow, 1998.

[7] Bahri A., *Flow lines and algebraic invariants in contact form geometry*, Progress in Nonlinear Differential Equations and their Applications, 53. Birkhuser Boston, Inc., Boston, MA, 2003.

[8] Bahri A., *Critical points at infinity in some variational problems*, Research Notes in Mathematics, 182, Longman-Pitman, London, 1989.

[9] Bahri A., *Un problème variationnel sans compacité dans la géométrie de contact*, Comptes Rendus Mathématique Académie des Sciences, Paris, Série I 299 (1984) 754–760.

[10] Bahri A., *Pseudo-orbits of Contact Forms*, Pitman Research Notes in Mathematics Series, 173. Longman Scientific & Technical, Harlow, 1988.

[11] Bahri A., *An invariant for Yamabe-type flows with applications to scalar-curvature problems in high dimension*. A celebration of John F. Nash, Jr. Duke Math. J. 81 (1996), no. 2, 323–466.

[12] Bahri A. and Brezis H., *Equations elliptiques non linéaires sur des variétés avec exposant de Sobolev critique*. C. R. Acad. Sci. Paris Ser. I Math. 307 (1988), no. 11, 573–576.

[13] Bahri A. and Coron J. M., *On a nonlinear elliptic equation involving the critical Sobolev exponent: the effect of the topol-*

ogy of the domain, Comm. Pure Appl. Math. 41-3 (1988), 253–294.

[14] Bahri A. and Coron J. M., *The scalar-curvature problem on the standard three-dimensional sphere*, J. Funct. Anal. 95 (1991), no. 1, 106–172.

[15] Bahri A. and Lions P.-L., *On the existence of a positive solution of semilinear elliptic equations in unbounded domains*, Ann. Inst. H. Poincaré Anal. Non Linéaire 14 (1997), no. 3, 365–413.

[16] Bahri A. and Rabinowitz P., *Periodic solutions of Hamiltonian systems of 3-body type*, Ann. Inst. Poincaré, Anal. non linéaire 8(1991), 561–649.

[17] Bahri A. and Xu Y., *Recent progress in conformal geometry*, ICP Advanced Texts in Mathematics, 1. Imperial College Press, London, 2007.

[18] Ben Ayed M., Chtioui H. and Hammami M., *The scalar-curvature problem on higher-dimensional spheres*, Duke Math. J. 93 (1998), no. 2, 379–424.

[19] Ben Ayed M., Chtioui H. and Hammami M., *A Morse lemma at infinity for Yamabe type problems on domains*, Ann. Inst. H. Poincaré Anal. Non Linéaire 20 (2003), no. 4, 543–577.

[20] Brezis H. and Coron J.-M., *Convergence of solutions of H-systems or how to blow bubbles*, Arch. Rational Mech. Anal. 89 (1985), 21–56.

[21] Bourguignon J. P. and Ezin J. P., *Scalar curvature functions in a conformal class of metrics and conformal transformations*, Trans. Amer. Math. Soc. 301 (1987), no. 2, 723–736.

[22] Chen Y., *On a nonlinear elliptic equation involving the critical Sobolev exponent*, Nonlinear Anal. 33 (1998), 41–49.

[23] Ding W. Y., *Positive solutions of $\Delta u + u^{\frac{n+2}{n-2}} = 0$ on contractible domains*, J. Partial Differential Equations 2 (1989), no. 4, 83–88.

[24] Escobar J. and Schoen R., *Conformal metrics with prescribed scalar curvature*, Invent. Math. 86 (1986), 243–254.

[25] Kazdan J. L. and Warner F. W., *Curvature functions on compact 2-manifolds*, Ann. of Math. 99 (1974), 14–47.

[26] Gamara N., *The CR–Yamabe conjecture, the case $n = 1$* , J. Eur. Math. Soc. 3(2001), 105–137.

[27] Gamara N. and Yacoub R., *CR Yamabe conjecture – the conformally flat case*. Pacific, J. Math. 201 (2001), no. 1, 121–175.

[28] Schoen R. and Yau S. T., *On the proof of the positive mass conjecture in general relativity*, Comm. Math. Phys. 65 (1979), no. 1, 45–76

[29] Schoen R. and Yau S. T., *Proof of the positive mass theorem. II*, Comm. Math. Phys. 79 (1981), 231–260.

[30] Struwe M. *A global compactness result for elliptic boundary value problems involving limiting nonlinearities*, Math. Z. 187 (1984), no. 4, 511–517.

[31] Thom R., *Sous-variétés et classes d’homologie des variétés différentiables. II. Résultats et applications*, C. R. Acad. Sci. Paris 236 (1953), 573–575.



f.l.t.r.:
 Mohameden
 Ahmedou,
 Mohamed Ben Ayed,
 Ali Maalaoui and
 Vittorio Martino

Mohameden Ahmedou [mohameden.ahmedou@math.uni-giessen.de] is a professor at the Mathematisches Institut, Giessen University, Germany.
 Mohamed Ben Ayed [mohamed.benayed@fss.rnu.tn] is a professor at the Faculté des Sciences, Sfax University, Tunisia.
 Ali Maalaoui [ali.maalaoui@aurak.ae] is an assistant professor at the American University of Ras Al Khaimah, UAE.
 Vittorio Martino [vittorio.martino3@unibo.it] is an assistant professor at the Università di Bologna, Italy.

Beppo Levi's Mathematics Papers Return to Italy

Maurizio Mattaliano (Institute of Applied Calculus, Rome, Italy)

In June 2015, Beppo Levi's (1875–1961) "Italian" papers reached Rome from Buenos Aires, after being donated by the mathematician's daughter Emilia (Mia Resta) to the Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC – *Institute of Applied Calculus*), which is under the directorship of Roberto Natalini and is part of the Consiglio Nazionale delle Ricerche (CNR – *National Research Council*).

Ever since 1939, the papers had been in Argentina, where the Italian mathematician had migrated due to infamous racial persecutions. The Italian Racial Laws were announced on 18 September 1938 (but had already been applied administratively since 1 September) directly from the balcony of the City Hall of Trieste by Benito Mussolini and were then ratified with the Legislative Decree of 17 November 1938. Article 13 of these laws explicitly forbade Jewish people being employed by public authorities, as well as state and state-owned companies.

The 10 legal personalities who signed the ridiculous and appalling *Manifesto of Race* (on 14 July 1938), de facto taking a great historical and moral responsibility for the whole affair, were all part of the Italian scientific community. Reading through the list of signatories, there are sadly the names of many of Levi's colleagues – well known and established university professors who committed themselves to the dominant ideology and politics.

Those were the days of good and bad words, for and against the measures that indiscriminately affected all Italian Jews. Among the "good" words, it is first of all right to recall those of Raffaele Gurrieri (1862–1944), Editor-in-Chief of the journal *L'Università italiana* and the only professor in Italy who had the courage and the spirit to express his dissent regarding the absurdities contained in those laws in one of his articles:

"With political hate, fuelled on past injustices, racial hate, which is even more terrible and harmful, shall disappear too; hate that has no reason to exist because in this world there is room for all of us... Italy has the great merit of never having felt deeply, nor nurtured, racial hate: let's treasure this virtue."

His was an isolated voice, which was immediately stifled by the fascist regime because Gurrieri was soon removed from directing the journal he had funded. Among the bad words, the ones that stand out, because of their idiocy, are the ones uttered by Father Agostino Gemelli (1878–1959) on 9 January 1939 from the great lecture hall of the University of Bologna. This same hall had hosted the noble Levi himself various times and it was a place he was now forbidden even to enter:

"It is without a doubt a tragic and painful situation the one of those who can't, because of their blood or religion, be part of this great country; a tragic situation in which we see once again, as many times over the centuries, the execution of a sentence that the deicidal people have taken upon themselves and because of which they wander the world, unable to find the peace of a homeland, while the consequences of the horrible crime will persecute them everywhere and for all of time."

The *great country* had expelled Levi from his university office, violating the basic human and civil rights that he benefited from as an Italian citizen; it had deprived him of his identity, deleting his name from the catalogues of all Italian libraries, from the phone books and every other place; it had banished his children from public schools and their future now relied on nothing and was enveloped in an impenetrable black cloud.

The *great country* had trampled the dignity of every Italian Jew with an endless number of brutal measures that were soon to escalate to acts of verbal and physical violence, reaching its peak of unimaginable horror with the deportation of many children, women and men to the Nazi *lagers*, where almost all of them met their death. Insanity had infected a portion of the world and wounded all of humanity.

This is how the first part of Levi's life ended, in a dramatic and unexpected way, when he had to choose to go into exile and leave the *great country* where he was born and where he would never return.

A new dawn was waiting for him on the horizon and a new homeland awaited him on the other side of the ocean: Argentina. This was a large and generous country that would greet him with open arms, where it would be possible for him and his family to return to leading a normal life and to rebuild, day after day with renewed hope, the certainty and safety that had melted in Italy like snow in the sun.

Levi had been invited to Argentina by the University of Rosario, where he would be the head of the annexed Institute of Mathematics for many years. An avid scholar of geometry and logic and a world renowned analyst, but also a pragmatic man with great university experience (gained over many years of fruitful work as head and professor of his faculty in Italy), Levi would bring a breath of fresh air to the Argentine School of Mathematics. The South American cultural and intellectual climate was one of the most fertile and stimulating in which to plant and spread new ideas and the University of Rosario was the most appropriate place in which to do it, surrounded by outstanding scientists and in the best work-

ing conditions. Among the brilliant initiatives of Levi, it is worth mentioning his editorial efforts, such as the foundation of the journal *Mathematicae Notae*.

Leaving Trieste for Buenos Aires on the Italian ocean liner Oceania, Levi, among his essential documents, took with him a selection of mathematics papers that were among the most important of his career as a scholar and scientist, the same papers that today, after 76 years, are returning to Italy. These papers are now yellowed with age, made old by history and ancient by glory but which have, as has already been established with this return trip, a highly symbolic value for the entire international scientific community – a value that transcends their interesting content.

When he arrived in Argentina, Levi even found the time and means to take care of the Italian Jews that had chosen too late to go into exile. Among the friends and acquaintances who asked him for advice or for real help, one name stands out – the name of someone we all know and love: Vito Volterra (1860–1940), the unforgotten and unforgettable teacher of many generations of scientists and an exemplary model of coherence of life and intellectual honesty.

The letter that follows,¹ sent by Tullio Levi-Civita (1873–1941) on 23 July 1940, is a testimony to how Levi acted to facilitate the expatriation of Enrico Volterra (1905–1973), Vito's youngest child, who was already a pupil of Levi-Civita and who had sought refuge in England awaiting a more stable solution. As shown in the correspondence between the Volterras (Vito and Enrico) and Levi-Civita, and this precious letter of Levi, the mobilisation was wide-ranging and also involved – via Agostino Gemelli – the highest ecclesiastical authorities.

“Dear Professor, About 10 days ago I received your correspondence (of the 26/6) with your recommendation regarding Volterra. I have immediately taken care of it, as I had already done shortly before. The path suggested by the Dean is a bit long; that is, because these relations involve the Curia, to put everything in the hands of the subdean, who seems to have a very good relationship with them. This causes me to receive answers very slowly and unfortunately with results not different than the ones you have been obtaining until now; that is only declarations of good will and nothing else. I haven't received a response yet to my last attempt. I don't have any news from England either. I confirm that I am and will be doing all that I can, it is just a pity that Volterra wasn't able to find a way to get to the other side of the pond by his own means as I had urged him to many times. I send you my best regards and I should be grateful if you could extend my greetings to professors Enriques and Volterra. Yours, B. Levi.”

At the end of World War II, in a Europe that was finally free of the terrible fascist and Nazi dictatorships, when normal postal communications resumed, Levi would

start to write to Italy again, to give news of himself and his large family, composed of his wife Albina Bachi and their three children Giulio, Laura and Emilia. One of the first people he wrote to was his old friend Mauro Picone (1885–1977), a high-profile mathematician during the fascist period because of his technical and scientific contribution to Mussolini's war machine, with the sophisticated and complex mathematical calculations that were carried out by the computers at the IAC, the Institute of Applied Calculus that he had founded in 1927 (the first of its kind in the world) and which today carries Levi's name. On the other hand, Picone was also the person who, after the notorious Racial Laws, didn't hesitate to offer the post of researcher in his institute to Alessandro Terracini (1889–1968) – who preferred to emigrate to Brazil – and did not fail to send his moral and material help from Rome to another Jewish mathematician Guido Ascoli (1887–1957), who was left isolated in Turin. He did so by sending money and more, and his help was so consistent and substantial as to lead the mathematician from Turin to write a letter² to Picone in September 1943:

“I thank you profusely for your financial reassurance and for your promises, of which I appreciate all your exceptional kindness. I will never forget that I have found a real friend in you, in the most ungrateful of times.”

Before Levi's letter arrived in Italy, Picone had sent a long essay to the Minister of Education, endorsed by many scientists, with the aim of awakening the Italian Government to the financial struggles that prevented Terracini from returning from Brazil, as well as many other Jewish Italians scattered all over the world who were not able to return from their enforced exile. The Jewish mathematician Beniamino Segre (1903–1977), who was facing the same problems, had written to Picone from Turin on 2 July 1946:

“...I am delighted at the idea of finally resuming the relationships that were so abruptly torn apart. I am very glad to read about Terracini. My situation is no different: my wife and my children have remained in Manchester, and are waiting for me to solve a series of problems, most of which are financial, before they can join me. One of these problems relates to the total or partial reimbursement of the expenses for the trip and the shipping of luggage, that I have requested long ago via the Embassy in London, where they have eagerly supported my request. I would be ever so grateful if I could count on your valuable support as well...”

When the Racial Laws were abrogated with the Royal Decrees of 20 January 1944, the problem for Jewish Italians was no longer how to leave but how to return to Italy. It is clear that Picone was a reliable colleague and valuable friend to turn to for this purpose and the following paragraphs aim to explain why.

¹ Historical Archive of the Lincean Academy. Dossier Volterra.

² Historical “Mauro Picone” Archive. Dossier Guido Ascoli.

Contrary to what a recent historiography has tried to state about the alleged role Picone played during the fascist period – accusing him of various forms of cooperation with the regime – at the end of the war, there were neither the necessary conditions nor any new element to involve him in the “purge” to which many university professors had come near to, among them the powerful mathematician and renowned antagonist of Picone, Francesco Severi (1879–1961). Therefore, the historical reality appears quite different from the one imagined if it is also taken into consideration that, in the post-war period, Picone would be involved as a full member of various organisations that would take care of the reconstruction of the country. On 23 March 1946, the renowned antifascist and economist Antonio Pesenti (1910–1973), then President of the *Centro economico per la ricostruzione* (“Centre for Economic Reconstruction”), wanted to have him on his side to be part of the commission that was in charge of reorganising scientific research in Italy. The commission included some prominent personalities of the Italian cultural landscape, with the implicit condition that none of them had been involved with fascism. Maybe it is useful to add (especially to clarify for those who may have formed a different opinion on the Sicilian mathematician from other readings) that after 8 September he taught in partisan schools and was also the teacher and protector of the antifascist mathematician Renato Caccioppoli (1904–1959). In conclusion, these are the actual facts that everyone knew back in the post-war period and that can’t be invalidated by an unfortunate choice of words uttered by Picone himself during the “rituals” that the regime forced on the universities. In addition, there are some very significant testimonies, for example the one that follows in a letter that Guido Ascoli³ sent to Picone on 18 October 1945, that better explain the fascist “creed” of Picone, which seems shrouded by opportunism in the words of Ascoli:

“In the past few years, many things, crushing my natural optimism, have roused in me a great disesteem in men, and in particular for those who should, because of their intellect, be an example of rectitude and character; and the participation in the purge of the University of Milan, putting me in contact with many small and huge acts of cowardice, has given me the final blow. Therefore, finding a good person among the ex-fascist academics, who after all used fascism only with the aim of realising a good deed and a great idea, which does Italy a great credit outside and above any sectarianism, is a great consolation. I was delighted to see that your institution has found the consideration it deserves in the new political environment, and that keeping it efficient and in continuous development is always uppermost in your mind.”

These are some of the reasons that explain and answer the previous question about why the skilful and influential Picone was chosen in those difficult times by Jewish mathematicians needing effective and unselfish help.

³ Historical “Mauro Picone” Archive. Dossier Guido Ascoli.

Therefore, it will be apparent that Levi’s “maths papers” are headed to Rome to add value to the historical “Mauro Picone” archive not by chance or by a trick of fate; in fact, this is the most appropriate location for them, where they can be forever next to the originals of the wonderful mementos that Picone kept of Volterra, Ascoli and Fubini, as well as many other documents that commemorate the good relationships that he had with Jewish mathematicians such as Federico Enriques (1871–1946), Guido Castelnuovo (1865–1952) and the previously mentioned Levi-Civita.

On 28 March 1946,⁴ when Picone replied to Beppo Levi’s letter, the extremely poor Italian Government had yet to give its opinion regarding the memo Picone had sent about the return of Italian scientists who had found shelter abroad after the Racial Laws, nor, as far as we know, would they ever reply:

“Dearest Beppo, you can imagine our joy at hearing from you. I would have liked to reply right away [...] but [...] the wish to be able to give you positive news about a ministerial decision, which we requested, regarding the repatriation of our friends in America, has caused me to delay my answer even further. I was hoping to be able to tell you about an action of our Government to provide the Italian scientists who had to leave Italy during the fascist regime with the means necessary to bear the cost of the return trip with their families. But unfortunately the decision seems still far from being reached. As you can imagine, the Italian scientific landscape strongly needs the return of our Jewish friends who have, with their work, very much set the foundation for scientific research in various sectors, and in particular in mathematics. I would definitely not suggest that you make the sacrifice needed to come back, because unfortunately there are still many obstacles to the return to a normal life in our country! [...] In the meanwhile, a sad bereavement befell the Italian mathematical community: you will know that Fubini has died. [...]”

Guido Fubini (1879–1943), family friend of Levi’s, had immigrated to Princeton in the US right after the issuing of the Racial Laws; from there, on 31 January 1940,⁵ he sent his news to Picone:

“I am very happy here; I am staying in a nice cottage in between parks and avenues for a very reasonable price. The university is like a park with cottages scattered all over it: the library ... is extraordinary. You can find anything, old or new. The congress of New York is no more (I think). Otherwise I would have written to you to not come here, because you probably would have found a reception that would have been of hindrance. [...] I have been working: I have works about to be published in the Annals and elsewhere. The colleagues here are so nice, so kind, so affectionate. It would be

⁴ Historical Archive. Lincean Academy.

⁵ Historical “Mauro Picone” Archive. Dossier Guido Fubini.

impossible to find any better (Alexander, Lefschetz, Veblen, Weil, Einstein, Wedderburn, V. Neumann). It is a whole new world here: topology (Alexander and Lefschetz, with first-order results), V. Neumann with his essential discoveries on linear operators, Wedderburn in algebra, etc. I have realised (too late, at my age) that I am an ignorant. But better late than ever. [...]"

Although this article has included many elements and points that associate the name of Levi with that of Picone, there are even more that could have been added. Taking a step back, the following concerns an extraordinary character who had a critical influence on the life and mathematical future of both of them: Levi's brilliant brother, Eugenio Elia Levi (1885–1917).

Beppo Levi was born in Turin on 14 May 1875, son of Giulio Giacomo and Diamantina Pugliese. His father was a very cultured lawyer who had to study in France before the Albertine Statute. On the other hand, Levi was one of 51 Jewish students to graduate from one of the universities of Turin in the last 30 years of the 1800s (recorded in the chronicles of the journal *Vessillo israelitico*) and the second one to graduate in mathematics (in 1892).⁶ After the death of his father in 1898, he had to take care of his large family, consisting of his mother and eight brothers, the second to last of which was Eugenio Elia. Beppo was the first one to realise the genius of his little brother and he was also the one who made him enrol, thanks to the help of Volterra, at the *Scuola Normale Superiore* of Pisa in 1900, from which he graduated with a first class degree in mathematics in 1904. Eugenio Elia remained in Pisa for a few more years as an assistant lecturer to Ulisse Dini. During that time, he became the teacher, mentor and one of the greatest friends of young Picone, who was also studying at the *Normale*.

At this point, the article must come to a close for reasons of space but for anyone interested in learning more about Eugenio Elia Levi, there are two books entirely dedicated to him that will be published soon.⁷ These books will speak exhaustively of the mathematical skill of Eugenio Elia and of how he helped many mathematicians of his time, among them Picone.

On the other hand, it is worth exploring the relationship (which was not only personal but professional) that developed between the Levi brothers, united by their passion for mathematics but also by a common vision of the world, which brought them to side with the reformist socialists during the Great War, invoking the entrance of Italy into the conflict. Eugenio Elia, who left as a volunteer, died on the front line on 28 October 1917, hit on the back of the head with a precise shot from an Austrian sniper.

⁶ See B. Maida, *Dal ghetto alla città [From the ghetto to the city]*, published by Silvio Zamorani, Turin, 2001.

⁷ See A. Celli, M. Mattaliano, *Eugenio Elia Levi, le speranze perdute della matematica italiana [Eugenio Elia Levi, the lost hopes of Italian mathematics]*, EGEA, Milan 2015, and A. Celli, M. Mattaliano, *Eugenio Elia Levi: I documenti dimenticati [Eugenio Elia Levi: The Neglected Documents]*, CNR Editions, Rome, soon to be published.

With the death of his brother Eugenio Elia, Beppo Levi lost an important part of himself that completed and gave value to all his final actions and thoughts. This was a loss that was first of all personal but also intellectual, which can be appreciated by reading the mournful words he wrote in a letter⁸ to the famous pedagogue Giuseppe Lombardo Radice (1879–1938) on 6 February 1918:

"I thank you and am very grateful for your thoughts for me and Eugenio: maybe no one understood this intimate intellectual fondness that you talk about: no one said a single word about the impossibility of us being separated. For a long time after the tragedy I have continued to talk to him and I felt like I was waiting for his return, knowing at the same time that this was impossible, while I was emptying that house in Genoa. And as time passes I become more and more aware of my solitude."

In 1956, Beppo Levi would be given the Feltrinelli award for Physical, Mathematical and Natural Sciences by the Lincean Academy. This recognition was strongly championed by Picone, who at the time was administrator of the academy and who would shortly curate the collection of the mathematical works of Eugenio Elia Levi in two volumes to be published in 1959 and 1960 by the Italian Mathematical Union.

Beppo Levi would barely have the time to appreciate this new effort of Picone: he would die in Rosario on 28 August 1961.



Maurizio Mattaliano is the director of the historic archive "Mauro Picone" and in that position he has edited and published various books and numerous articles that deal with the history of mathematics and computer science. His most recent book is "Eugenio Elia Levi. Le speranze perdute della matematica italiana" (Milan, EGEA, 2015). He is a collaborator with the Centro Pristem at Bocconi University. He is a member of the scientific committee of a new book series to be published by the Italian National Research Council entitled "Matematica e dintorni".

⁸ Private Archive of the Momigliano-Levi family.

Historical Archive of the Istituto per le Applicazioni del Calcolo “Mauro Picone” (IAC – Institute of Applied Calculus)

Maurizio Mattaliano (Institute of Applied Calculus, Rome, Italy)

The *Istituto per le Applicazioni del Calcolo* “Mauro Picone” (IAC – Institute of Applied Calculus), under the directorship of Roberto Natalini and part of the *Consiglio Nazionale delle Ricerche* (CNR – Italian National Research Council), will celebrate its 90th anniversary in 2017.

The IAC was founded in Naples in 1927 by the mathematician Mauro Picone at the *Istituto di Calcolo Infinitesimale* (Institute of Infinitesimal Calculus) of the University of Naples and was then moved to Rome in 1932 with the name *Istituto di Calcolo del Consiglio Nazionale delle Ricerche* (Institute of Calculus of the Italian National Research Council).

The IAC, up until the present day, has maintained the high expectations and tradition of seriousness of purpose on which the institute was founded, rendering it useful for experimental sciences and techniques, as well as for the progress of some branches of pure mathematics. The institute was a completely original idea of its founder, who made the IAC the first institute of calculus in the world and a precursor to the direction that modern research into applied mathematics would later take when pursued by other institutes of calculus created in its image outside Italy.

Many famous scientists contributed to the work of the IAC in the first half of the 20th century. The most noteworthy among the physicists were: E. Fermi, G. Krall, L. Sobrero, M. Salvadori, C. Minelli, R. Einaudi, C. Tolotti, A. Signorini, E. Amaldi, G. Bernardini, G. Grioli, P.G. Bordononi and W. Gross; and, among the scholars of analysis and calculus, Picone himself, R. Caccioppoli, E. De Giorgi, G. Scorza-Dragoni, G. Cimmino, C. Miranda, F. Conforto, W. Gröbner, L. Cesari, D. Mangeron, S. Faedo, T. Viola, L. Tonelli, A. Ghizzetti, L. Amerio, E. Batschelet, G. Fichera, M. Sadosky, L. Stankiewicz, N. Zeilon, E. Baiada, H. Buckner and P. Lesky.

As a testament to the scientific and technical work of the institute over these years, there are hundreds of papers dealing with various different aspects of pure and applied mathematics. During this time, the IAC explored countless areas of interest, which are impressive due to both the depth of the results achieved as well as their diversity. They spanned a large range of subjects: mechanics and mechanical engineering; atomic physics; cosmic rays; optics and optical engineering; chemistry; thermodynamics and thermal engineering; electromagnetism;

electrotechnics; hydrodynamics; hydraulics and hydraulic engineering; engineering and construction of buildings, bridges, dams, railways and mobile rail technology; naval and aeronautical engineering; astronomy; geodesy; geophysics; ballistics and shooting techniques; statistics; finance; mathematical economics; tabulation of functions and many more.

There were also many collaborations of various kinds between the IAC and research institutes outside Italy. For example, in 1951, various institutes turned to the IAC to solve their difficult calculus problems: the Institut de Mécanique des Fluides of the Université d’Aix-Marseille, the Institut für Mathematik in Innsbruck, the Instytut Matematyki of the Uniwersytetu Jagiellońskiego in Krakow, the Instytut Matematyczny of the Uniwersytet Wrocławski, the Institute for Numerical Analysis in Los Angeles, the National Bureau of Standards in the USA, the Department of Civil Engineering of Columbia University, the Department of Mechanics of the Illinois Institute of Technology (Chicago), the International Radio Consultative Committee, Cambridge University and many more (which won’t be listed due to restrictions on space).

One of the aspects of the IAC that is worth emphasising in this centenary of World War I is that the history of the institute itself has its roots in the Great War, since Mauro Picone was called to arms in April 1916 and was sent to the front. Strangely, but fortunately, he never had to fire a shot. However, his mathematical abilities were used in the field of ballistics to create new trajectory charts. He carried out this task in the best possible way but he also discovered the huge potential of numerical calculus and experienced a sort of spiritual awakening – as one of his best pupils Carlo Miranda called it – which influenced him for the rest of his life. It was then that he started developing the idea of creating an institute where the potential of calculus could be made available to the experimental and technical sciences.

Picone supported fascism early on and his reasons are well summarised in an unusual pamphlet published in 1927 about the future outlook of the yet-unborn IAC, in which the mathematician states: “...our Country is lucky to have the government of BENITO MUSSOLINI promoting, subsidising and inspiring all the good initiatives that can increase the strength and the moral and material patrimony of the nation, we have to be honest” [1].

Therefore, the IAC was born and flourished under the shadow of fascism, which abolished democracy in Italy for 20 years. Nevertheless, these were prolific years for the IAC, which, thanks to its expertise, worked tirelessly in collaboration with private and public institutions to produce a tremendous amount of work. The level of activity would become even more intense during World War II, when commissions from the Ministry of War and especially from the Ministry of Aeronautics increased substantially, with the latter requesting the compilation of “ballistics trajectory charts for nosediving airplanes” from low- and medium-altitude. It was a complex job that the IAC carried out so well in aid of the war that it convinced the Nazis to establish an institute similar to the one in Rome but for aeronautics. The *Luftwaffen-Institut für Mathematik* was established in Braunschweig, Germany, in 1941 and was entrusted to Wolfgang Gröbner, a former pupil of Picone [2], [3].

It is for these reasons, and because of all the distinctive characteristics of the IAC that have been mentioned (albeit briefly), that its historical archive can be considered unique in the context of international archives of mathematics. It is truly a piece of cultural heritage that should be protected and preserved.

The cornerstone of the whole archive is Mauro Picone, with the hundreds of letters he exchanged with the great mathematicians and scientists of his time, some of the most famous and scientifically significant being: John von Neumann, Jacques Louis Lions, Enrico Fermi, Johannes Gualtherus van der Corput, Alexander Weinstein, Olga Taussky-Todd and Gaston Maurice Julia.

But this is not all that the archive contains. It also stores an impressive number of exquisite documents of various kinds. The number of documents can be deduced from the fact that the history of the IAC stretches over most of the 20th century, following an extraordinary path defined by its scientific successes. Under the guidance of its founder, in the 1950s the IAC became one of the best known and internationally famous mathematical institutes. Internationally renowned mathematicians, such as Renato Caccioppoli and Ennio De Giorgi, trained under Picone’s guidance.

Here it is appropriate to give an example, perhaps the best one among all those possible, of the potential of the archive of the IAC and of the contribution it can make to the history of mathematics. This example is a book curated by A. Guerraggio, M. Mattaliano and P. Nastasi, published in 2007 by the Polish Academy of Sciences in Rome and entitled *Mauro Picone e i Matematici Polacchi (1937–1961)* (“Mauro Picone and the Polish Mathematicians”) [4]. This book contains some unique correspondence (stored in the archive) between Picone and the mathematicians of that country during the years indicated in the title. These Polish mathematicians, driven by their regained independence, were creating one of the world’s foremost academies in the period between the two wars. The Nazis would decimate this academy with the alarming massacre of hundreds of university professors, whose names are too numerous and too painful to list. Among the correspondence contained in the aforementioned

book, the (copious) exchange with the famous mathematician Waclaw Sierpiński stands out. Among their letters, one in particular will be mentioned here because of how touching it is: the one that Sierpiński sent to Picone from Krakow on 12 October 1945 [4], in which the mathematician lists his colleagues who had been killed by the Nazis or who had died due to the suffering endured during the war, such as the undisputed genius Stefan Banach.

The archive also contains Mauro Picone’s personal letters, which were donated to the IAC after his death according to his will, together with his private library.

For about a year, the archive has been undergoing its first and partial archival organisation. The main obstacles to this process essentially depend on the nature of a large proportion of the documents – about 60% of them – in which sophisticated and complicated mathematical calculi require an evaluation that is more scientific than archival, and which therefore need the involvement of a highly specialised and expert team. It is also tragic to add that a significant portion of the archive – at least 40% of it – has been lost over the years.

It is perhaps useful to close this article by mentioning that since 2002 the IAC has allowed all scholars who request it online access to a vast compilation – edited by Maurizio Mattaliano – called *Storia dell’IAC attraverso i suoi documenti* (History of the IAC through its documents), composed of hundreds of webpages. In this compilation, following guided pathways, it is possible to take a first virtual look inside the archive, viewing images of a substantial portion of the documents stored in it.

Bibliography

- [1] M. Picone, *Operosità scientifica e curriculum accademico del dott. Mauro Picone, Professore stabile di Calcolo Infinitesimale nella R. Università di Napoli*. Napoli, 11 marzo 1927, [Opuscolo].
- [2] M. Mattaliano, *Quei legami spezzati dalla burrasca*, “Sapere”, anno 73°, n. 3, 2007, ed. Dedalo (Bari).
- [3] A. Guerraggio, M. Mattaliano, P. Nastasi, *Calcoli di guerra*, “Sapere”, anno 62°, n. 2, 2006, ed. Dedalo (Bari).
- [4] A. Guerraggio, M. Mattaliano, P. Nastasi, *Mauro Picone e i matematici polacchi: 1937–1961*, Serie “Conferenze”, Accademia Polacca delle Scienze, Biblioteca e Centro Studi a Roma, Varsavia-Roma, 2007.

University Goes to School

Vladimir Salnikov (University of Luxembourg, Luxembourg)

This article is about various activities that university professors and researchers organise for high school students. Initially, we thought about publishing just one “success story” about a mathematics club but then realised that we know a lot of them, so there will be a series of texts. In this issue, you will find information about two rather young initiatives in Switzerland. In the next issue, some activities in France and Russia will be presented, with

traditions that are significantly longer (dating back to Soviet times).

The message to take away is: if you know a high school student interested in mathematics or science in general then try asking around. Something like this should exist close to you. If you are a university professor and want to organise this kind of activity then ask around as well. There are people willing to share their experiences and results. So, enjoy reading the success stories.

The ETH Math Youth Academy

Kaloyan Slavov (ETH Zürich, Switzerland)

According to the 2012 PISA survey,¹ Switzerland (along with Liechtenstein) is best in Europe and 9th in the world in terms of the general quality of mathematical education in school. The level of the students is homogeneously very high. However, opportunities for students to go beyond the standard mathematical curriculum do not abound, at least in comparison to other countries (in Eastern Europe or in the US, for instance).

The large-scale, long-term research project Swiss-MAP,² funded by a grant from the Swiss National Foundation, includes a postdoctoral position at ETH Zürich with a focus on designing and implementing school outreach activities. The author has held this position since September 2015 and has launched a programme aimed at providing high school students with opportunities for creative thinking and delving deeper into exciting mathematics. The main activity of the recently established ETH Math Youth Academy³ consists of regular weekly “math circle” classes, which take place at ETH and focus on topics beyond the standard curriculum. The design has been heavily influenced by the author’s own participation in similar activities in the thriving environment as a high school student in Bulgaria.

The focus in the classes is on “elementary” and yet nontrivial mathematics, i.e. the treated topics belong entirely to the high school domain with no analysis or linear algebra as covered in the first years of university. While students who continue in mathematics will inevitably master the standard topics later, the development of creative, out-of-the-box thinking is beneficial for all students, regardless of their future field of study or career path. In addition, it is easier for students to become comfortable with rigorous proofs – which are heavily empha-

sised in the classes – in a more concrete and accessible setting. Most importantly, at least for students at this age, the aesthetics of mathematics can be more readily and vividly illustrated in an “elementary” context.

The classes are in the form of mini-courses, each lasting 3-6 weeks, organised by topic or technique. There are two groups of students, main and advanced, according to age and experience. Topics in the main-level course include elementary graph theory, invariants and the pigeonhole principle. As a specific example, in a mini-course on the “Extreme principle”, the theorem of Sylvester-Gallai is discussed:

Let S be a finite set of points in the plane, with the property that the line joining any two of them contains a third. Prove that all the points in S lie on a line.

Proof. Suppose the contrary. Among all non-zero distances from a point in S to a line joining two points of S , take a *smallest* one, say from P to l . Since l contains at least three points of S , we can find two, A and B , which are on the same side of l with respect to the foot Q of the perpendicular from P to l . Say A is between Q and B . But now the distance from A to the line PB is smaller than the one from P to l . \square

In a mini-course on elementary number theory, we start systematically and from scratch to introduce divisibility and congruences, reaching the theorems of Euler and Fermat and illustrating them with many applications. A subsequent mini-course on number theory focuses on quadratic residues and Gauss’s Quadratic Reciprocity Law, again with numerous applications. A Euclidean geometry mini-course develops and illustrates the properties of inversion as a transformation in the plane. Hall’s Marriage theorem, along with related theorems and various applications (e.g. completing Latin squares) is a topic

¹ <http://www.oecd.org/pisa/keyfindings/pisa-2012-results.htm>

² <http://www.nccr-swissmap.ch>

³ <https://www.math.ethz.ch/eth-math-youth-academy>

for the advanced class. Another topic for the advanced class is unique factorisation of elements in the rings of integers of certain imaginary quadratic number fields (defined and treated in a completely explicit manner), with the concrete goal of solving Diophantine equations, e.g. $x^2 + 2 = y^3$ or $x^3 + y^3 = z^3$.

In this way, although many of the applications of the theory lead toward the kind of problems used in various mathematical competitions, the classes do not consist of isolated “problem-solving” sessions: preparation for mathematical Olympiads is a by-product but not the main goal. Instead, this is a middle ground between Olympiad preparation and theoretical mathematical studies. In fact, it is to be expected that these mini-courses will naturally give rise to future student research projects.

The target audience consists of all interested high school students (aged 14 or above). Being careful not to use the adjectives “gifted” or “talented” is important because, on the one hand, this may scare some of the modest students away and, on the other hand, it is neither possible nor is there a need to judge at this early stage who is gifted and who is not. Any student motivated to spend two hours a week after school doing more mathematics is welcome to attend the classes.

Parallel to the weekly classes, an initiative has been launched for giving public talks at various high schools. These are intended to be accessible to a broad general

audience and to be interesting and inspiring for all the students attending. So far, only two such public talks have taken place — one on “Mathematical induction” and one on “Mathematical games” (available online from the project’s website). It is hoped that there will be further invitations from more schools, as this is an effective way to popularise mathematics within the broader community.

As of April 2016, there are a total of about 15 students attending regularly. There are two main challenges for the growth of the project. Firstly, mathematics circles are a relatively new phenomenon in Switzerland and the tradition is yet to be established. Secondly, students have a very busy and rigid school schedule, which does not allow too much pursuit of independent initiatives outside of school. However, the keen students currently attending find this type of extracurricular mathematics truly exciting and it is hoped that the project will expand considerably over its second year.



Kaloyan Slavov is a postdoc at ETH Zürich who is interested in algebraic geometry. He obtained his PhD at MIT, following a BA at Harvard.

Activities at the University of Geneva

Elise Raphael (University of Geneva, Switzerland)

The University of Geneva has recently developed several activities aimed at secondary school students in order to promote mathematics and physics. The *Club de maths* offers fun extra-curricular mathematics courses to groups of children, the *Olympiads* allow any interested pupils to test their competences on unusual problems and, on a more academic level, the *Athena programme* allows highly motivated high school students to attend certain university courses.

Club de maths

The mathematics department of the University of Geneva has welcomed numerous Russian professors and PhD students over the past decades, amongst whom most attended *mathematical circles* in their youth. One of them, Alexander Glazman (Silver Medallist at the Olympiads in 2006), started the Club de maths in September 2013 under the guidance of Professor Alekseev.

The idea is simple: any pupil from secondary schools in Geneva can spend two hours a week dissecting mathematics problems at the mathematics department. Is this not an extra-curricular activity like any other?

Well, this is hard to tell. Indeed, the children that decide to voluntarily attend mathematics problem ses-

sions on Wednesday afternoons are interested and gifted in mathematics, and often bored by the mathematics lessons they have to follow at school. But still, showing them beautiful proofs or simply giving them hard problems to solve doesn’t keep them thinking for two hours.

With each week comes a new sheet of problems (about ten of them), generally all related to some topic, with definitions if necessary. Pupils are expected to understand the concepts through problems and are not taught much theory during these classes. The topics range from the pigeonhole principle to graph theory, with some logic and game theory. No programme has been fixed and teaching assistants are free to teach according to what their class seems to like or understand the best. The idea is not to cover the academic programme faster (or at all) but to show some different mathematics, and this is stressed when the activities are presented to all the secondary school teachers.

Over the first two years, there were two groups of roughly 10 pupils, aged 10-13. This expanded to three age groups this year, with most of the previous years’ students continuing in the next group. Around 30 pupils aged 10-16 are now spending part of their Tuesday evenings or Wednesday afternoons doing mathematics for fun.

Olympiads

Once the success of the Club de maths was clear, a natural extension presented itself: a mathematics competition in the spirit of the international mathematics Olympiads.

The first mathematics Olympiads at the University of Geneva were organised in November 2014 and have already been repeated twice. Indeed, many children from the Club de maths attended these events but they were not the only ones. Advertisements were sent to the schools to attract more pupils, some of whom later joined the Club de maths.

Students have three hours to solve 20 to 30 problems. Correct answers give them a certain number of points depending on the difficulty of the problem. An award ceremony takes place after each event and the students who obtained the highest scores receive prizes consisting of mathematical books and games. Individual results are sent along with solutions to each pupil who participates.

Here are three problems that got students sweating last November:

- *A broken line crosses each of its line segments exactly two times. What is the minimal number of line segments in it?*
- *Jean puts 0 or 1 in each cell of a table 10×19 and then finds the sum of numbers in each horizontal and vertical line. What is the maximal number of different sums he could get?*
- *Find the greatest common divisor of all 6-digit palindromes.*

Athena programme

Both the Club de maths and the Olympiads stimulate mathematical curiosity but cannot help prospective students understand what is studied at university. The Athena programme does.

The idea originated from the head of the physics department Michele Maggiore, along with Andreas Müller. This programme makes it possible for gifted high school students in their last years at school to attend a physics or mathematics university course. Initially (in Autumn 2015), four physics courses and two mathematical courses were made available. Over 100 applications were received and distributed over these courses. The selected students attended the classes alongside regular university students but were allowed extra time with tutors to help them cope with the new notions and extra work. Most of them took the final exams and the successful ones will

get their credits if they join the university to study maths or physics.

Such activities do not organise themselves overnight and many professors, PhD students and Master's students have been involved. I joined the fun when I started my PhD, in September 2014, as part of my teaching assignments. I first taught the youngest pupils in the Club de maths for a year. It is a very interesting teaching task but a very demanding one, creating the exercises and trying to find the right balance between the mathematical content and the playful aspects.

I didn't go into teaching because, even though I love it, I cannot cope with discipline. I therefore enjoy teaching at university level. Teaching the children, because it is more of a hobby for them than a class, is both very rewarding and frustrating. Some days they ask the most relevant questions (and you would gladly exchange your passive first year students for them) and other days you can see that they're just waiting for you to give them the answer and go on a break. My best experience with them was probably last Easter, when I organised a mathematical treasure hunt. It took me forever to prepare but they enjoyed it a lot and solved the problems as a team.

This year, I had the chance to teach *Méthodes élémentaires*, which was part of the Athena programme. It is a third-year mathematics course again based on Olympiad problems with almost no prerequisites. Most of the additional students were highly motivated and I believe that giving them a taste of their potential studies is a good way to tip the balance in favour of mathematics.

If you want to learn more about the activities aimed at secondary school students currently organised by the University of Geneva, you can visit the following websites:

- <http://www.unige.ch/sciences/programme-athena.html>
- <http://www.unige.ch/math/fr/clubmath/>.
- <http://mathscope.ch> (another well-established activity).



I am currently a PhD student at the University of Geneva (Switzerland) under the supervision of Anton Alexeev. My interests lie in Lie theory and quantum algebra, as well as rock climbing (as a non-research interest).

Nesin Mathematics Village

Salih Durhan (Nesin Mathematics Village, Izmir, Turkey)

Nesin Mathematics Village proves that an unorthodox model for a mathematics institute can be viable. Hear the amazing story of the maths village.

Brief history

The story of Nesin Mathematics Village, referred to as “*The Village*” by its frequent visitors, goes back to 1997, the year when Istanbul Bilgi University accepted its first intake of students. Ali Nesin was the head of the mathematics department and I was among the clueless teenagers who somehow ended up studying mathematics at Bilgi University. Soon, some of us would follow Ali Nesin’s vision and take part in the dream that led to the maths village.

Ali Nesin had prepared an intense programme. He wanted to inspire his students to become mathematicians and he was willing to do anything necessary to provide them with the best undergraduate education he could possibly think of. Well, that meant axiomatic set theory for the first year students: ordinals, cardinals, the axiom of choice, ordinal arithmetic and ultrafilters – the real deal and no white lies. I vividly recall constructing the natural numbers, the integers, the rationals, the reals and even a nonstandard model of the reals with perfect rigour in axiomatic set theory. Soon, Ali Nesin had to devise nonstandard teaching hours to carry out his ultraprogramme. This started the mathematics Summer schools of Bilgi University in 1998. There was no Summer semester at Bilgi University at the time but Ali Nesin somehow convinced the university to support this completely unofficial Summer school and, even more surprisingly, he convinced around 30 students to join him in Antalya (a seaside tourist town in southern Turkey) so we could enjoy eight hours of group theory and point set topology per day for a month and a half. Such thrills are not for the faint of heart. There were four of us left continuing the maths programme by the second year but we were all determined to become mathematicians, while the rest continued onto computer science. The following years were more of the same, with intense regular semesters and Summer schools. Each year, a few more students survived the first year and the department became a tightly knit group of lecturers and students. It was a lot of work and a lot of fun. As students, we had to face a very demanding curriculum but we were rewarded for our efforts with a real feeling of accomplishment and had continuous support from our lecturers.

We quickly fell in love with the Summer schools. There was intense mathematics as usual but we were able to socialise and connect more as a group in different ways each Summer. We were far away from the daily distractions and worries of city life and this gave us plenty of time to work and enjoy life. Students did not earn any credits for the courses and the lecturers did not get paid.

It wasn’t that the courses were not for credit; it was that they were officially non-existent and would never show up on a transcript, which made the whole thing even more appealing. There was no external recognition of what we were doing but we did not mind. In fact, we were proud to be doing something worthwhile even though no one else seemed to care at the time. Today, more than 10 of the students who went to these Summer schools hold PhDs.

By 2002, within only five years of the first intake of students, there were four Bilgi University mathematics graduates pursuing graduate degrees in well-respected US universities. In the following years, the Summer schools became well known among undergraduate mathematics students in Turkey. More students from outside Bilgi wanted to join the Summer schools but there was only a limited amount of support available from Bilgi University. There was also the issue of having to deal with poor learning conditions. Affordable hotels do not come with a quiet classroom and a large blackboard. It must have been clear to Ali Nesin that he needed a maths village.

In 2007, Ali Nesin bought 2.5 acres of land one kilometre away from Sirince, a beautiful small village in the mountains close to Selcuk, Izmir. Sevan Nisanyan, an old friend of his, was instrumental in the choice of location and in the physical development of the maths village. His taste and knowledge of architecture is reflected throughout the maths village. It takes a lot of effort to convince visitors that the maths village is not built out of restored Ancient Greek or Byzantine ruins. All structures in the village are made of wood and stone. They blend into the mountain with the trees and flowers. There are plenty of open air classrooms and small isolated areas to work undisturbed.

The maths village started out as a few tents and a small classroom, and hosted around 100 students throughout the Summer of 2007. The concept was beautiful so it kept attracting more students and mathematicians but this



Ali Nesin teaching at the mathematics village.

meant that the village needed more money both to invest in facilities and to cover running costs. Undergraduate students did not really have much money to contribute to their living expenses at the village and Ali Nesin was determined not to turn down any student for financial reasons. Government funding agencies provided only quite limited support for a few years. Donations were used to invest in facilities but the running costs of the village were resulting in a huge deficit. Ali Nesin poured his personal savings into the maths village but this could only serve to delay the problem. The only sustainable solution for the village was to generate its own funds.

The village therefore started offering two-week programmes to high school students for a modest fee. These programmes are completely independent of the standard high school curriculum and yet they became very popular very quickly. Academics deliver courses like number theory, graph theory, set theory and analysis to high school students and the children love it. Parents are more than happy to send their children to these programmes and the village uses the funds generated from these programmes to support undergraduate and graduate students.



The library also serves as a lecture hall.

Current programmes

The main event at the maths village is the traditional undergraduate and graduate Summer school, though many other events have been added to the mix. There are almost 50 different courses planned for the Summer of 2016, ranging from beginning undergraduate to graduate level and lasting for a week or two each. The instructors are academics from all over the world and English is the preferred language. The students come from various universities in Turkey and there are some international students as well. Bilgi University students are no longer the majority. I missed the early days of the maths village but after moving to Cyprus in 2010 I did not miss a single Summer school. I could teach whatever I wanted and there was always a motivated group of students attending the lectures. Students are encouraged to contribute to their living expenses but undergraduate and graduate mathematics students are never turned down for financial reasons. In practice, almost all living expenses of these students are covered by the village.

Each high school programme during the Summer is two weeks long, and more students attend these than any other programme. Volunteering academics teach the

courses for high school students and over the years these programmes have inspired quite a few students to pursue mathematics. Some of these students are continuing their undergraduate education and some are in graduate schools around the world. In the Summer of 2015, I was part of a research team investigating the effect of high school programmes at the village. The results are under review but I can confidently say that we observed a significant improvement in the attitude of students towards mathematics. Anecdotal evidence is substantial in this direction: I have heard “I hate mathematics but what we see here is different. This is really great; why don’t they teach us this in school?” many times over the last five years.

On top of these teaching-oriented programmes, the village also hosts conferences and workshops in mathematics and related areas. It has taken time to establish the maths village as a venue for research events in mathematics but the progress is promising. At the end of each event we have more and more mathematicians falling in love with the village, which in turn leads to more and more research-oriented events being held there. In 2016, the village will host the “Experimentation with Mathematical Algorithms Workshop”, the “Antalya Algebra Days”, “Geometrie Algébrique en Liberté” and “Women in Numbers Europe”.

Even when there are no specific programmes, research is ongoing at the village. This is of course to be expected. If you put mathematicians together in a relaxed atmosphere where they do not carry any of the burdens of daily life, they will start talking mathematics. There are various groups who arrange their Summer school teaching at the village to coincide so that they can work on their research projects together. The team of A. Borovik, A. Deloro and S. Yalcinkaya deserves a mention here; they have so far contributed to seven research articles with their work at the maths village. They have inspired more people to do the same and, as the demand was obvious, the village started a programme for research groups. Teams of researchers can apply to this programme to conduct whatever research they wish in the productive village environment. It is also possible to get a grant from the village to cover lodging and dining expenses.

What makes the maths village a success story is not purely academic merit. The collaborative nature of the maths village is very important to its development. Mathematicians from all over the world have contributed to the programmes in the village, with no material expectations and often spending from their own pocket. The joy of sharing and caring is not a myth; it is a reality of life. The maths village is a manifestation of this reality in the context of mathematics. Everyone in the village contributes to village life. Academics teach, graduate students help undergraduates and undergraduates help high school students. Everyone contributes to the daily chores, whether this be serving dinner or picking up rubbish. As such, the maths village is not a venue so much as a community. All the mathematicians who came out of Bilgi University, including myself, are now contributing to the maths village. There is no doubt that within the next few years, we will have mathematicians teaching in

our Summer schools who started out attending the high school programmes.

Future

The ideal to inspire a few teenagers to become mathematicians in 1997 gave rise in 2007 to a small camp serving around 100 students living in tents. Now, the maths village is a self-sustaining non-profit organisation that spends around \$1 million annually for day-to-day operations. Initially, the activities at the maths village took place only during the Summer months but now the village is active all year long, with more than 10 permanent staff. Activities held at the village include one-day school visits, high school programmes, undergraduate and graduate Summer schools, specialised workshops and Summer schools on topics closely related to mathematics such as computer science and physics, workshops, conferences and research groups. You can view the events at the mathematics village at <http://nesinkoyleri.org/eng/> and a quick look at upcoming events shows seven international workshops and conferences. In 2015, the total number of participants in various events held at the village was almost 8,000, with an average visit length of five days.

Ali Nesin's hard work and dedication is still the driving force behind the maths village. However, the maths village ideal is spreading and finding appreciation both among mathematicians and the general public. This is exactly what is needed, as there is no governmental or corporate support behind the village. It is a minor miracle that



One of the study areas in the village.

an independent mathematics institution is able to survive and even expand with modest donations from ordinary people and the volunteered time of mathematicians. So, organise a conference, apply for a research group or offer a course for the Summer school at the maths village! You will see that it feels great to be part of a miracle.



Salih Durhan [salih1@gmail.com] is a resident mathematician at Nesin Mathematics Village. He received his PhD in 2007 at UIUC, worked as a postdoctoral fellow at McMaster University (2007–2010) and was an assistant professor at METU NCC (2010–2015).

ICMI Column

Gabriele Kaiser (University of Hamburg), Convenor

The 13th International Congress on Mathematical Education will take place in Hamburg, 24–31 July 2016. This congress takes place every fourth year; last time, it was organised by South Korean colleagues in Seoul.

As usual, there will be four plenary talks and two plenary sessions enriched by 70 invited lecturers – renowned scholars describing the state-of-the-art in their areas of research. The heart of the congress will be 54 Topical Study Groups (TSG), each of which will meet four times for 90 minute sessions. These Topical Study Groups will continue activities from previous ICMEs but have been increased in number and thematic broadness. They cover all the important themes of mathematics education across educational levels and general thematic aspects. All participants contributing to the congress with a paper or a poster will participate in these groups and all presentations will be organised within these groups. Currently, 820 presentations are scheduled for the four regular sessions of these TSGs and 1120 oral communications for the TSGs will take place in the sessions attached to each TSG. Furthermore, 650 posters attached to the TSGs will be displayed in two poster sessions.

In order to enhance the active participation of congress attendants, participants of ICME-13 could propose discussion groups and workshops. The proposals were reviewed by the members of the IPC. About 43 discussion groups (each with two sessions lasting 90 minutes) and 42 workshops (each with one 90 minute session) will take place.

Overall, the number of registered participants is nearly 3200, with 300 accompanying persons also registered so far.

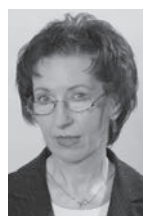
Additional activities will take place. On Sunday 24 July 2016, a special day for early career researchers will take place, with many activities covering research methods and publication activities. So far, 450 participants have registered for this special activity.

From Thursday 27 to Friday 29 July 2016, a special activity for German teachers (held in German) will take place. The teachers will have the chance to become acquainted with research results and teaching proposals from well known German mathematics educators. Already, 190 teachers have registered for this sub-conference.

Another important activity of ICME-13 is the support of scholars from less-affluent countries. In addition to the solidarity grant, money from the German Ministry of Education and Research and the Bosch foundation has supported 170 scholars from non-African countries and 50 scholars from Africa, that is, 220 scholars or about

7% of the expected number of participants. These activities show the strong orientation of the congress toward social dimensions of mathematics education.

ICME-13 has already started a strong publication programme in connection with Springer Publishing House. 27 ICME-13 Topical Surveys will appear before the congress, displaying the state-of-the-art in specific fields (accessible via the website <http://www.springer.com/series/14352>). After the congress – in addition to the two volumes of congress proceedings – about 40 post-congress monographs from the TSGs and other activities will probably appear, displaying the richness of the discussions at ICME-13.



Gabriele Kaiser holds a master's degree as a teacher for mathematics and humanities for lower and upper secondary level. She completed her doctorate in mathematics education in 1986 with a study on applications and modelling 1997 a post-doctoral study on international comparative studies, both at the University of Kassel. Since 1998, she is full professor for mathematics education at the Faculty of Education of the University of Hamburg. Since 2005 she serves as Editor-in-chief of ZDM Mathematics Education. She is Convenor of the 13th International Congress on Mathematical Education (ICME-13).

ERME Column

Thérèse Dooley (St. Patrick's College, Dublin, Ireland) and Ghislaine Gueudet (ESPE Bretagne, Rennes, France)

News from CERME 10

The 10th Congress of European Research in Mathematics Education (CERME 10) will take place in Dublin (Ireland), from 1st to 5th February 2017. Ghislaine Gueudet (France) is the Chair of the International Programme Committee (IPC), which is composed of Thérèse Dooley (Ireland, Chair of the Local Programme Committee), Andreas Eichler (Germany, Co-Chair of the IPC), Marianna Bosch (Spain), Markku Hannula (Finland), Jeremy Hodgen (UK), Konrad Krainer (Austria), Despina Potari (Greece), Kirsti Rø (Norway), Cristina Sabena (Italy), Michiel Veldhuis (Netherlands) and Nad'a Vondrova (Czech Republic). Thérèse Dooley and Maurice O'Reilly are Chair and Co-Chair of the local organisation.

The chief aims of ERME are to promote communication, cooperation and collaboration in research in mathematics education in Europe. Its conference, CERME, which is designed as a starting point for promoting these aims, deliberately and distinctively moves away from research presentations by individuals and toward collaborative group work. CERME's main feature is the *Thematic Working Group* (TWG), where members work together on a common research domain. TWGs allow about 13 hours over four days for the attendees to meet and progress their work. Each TWG aims to promote good scientific debate with the purpose of deepening mutual knowledge about the problems and methods of research in a particular field of interest. Conference participants are expected to work within just one group.

There will be about 24 TWGs at CERME 10: details about the focus of each group can be accessed from the list of TWGs on the CERME 10 website. Researchers wishing to have their work discussed at the conference should submit a paper or a poster proposal to one of these TWGs. CERME papers and posters must be about

research (empirical, theoretical or developmental). In addition, there will be plenary activities and a poster session. Amongst the plenary activities, there will be an address by Lieven Verschaffel (Belgium) on Early Years Mathematics and one by Elena Nardi (UK) on University Mathematics. There will also be a panel on Solid Findings that will directly refer to texts regularly published in the EMS Newsletter by the EMS Educational Committee. The deadline for submission of papers and posters is 15 September 2016. All details are available at <http://cerme10.org/>.

In order to support researchers who might not be able to attend CERME without financial assistance, a limited amount of support is available to researchers through the Graham Litter Fund. Applications for this support should be submitted before 15 September 2016. ERME is deeply interested in the active participation of young researchers in mathematics education. The IPC therefore includes two elected representatives of young researchers, and young researchers participate as co-leaders of most TWG teams.

We invite you to visit the website of CERME 10, <http://cerme10.org/>, which will be updated on a regular basis.



Thérèse Dooley is a senior lecturer in mathematics education at the Institute of Education, Dublin City University. Her research interests include primary and post-primary mathematics, the role of language in the construction of mathematical knowledge, the enhancement of mathematics teaching and learning through researcher/teacher collaboration, and mathematical task development. She is Chair of the Local Organising Committee of CERME 10.



Ghislaine Gueudet is a professor in mathematics education at the ESPE Bretagne (School for Teacher Education), University of Brest. Her research concerns university mathematics education and the design and use of educational resources (digital resources in particular). She is Chair of the International Programme Committee of CERME 10.

Another Update on the Collaboration Graph

Michael Jost, Nicolas D. Roy and Olaf Teschke (all FIZ Karlsruhe, Berlin, Germany)

The ramifications of the collaboration graph have been part of mathematicians' folklore since at least the 1950s.¹ Only about four decades later, the advancement of both computational power and reliable data in electronic form made it possible to create online tools to quickly compute the shortest paths of joint publications between mathematicians who have published since 1940.² Without doubt, the Erdős number, defined as the length of a shortest collaboration graph to the node with by far the highest valence, is its most famous feature. The great Erdős Number Project (ENP) site³ contains a huge amount of information on it. Among others, it maintains files with all known co-authors of Paul Erdős (not just restricted to mathematics) and their co-authors, a collection of currently 11,514 people with Erdős number at most two.

Information before 1940 has so far been gathered mostly in the attempt to trace famous people. The impressive collection at the Erdős Number Project⁴ basically has exhaustive lists of Nobel Prize winners, Fields Medallists and a large number of other prize winners and famous scientists. Among others, it contains a path of length 15 to Laplace, which includes Jean Darcet (born 1724) – probably the earliest known scientist so far with a finite Erdős number.

The *Jahrbuch über die Fortschritte der Mathematik*⁵ is a rich source of mathematical publications from the period 1868–1943 but only tiny fractions of its information could be evaluated within the collaboration graph until recently. The main deficit was the lack of proper author identification, which turned out to be especially challenging for a large proportion of its entries. Not only did misprints occur much more frequently within its corpus but also the rather small size of the mathematical community at that time led to rather casual behaviour in the documentation of author names, often with completely missing first names, abbreviated surnames or misleading initials.⁶

¹ According to R. De Castro and J. W. Grossman [Famous Trails to Paul Erdős, *Math. Intell.* 21, No. 3, 51–63 (1999); extended Spanish version *Rev. Acad. Colomb. Cienc. Exactas, Fis. Nat.* 23, No. 89, 563–582 (1999)], the first reference in the literature to an Erdős number dates back to [J. Bardeen et al., Microscopic theory of superconductivity. *Phys. Rev.* (2) 106 1957 162–164 (1957)].

² <http://www.ams.org/mathscinet/collaborationDistance.html>.

³ <http://wwwp.oakland.edu/enp/>.

⁴ <http://wwwp.oakland.edu/enp/erdpaths/>.

⁵ See also S. Göbel, *Jahrbuch über die Fortschritte der Mathematik* and *Zentralblatt MATH* – reporting on more than 140 years of mathematics. *Eur. Math. Soc. Newsl.* 73, 45–46 (2009).

Only in recent years have author assignments of this historical part of the zbMATH database been sufficiently improved to release an interface, available at <https://zb-math.org/collaboration-distance/> or via the zbMATH author profiles, to compute collaboration distances within its full scope. More precisely, the share of authorships that can still be assigned with ambiguities has dropped below 5% for the *Jahrbuch* data, which coincides roughly with the average uncertainty level of the database and makes it very unlikely to affect the shortest paths.

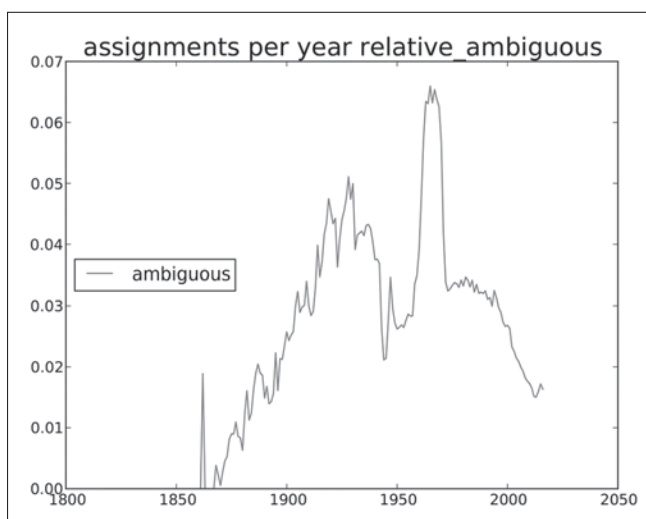


Figure 1. Share of ambiguously assigned authorships for the zbMATH database depending on publication year.

Specifics of collaboration data from the *Jahrbuch*

Perhaps the most striking feature about collaboration data from the *Jahrbuch* is that they generally do not exist, due to the simple fact that the vast majority of mathematical publications from the 19th century are sole-authorship. More precisely, the historical share of collaborative work in zbMATH can be seen in Figure 2 (see next page).

Consequently, the *Jahrbuch* contributes a disproportionate fraction of isolated nodes to the collaboration graph. A peculiar effect can also be seen from the diagram: the surprising rise and fall of multi-authored contributions between 1870 and 1885 (almost 5%). This is generated by the popularity of publishing mathematical problems as well as joint solution attempts in several

⁶ A typical example, which has already been mentioned in this column, is the “O.L.B.D. Eytelwein” in the first *Crelle* volume, which stands for Ober-Landes-Bau-Director, while the first names “Johannes Albert” are completely missing.

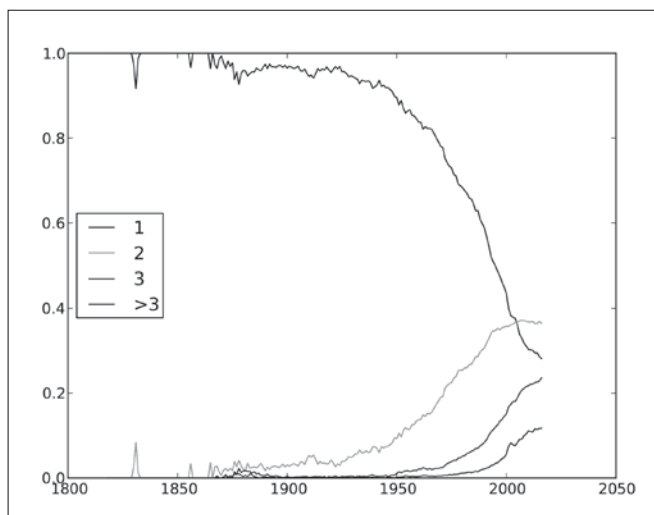


Figure 2. Distribution of papers with one, two, three and more authors in zbMATH, depending on publication year.⁷

journals at that time. Of course, counting them as research collaboration is debatable from today's viewpoint⁸ but their inclusion in the *Jahrbuch* back then seems to reflect their accepted significance at the time. Their inclusion in the collaboration graph certainly has the value of adding many illustrious names to its main component, which would otherwise remain isolated; a prominent example is the “Solutions of questions 8861, 9588” [Ed. Times L. 34–35 (1889)], which has, among its authors, a certain Ch. L. Dodgson, an Oxford Tutor not only known for his mathematical treatises like “Euclid and his modern rivals” [London: Macmillan. xxxi, 299 p. (1879)] but also for his other works published under the pen name of Lewis Carroll. Through his co-solver T.C. Simmons, who managed to give another joint solution with Cayley (linked to Erdős via Hardy and Heilbronn), this gives the author of “Through the Looking-Glass” an Erdős number of 5 (or as we would prefer to put it, it gives Erdős an Alice number of 6).

Probably even more problematic is the *Jahrbuch* custom of counting editors of works and letters as co-authors. Formally, this would create a path of length 6 from Kepler to Erdős but the link via Walther Franz Anton van Dyck certainly goes beyond the traditional concept of collaboration. Slightly more justified would be to view Leibniz and Bernoulli as collaborators of their exchanged letters (which were published much later) but Leibniz – who needs to be mentioned in the year of his anniversary – has only a quite weak link to the main component of the graph created by editorship of Newton's works. Also, one might prefer to delete edges generated

⁷ For 1940–1995, this shows a pattern very similar to the diagram in [J. W. Grossman and P. Ion, On a Portion of the Well-Known Collaboration graph, *Congr. Numerantium* 108, 129–131 (1995)].

⁸ In fact, the ENP omits “joint editorships, introductions to books written by others, technical reports, problem sessions, problems posed or solved in problem sections of journals, seminars, very elementary textbooks, books on history, memorial or other tributes, biography, translations, bibliographies, or popular works”.

by the series “Ostwalds Klassiker der exakten Wissenschaften”, which printed treatises of famous authors on similar subjects together.

Another *Jahrbuch* entry enabling many interesting connections is the volume “Science in the changing world” [M. Adams. 286 p. London, G. Allen & Unwin (1933)], authored by such famous people as Thomas Holland, H. Levy, Julian Huxley, John R. Baker, Bertrand Russell, Aldous Huxley, Hugh l'A. Fausset, Hilaire Belloc, J. B. S. Haldane and Oliver Lodge. Through John Burdon Sanderson Haldane (Erdős number 3, via Cedric A.B. Smith and H. Kestelman), they all receive an Erdős number of 4, which is especially interesting in the case of Bertrand Russell, mathematician and Nobel Prize winner, for whom a finite collaboration path within the main component of the graph seems not to have been clear before (consequently, Alfred North Whitehead also earns an Erdős number of 5).

For many other prominent scientists, their Erdős numbers could be decreased successfully by the newly added edges, e.g. Niels Bohr now has 4 (through Heisenberg, Pólya and Davenport) instead of 5 and he has a short path of length 4 to his brother and mathematician Harald (Erdős number 5) via Dirac, Schrödinger and Courant (the previous shortest known path had length 8, through Erdős) and a path of length 7 to his son (and also Nobel Prize winner) Aage (Erdős number 5) via Heisenberg, Born, Geppert-Meyer, Jensen, Stech and Alder (previous shortest known path length 10, again through Erdős).

As a final famous example, the *Jahrbuch* informs us that the second part of “Notes de tératopologie” [*Rev. sci.*, Paris, 77, 180–181 (1939)] by Dieudonné (who wrote Part I alone and Part III with Cartan) was published together with a certain N. Bourbaki. This sole recorded explicit co-authorship of the latter gives him an Erdős

Figure 3. A hitherto seemingly unknown collaboration path.

number of 4, a fact that seems not to have been noticed before.

Some general facts and figures

Since the historical part of the collaboration graph is a comparatively sparse subgraph due to a limited number of edges, it has a significant influence on some invariants but almost none on others. First, naturally, it increases the number of connected components dramatically; but since it is only the large (namely, the Erdős) component that is usually discussed, this is not of much interest.

Another effect of adding the historical data is that, again, at least at the moment, Erdős is in the centre of his graph component (which has a diameter of 24), with an eccentricity of 13 (in the graph based on data from 1940, Israel Gelfand, Yakov Sinai and J. Bryce McLeod have been in the centre on several occasions; naturally, Erdős benefits from the addition of data that puts his lifespan more in the centre). He also has the smallest average distance (4.62; at the moment, Shing-Tung Yau comes in second with 4.68).

Overall, in the collaboration graph generated by zbMATH data, the large component comprises 670,443 authors out of 935,577 (with 163,870 isolated nodes), whose distance to the centre is as follows:

Erdős number 0 ---	1
Erdős number 1 ---	484
Erdős number 2 --	9179
Erdős number 3 ---	72324
Erdős number 4 ---	240331
Erdős number 5 ---	229743
Erdős number 6 ---	86565
Erdős number 7 ---	23404
Erdős number 8 ---	6173
Erdős number 9 ---	1661

Erdős number 10 ---	422
Erdős number 11 ---	107
Erdős number 12 ---	35
Erdős number 13 ---	14

Among the very distant people, the most famous (in the sense that there is an important theorem named after him) is probably Friedrich Hartogs, who has an Erdős number of 10. Naturally, there is much more to explore in this newly available realm – you could just try it yourself!

Michael Jost has been working with zbMATH since 1994. As a computer scientist he was active in numerous projects and development efforts in the area of scientific information and communication, such as EuDML. Recently, he has been working (once again) on the application of latest search engine technology and efficient algorithms on large data sets for zbMATH, and on eLibM.



Nicolas Roy received his PhD in mathematics in Grenoble in 2003 and then worked for seven years as a researcher and assistant lecturer at the Humboldt University in Berlin. Between 2011 and 2012, he acted as a developer and specialist for mathematics education for the e-learning platform Bettermarks.com. Since 2013, he has

been member of the editorial board and responsible for author identification at zbMATH.org.

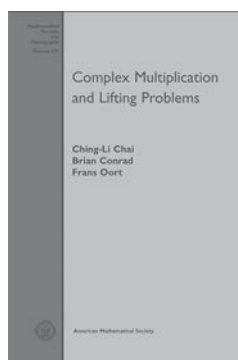
Olaf Teschke [olaf.teschke@fiz-karlsruhe.de] is a member of the Editorial Board of the EMS Newsletter, responsible for the Zentralblatt Column.

In Memory of Claude Goutorbe (1952–2016)

Claude Goutorbe passed away in April 2016. He was one of the founding members of Cellule Mathdoc in 1995 as a senior software developer. He has been pivotal in developing services that are used daily by thousands of mathematicians. He was at the core of the cooperation between France and Germany that endowed Zentralblatt Math with web access as early as 1996. He then created the web interface of the Numdam digital library in 2002 and extended the system to support the electronic publishing of mathematics journals in the Cedram platform around 2005. He also participated actively in many European and international projects (LIMES, EMANI and EuDML, to name just a few). He was recently polishing, with younger colleagues, the modern platform that will this year replace the system he built for Numdam. The systems he made were fit for purpose, easy to use and somewhat similar to him, in that they were discreet, modest and quite powerful. He will be considerably missed.

*Thierry Bouche
Director of Cellule Mathdoc, Grenoble, France*

Book Reviews



Ching-Li Chai, Brian Conrad
and Frans Oort

Complex multiplication and lifting problems

(Mathematical Surveys and Monographs, 195)
Providence, RI: American
Mathematical Society
2014, ix, 387 pp
ISBN 978-1-4704-1014-8

Reviewer: Gregory Sankaran
(University of Bath, UK)

The three authors of this book consider the at first sight straightforward question of whether an abelian variety over a finite field has a lift to characteristic zero that is a CM abelian variety (a CM lift). Immediately one realises that the problem needs to be more carefully formulated, and even a first attempt to do that reveals subtleties. Nevertheless, in 2006 the authors [1] had given two versions ((I) and (IN), below) of the problem, and soon afterwards counterexamples were found to one of the versions. It eventually turned out that these counterexamples were in some way central to understanding the problems and, in many cases, answering them. This book explains how.

The experts may begin at the beginning, but the inexperienced (but necessarily skilled) reader is advised to turn first to page 87, near the end of Chapter 1, where the authors ask us to consider five (actually six) assertions concerning existence of a CM lift of an abelian variety B over a finite field \mathbb{F}_q or of its extension of scalars B_κ to a finite extension $\kappa : \mathbb{F}_q$. One should first assume, to avoid trivialities, that B is isotypic over \mathbb{F}_q , i.e. has up to isomorphism a unique simple factor. Then the assertions are

(CML) *CM lifting*: There is a characteristic zero local domain R with residue field \mathbb{F}_q , and an abelian scheme A over R of relative dimension $g = \dim B$, together with a CM field $L \subset \text{End}^0(A) = \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(A)$ of degree $2g$ over \mathbb{Q} , and an isomorphism $\phi : A_{\mathbb{F}_q} \rightarrow B$ of abelian varieties over \mathbb{F}_q .

(R) *CM lifting after finite residue field extension*: R now has residue field κ and $\phi : A_\kappa \rightarrow B \times_{\text{Spec}(\mathbb{F}_q)} \text{Spec}(\kappa)$.

(I) *CM lifting up to isogeny*: as (CML), but now ϕ is an isogeny, not an isomorphism.

(IN) *CM lifting to normal domains up to isogeny*: as (I), but R is required to be a normal local domain.

(RIN) as (IN), but with the residue field of R being κ as in (R).

(sCML) *Strong CM lifting*: for every CM field $L \subset \text{End}^0(B)$ of degree $2g$ with $O_L \subset \text{End}(B)$, (CML) holds for B in such a way that $L \subset \text{End}^0(A)$.

Already in 1992 *F. Oort* [2] had shown that (R), and hence (CML), fails in general. In other words, an isogeny is neces-

sary, and one should turn one's attention to (I) and (IN). The examples given there are of a restricted type, however, and a substantial part of this book – Chapter 3, on CM lifting of p -divisible groups – is partly motivated by the authors' desire to understand the true extent of this failure. The results of Chapter 3 are then used in Chapter 4 to show the main result of the book: that assertion (I), on the other hand, is always true. Thus, to get a CM lifting, allowing isogeny is enough but allowing field extensions is not. This also implies that (RIN) is true, because the normality condition can be achieved if one allows field extension, as the authors show. On the other hand, (IN) is false in general. In Chapter 2 of the book, specific examples are given, but more than that: the authors give necessary and sufficient conditions for a lifting in this sense to exist. The condition is quite subtle, in that it does not depend merely on B , or even on B and L . The essential notion is that of a CM type (L, Φ) . This consists of a CM field L of degree $2g$ over \mathbb{Q} , and a collection Φ of g maps from L into some algebraically closed field K of characteristic zero, in this context usually $\overline{\mathbb{Q}_p}$, which are inequivalent under the action of complex conjugation. In other words, $\text{Hom}(L, K)$ consists precisely of elements of Φ and their composition with complex conjugation in L . In this situation, the authors define a field $E \subset \mathbb{Q}$, called the reflex field, by the condition that $\text{Gal}(E, \mathbb{Q})$ is the subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that stabilises the set Φ . The (main) obstruction to (IN) is then that if (IN) holds, the residue field κ_v of $O_{E, v}$ for the p -adic valuation of $E \subset \overline{\mathbb{Q}_p}$ must be realisable as a subfield of \mathbb{F}_q . This really can depend on Φ as well as B and L . The authors give, in Chapter 2, two classes of counterexample to (IN), one supersingular and the other absolutely simple. The second of these leads to the identification of the condition above as the essentially only obstruction to (IN). The first example is of less importance when one considers (IN) but proves illuminating in Chapter 4, when we are given the complete unconditional proof of (I). In fact, (I) is proved in a more precise form, with bounds on the isogeny degree needed. The basic example is a case of the “toy model”, a class of CM abelian surfaces C over \bar{k} for which L is a quartic field, p is inert in L and the subset $\bar{\Phi}$ of \mathbb{F}_p -homomorphisms from $\kappa = O_L/pO_L \cong \mathbb{F}_{p^4}$ that determine the action of κ on the \bar{k} tangent space to C is invariant under the unique involution of κ . In fact the authors classify such toy models, but the real progress comes from looking at the corresponding local condition, i.e. for p -divisible groups. It turns out that (very roughly) the algebraisation problem that is the core difficulty in the proof of (I) can be reduced to the toy model case, after which it is sufficient to solve the p -divisible group version of the problem. That is precisely the problem that has been considered in Chapter 3. Both the reduction steps and the results for p -divisible groups are very delicate and many incidental results of independent interest are proved along the way.

Before the lifting problems are stated in full, Chapter 1 gives a thorough and readable account of large parts of the theory of abelian varieties over finite fields in general, includ-

ing for example a review of the basics of Dieudonné theory and p -divisible groups. Additionally, a substantial part of the book (almost a third) is given over to two appendices containing further results that are either required for the main part or sufficiently interesting digressions to merit the space (or both). These parts make the book into a valuable resource even for purposes not directly connected with CM lifting. In particular, in Appendix A, Section 1 gives a proof of the $\ell = p$ case of Tate's isogeny theorem over finite fields (that $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell \simeq \text{Hom}(A[\ell^\infty], B[\ell^\infty])$). The usual proof, due to Tate, Milne and Waterhouse, is heavily algebraic but the one given here, based on notes by Eisenträger, avoids that. Even more useful, perhaps, is Section 2 of Appendix A, which reproves the Main Theorem of Complex Multiplication in a scheme-theoretic way which may be more accessible to modern readers than the famous but now stylistically dated book of Shimura. The other parts of Appendix A are a converse to the Main Theorem, needed in Chapter 2 of the book, and a result (due, though in a slightly less general form, to Shimura) about the existence of algebraic Hecke characters extending a given map between the Weil restriction of tori, which is needed in Chapter 3 in order to realise given CM types via p -divisible groups. Appendix B is more specific, being devoted to constructions of CM lifting via p -adic Hodge theory, but it also includes a comparison of various Dieudonné theories (classical, crystalline etc.).

The book as a whole is very attractive but, because of the technical difficulties of the subject matter, it is not easy read-

ing. Specialists will need no encouragement to study it, but it contains much information of wider interest too.

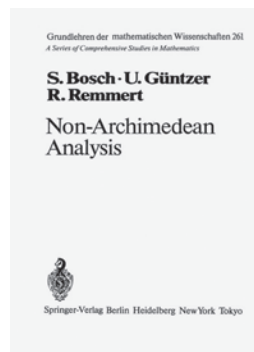
The Newsletter thanks Zentralblatt MATH and Gregory Sankaran for the permission to republish this review which originally appeared as Zbl 1298.14001.

Bibliography

- [1] Ching-Li Chai and Frans Oort. Hypersymmetric Abelian varieties. *Pure Appl. Math. Q.*, 2(1):1–27, 2006. Zbl 1156.14320
- [2] Frans Oort. “The” general case of S. Lang’s conjecture (after Faltings). In *Diophantine approximation and abelian varieties. Introductory lectures. Papers of the conference, held in Soesterberg, Netherlands, April 12–16, 1992*, pages 117–122. Berlin: Springer-Verlag, 1993. Zbl 0811.14025



Gregory Sankaran [G.K.Sankaran@maths.bath.ac.uk] is Professor of Pure Mathematics at the University of Bath. He studied in Cambridge and later worked there and in the Netherlands before moving to Bath. His research interests are in algebraic geometry, especially in the geometry of moduli spaces of algebraic varieties and in applications of modular forms to geometric problems.



S. Bosch, Ulrich Guntzer and Reinhold Remmert

Non-Archimedean Analysis. A Systematic Approach to Rigid Analytic Geometry

(Grundlehren der Mathematischen Wissenschaften, 261)
Berlin etc.: Springer Verlag
1984, xii, 436 pp.

Reviewer: Pierre Berthelot
(University of Rennes, France)

The Newsletter thanks Zentralblatt MATH and Pierre Berthelot for the permission to republish this review which originally appeared as Zbl 0539.14017. The Newsletter and Zentralblatt MATH are honoured to remember Reinhold Remmert, who passed away on 9 March 2016.

Since the introduction of rigid analytic spaces by Tate in 1961, rigid analytic geometry (i.e. the analog of complex analytic geometry over complete non archimedean fields) has had a growing importance in algebraic geometry, number theory, p -adic analysis, etc. However, the basic results of the theory had remained scattered in various papers, sometimes difficult to

find, and some fundamental notions have undergone various changes as the theory was making progress. Thus, the subject was not so easily accessible to non-specialists, and there was an increasing need for a systematic account of the theory of rigid analytic spaces in addition to the introductory book of *J. Fresnel* and *M. van der Put* [1]. The present book should meet that need.

The book is divided in three parts. The first one, “Linear ultrametric analysis and valuation theory”, is devoted to prerequisites and fundamentals in ultrametric analysis and analytic function theory. In chapter 1, the basic notions concerning ultrametric norms on abelian groups and rings are introduced. They cover such topics as the reduction functor, power multiplicative semi-norms and smoothing procedures, strictly convergent power series with coefficients in a semi-normed ring. Chapter 2 is devoted to the theory of normed modules and vector spaces. The bulk of the chapter is a discussion of various types of normed vector spaces characterized by the existence of (eventually topological) basis for which the norm of the projections of a vector are closely related to the norm of the vector itself. Of particular interest for rigid analytic geometry is the case of normed vector spaces of countable type; for these spaces, the chapter includes a proof of the “lifting theorem”, which gives conditions under which an algebraic basis of the reduction of a normed space can be lifted as a topological orthonormal basis of the space. The third and last chapter of part A discusses the extensions of norms and valuations. In addition to the case of field extensions and classical

valuation theory, the chapter introduces for K -algebras over a non-archimedean field K the notions of spectral norm and supremum norm; a special attention is given to the case of Banach algebras, and to the behaviour of the supremum norm under finite extensions, which will be of great importance in the theory of affinoid algebras (e.g. for the proof of the “maximum modulus principle”).

The second part, “Affinoid algebras”, develops the algebraic foundations of rigid analytic geometry. Chapter 4 is devoted to the study of the Tate algebra $T_n = K\langle X_1, \dots, X_n \rangle$ of strictly convergent power series in n variables over a complete non archimedean field K . A particularly important result is the Weierstrass division and preparation theorem, from which are derived some basic properties: T_n is noetherian, factorial, normal, its ideals are closed, etc. Chapter 5 then proceeds with the theory of affinoid algebras, i.e. quotient algebras of algebras T_n , which play the same role in rigid analytic geometry as the affine algebras in algebraic geometry. After establishing the analog of Noether’s normalisation theorem, which is one of the most useful tools in the study of affinoid algebras, some classical properties of the supremum semi-norm, such as the maximum modulus principle, are proved. The chapter ends with properties of the sub-algebra \hat{A} of elements of semi-norm ≤ 1 in an affinoid algebra A , including the important finiteness theorem for the reduction functor.

The third part of the book deals with the theory of rigid analytic spaces. Chapter 7 develops the local theory. To any affinoid algebra A is attached its maximal spectrum $\text{Sp}A$, and the basic problem in order to get a good notion of analytic space is to define a topology on $\text{Sp}A$ having reasonable properties from the point of view of analytic continuation. This is achieved thanks to the construction of a Grothendieck topology on $\text{Sp}A$. A subset U of $\text{Sp}A$ is called an affinoid subdomain if there exists an affinoid A -algebra A' , such that any homomorphism of affinoid algebras $A \rightarrow B$ for which $\text{Sp}B$ is sent in U factors uniquely through A' . For example, the rational domains, defined by inequalities $|f_i(x)| \leq |f_0(x)|$, $i = 1, \dots, r$, where f_0, f_1, \dots, f_r are elements of A generat-

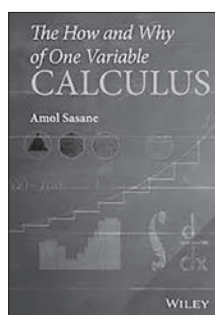
ing the unit ideal, are affinoid subdomains, and are shown to have good stability properties. A theorem of Gerritzen and Grauert, proved at the end of Chapter 7, implies in particular that any affinoid subdomain is a finite union of rational domains. Affinoid subdomains and finite coverings by affinoid subdomains can then be used as generators for a Grothendieck topology, as explained in the beginning of Chapter 9. Thanks to Tate’s acyclicity theorem, to which is devoted Chapter 8, it is possible to define the sheaf of analytic functions on $\text{Sp}A$ as a sheaf for that topology, associating to any affinoid subdomain the corresponding algebra. – Grothendieck topologies allow then to glue these local models to develop the global theory of rigid analytic spaces. This is done in the last sections of Chapter 9, which cover the theory of coherent modules, finite morphisms, closed analytic subvarieties, separated and proper morphisms. Kiehl’s finiteness theorem for direct images is discussed, although the proof is not included. The book ends with the example which was the starting point of the theory: Tate’s uniformization for elliptic curves with bad reduction.

Bibliography

- [1] Jean Fresnel and Marius van der Put, *Géométrie analytique rigide et applications. (Rigid analytic geometry and applications)*, (Progress in Mathematics, 18). Boston–Basel–Stuttgart: Birkhäuser, 1981



Pierre Berthelot [pierre.berthelot@univ-rennes1.fr] is currently a “professeur émérite” at the University of Rennes. A former student of Grothendieck, he has worked on various p -adic cohomology theories for algebraic varieties over a field of prime characteristic p . His construction of rigid cohomology is a direct application of the theory of rigid analytic spaces.



Amol Sasane

The How and Why of One Variable Calculus

Wiley, 2015

464 p.

ISBN 978-1-119-04338-6

Reviewer: Jean-Paul Allouche

This book is meant as a textbook in calculus for first year students and contains the words “How” and “Why” in its title. Most books concentrate on “How”, leaving a small section, if it is covered at all, to “Why” and this is the first reason to get interested in this book. The reader will find not only a book with detailed courses (with many useful and/or funny figures – see, for example, the Dedekind

cut on page 27) but also tentative answers to the “Why” questions, including the very first one: “Why study Calculus”. The chapters are devoted respectively to real numbers, sequences, continuity, differentiation, integration and series. All potential “missing” areas (i.e. topics not necessarily studied at high school level) are introduced. Furthermore, a large number of examples and exercises are presented. To give an illustration, the example on Page 101 states: “At any given instant of time, there exists a pair of diametrically opposite points on the equator of the Earth which have the same temperature”. Some examples and exercises are classical and some are less classical, e.g. calculate the area enclosed by a cardioid or by the two “petals” of a lemniscate, or study the design of a clepsydra. Solutions of all the exercises are given in the last chapter. Finally, a useful bibliography of 20 items will support those readers who desire to know more. While reading this book, I could not resist trying to think of the pleasure it would have been if it had been my very first book in calculus!

Letters to the Editor

History of the European Congress of Mathematics

Dear Editor,

The recent Newsletter articles on the first six ECMs show how this event has become established as an influential and valuable feature of European mathematical life. Yet they contain scarcely any reference to the one man whose energy and vision gave birth to this institution.

At the EMS Foundation Meeting in Madralin in 1990, Max Karoubi outlined his plans for a European Congress of Mathematics to take place in Paris in 1992, and proposed that it should be an EMS event. To some of us at the meeting, this seemed like an alarmingly ambitious undertaking for the infant Society. But Professor Karoubi's exciting ideas for the Congress, and the enthusiasm with which he presented them, were contagious. This, and his account of the groundwork that he had already done in securing widespread international support and financial backing, succeeded in persuading the meeting to adopt his proposal. It was agreed that the EMS should support the Congress as the first of a quadrennial series of such meetings. At a later stage, when plans for the Congress were already well advanced, it became clear that the organisation of the meeting should be the

responsibility of the mathematical societies of the host country. At that point, the organisation and finance of the Congress became the responsibility of the French mathematical societies. But there is no doubt that the whole concept of a European Mathematical Congress is due to Max Karoubi, and that without his dedicated work and enthusiastic advocacy there would be no ECM.

Christopher Lance
University of Leeds, UK

Professor Karoubi has been mentioned in the Newsletter of the EMS on several occasions in relation to the organisation of the first European Congress of Mathematics, for instance in "The First Years of the European Mathematical Society" by Aatos Lahtinen (Issue 96, page 12):

"Hirzebruch now took the chair and the council began to shape the society. Then, Max Karoubi made a tempting suggestion. He was preparing a large European Congress in Paris in 1992 and proposed it as the Congress of EMS, without any financial responsibility. After some consideration, the council eagerly approved the proposition. It also agreed that this would be a tradition: the society would have a congress every four years starting with the Paris congress."

Personal Column

Please send information on mathematical awards and deaths to newsletter@ems-ph.org.

Awards

The Norwegian Academy of Science and Letters has decided to award the **Abel Prize** for 2016 to **Sir Andrew J. Wiles**.

The Catalan Mathematical Society SCM and the Institute of Catalan Studies IEC has awarded the 2016 **Josep Teixidor Prize** for the best thesis or primer work in mathematics to **Joaquim Serra i Montoni** and the 2016 **Évariste Galois Prize** to **Fernández-Real Girona**. The monograph *Monoidal Categories and Topological Field Theory*, by **Vladimir Turaev**, Indiana University, and **Alexis Virelizier**, Université de Lille 1, is the 2016 winner of the **Ferran Sunyer i Balaguer Prize**, awarded by the Ferran Sunyer i Balaguer Foundation (Barcelona).

The **Association Marseillaise Pi-day** has received the 2016 **Prix d'Alembert** from the French Mathematical Society SMF for the organisation, since 2013, of popular celebrations of Pi-day in Marseille, France.

The laureates of the 2015 **INDAM SIMAI UMI Prize** are **Simone Di Marino**, **Eleonora Di Nezza**, **Stefano Bosia** and **Tommaso Lorenzi**. The 2016 **SIMAI Prize** has been awarded to **Paola Antonietti**.

The 2015 laureates of the "**Young Mathematician**" Prize of the St. Petersburg Mathematical Society are **Dmitry Stolyarov** and **Pavel Zatitskiy** for the work "Exact Bellman functions".

Ivan Nourdin and **Giovanni Peccati** of the Luxembourg Mathematical Society (SML), both professors at the University of Luxembourg, have received the 2015 **Award for Outstanding Scientific Publications** from the Fond National de Recherche of Luxembourg (FNR) for the book *Normal approximations with Malliavin calculus*.

Barry Simon (Caltech) has been awarded the **International János Bolyai Prize of Mathematics** by the Hungarian Academy of Sciences.

Deaths

We regret to announce the deaths of:

Pedro Gil Álvarez (16 March 2016, Spain)

Claude Goutorbe (20 April 2016, France)

Victor Khavin (21 September 2015, Russia)

Reinhold Remmert (9 March 2016, Germany)

Tosun Terzioglu (22 February 2016, Turkey), President of the Turkish Mathematical Society for 19 years (until 2008)

Miguel Torres (14 December 2016, Spain)



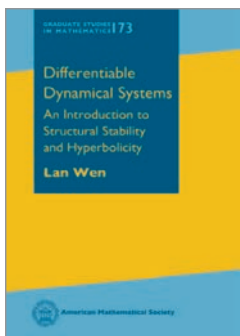
THE CASE OF ACADEMICIAN NIKOLAI NIKOLAEVICH LUZIN

Edited by Sergei S. Demidov, Russian Academy of Sciences & Boris V. Lëvshin
Translated by Roger Cooke

A campaign to "Sovietize" mathematics in the USSR in 1936 was launched with an attack on Nikolai Nikolaevich Luzin, the leader of the Soviet school of mathematics, in Pravda. Luzin was fortunate in that only a few of the most ardent ideologues wanted to destroy him utterly. As a result, Luzin, though humiliated and frightened, was allowed to make a statement of public repentance and then let off with a relatively mild reprimand. The present book contains the transcripts of five meetings of the Academy of Sciences commission charged with investigating the accusations against Luzin.

History of Mathematics, Vol. 43

Jul 2016 386pp 9781470426088 Hardback €120.00



DIFFERENTIABLE DYNAMICAL SYSTEMS

An Introduction to Structural Stability and Hyperbolicity

Lan Wen, Peking University

A graduate text in differentiable dynamical systems. It focuses on structural stability and hyperbolicity, a topic that is central to the field. Starting with the basic concepts of dynamical systems, analyzing the historic systems of the Smale horseshoe, Anosov toral automorphisms, and the solenoid attractor, the book develops the hyperbolic theory first for hyperbolic fixed points and then for general hyperbolic sets. The problems of stable manifolds, structural stability, and shadowing property are investigated, which lead to a highlight of the book, the Ω -stability theorem of Smale.

Graduate Studies in Mathematics, Vol. 173

Aug 2016 199pp 9781470427993 Hardback €87.00

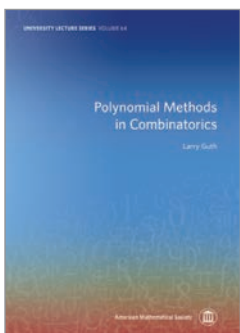


GALLERY OF THE INFINITE

Richard Evan Schwartz, Brown University

A mathematician's unique view of the infinitely many sizes of infinity. Written in a playful yet informative style, it introduces important concepts from set theory (including the Cantor Diagonalization Method and the Cantor-Bernstein Theorem) using colourful pictures, with little text and almost no formulas. It requires no specialized background and is suitable for anyone with an interest in the infinite, from advanced middle-school students to inquisitive adults.

Jul 2016 187pp 9781470425579 Paperback €32.00



POLYNOMIAL METHODS IN COMBINATORICS

Larry Guth, Massachusetts Institute of Technology

Explains some recent applications of the theory of polynomials and algebraic geometry to combinatorics and other areas of mathematics. One of the first results in this story is a short elegant solution of the Kakeya problem for finite fields, which was considered a deep and difficult problem in combinatorial geometry. The author also discusses in detail various problems in incidence geometry associated to Paul Erdős's famous distinct distances problem in the plane from the 1940s. The proof techniques are also connected to error-correcting codes, Fourier analysis, number theory, and differential geometry.

University Lecture Series, Vol. 54

Jul 2016 273pp 9781470428907 Paperback €53.00

Free delivery worldwide at eurospanbookstore.com/ams

AMS is distributed by **Eurospan** | group

CUSTOMER SERVICES:

Tel: +44 (0)1767 604972

Fax: +44 (0)1767 601640

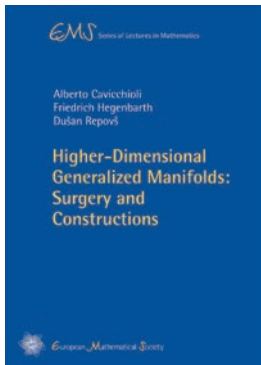
Email: eurospan@turpin-distribution.com

FURTHER INFORMATION:

Tel: +44 (0)20 7240 0856

Fax: +44 (0)20 7379 0609

Email: info@eurospangroup.com



Alberto Cavicchioli (Università degli Studi di Modena e Reggio Emilia, Italy), Friedrich Hegenbarth (Università degli Studi di Milano, Italy) and Dušan Repovš (University of Ljubljana, Slovenia)

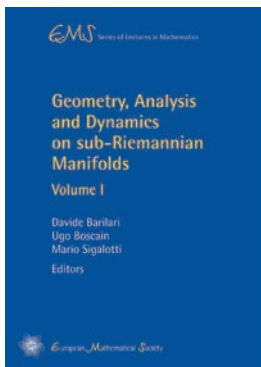
Higher-Dimensional Generalized Manifolds: Surgery and Constructions (EMS Series of Lectures in Mathematics)

ISBN 978-3-03719-156-9. 2016. 154 pages. Softcover. 17 x 24 cm. 32.00 Euro

Generalized manifolds are a most fascinating subject to study. They were introduced in the 1930s, when topologists tried to detect topological manifolds among more general spaces (this is nowadays called the manifold recognition problem). As such, generalized manifolds have served to understand the nature of genuine manifolds. However, it soon became more important to study the category of generalized manifolds itself.

A breakthrough was made in the 1990s, when several topologists discovered a systematic way of constructing higher-dimensional generalized manifolds, based on advanced surgery techniques. Generalized manifolds will continue to be an attractive subject to study, for there remain several unsolved fundamental problems.

This is the first book to systematically collect the most important material on higher-dimensional generalized manifolds and controlled surgery. It is self-contained and its extensive list of references reflects the historic development. The book is based on our graduate courses and seminars, as well as our talks given at various meetings, and is suitable for advanced graduate students and researchers in algebraic and geometric topology.



Geometry, Analysis and Dynamics on sub-Riemannian Manifolds, Volume I (EMS Series of Lectures in Mathematics)

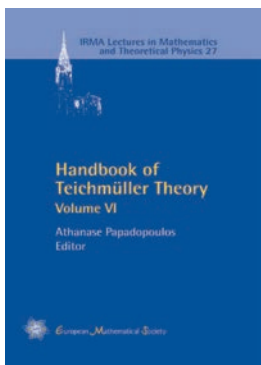
Davide Barilari (Université Paris 7 Denis Diderot, Paris, France), Ugo Boscain (École Polytechnique, Palaiseau, France) and Mario Sigalotti (École Polytechnique, Palaiseau, France), Editors

ISBN 978-3-03719-162-0. 2016. 332 pages. Softcover. 17 x 24 cm. 44.00 Euro

Sub-Riemannian manifolds model media with constrained dynamics: motion at any point is only allowed along a limited set of directions, which are prescribed by the physical problem. From the theoretical point of view, sub-Riemannian geometry is the geometry underlying the theory of hypoelliptic operators and degenerate diffusions on manifolds.

In the last twenty years, sub-Riemannian geometry has emerged as an independent research domain, with extremely rich motivations and ramifications in several parts of pure and applied mathematics, such as geometric analysis, geometric measure theory, stochastic calculus and evolution equations together with applications in mechanics, optimal control and biology.

The aim of the lectures collected here is to present sub-Riemannian structures for the use of both researchers and graduate students.



Handbook of Teichmüller Theory, Volume VI (IRMA Lectures in Mathematics and Theoretical Physics, Vol. 27)

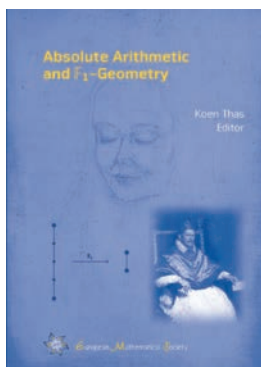
Athanase Papadopoulos (Université de Strasbourg, France), Editor

ISBN 978-3-03719-161-3. 2016. 652 pages. Hardcover. 17 x 24 cm. 88.00 Euro

This volume is the sixth in a series dedicated to Teichmüller theory in a broad sense, including various moduli and deformation spaces, and the study of mapping class groups. It is divided into five parts: Part A: The metric and the analytic theory; Part B: The group theory; Part C: Representation theory and generalized structures; Part D: The Grothendieck–Teichmüller theory; Part D: Sources.

The topics surveyed include Grothendieck's construction of the analytic structure of Teichmüller space, identities on the geodesic length spectrum of hyperbolic surfaces (including Mirzakhani's application to the computation of Weil–Petersson volumes), moduli spaces of configurations spaces, the Teichmüller tower with the action of the Galois group on dessins d'enfants, and several others actions related to surfaces. The last part contains three papers by Teichmüller, translated into English with mathematical commentaries, and a document that contains H. Grötzsch's comments on Teichmüller's famous paper *Extremale quasikonforme Abbildungen und quadratische Differentiale*.

The Handbook is addressed to researchers and to graduate students.



Absolute Arithmetic and \mathbb{F}_1 -Geometry

Koen Thas (University of Gent, Belgium), Editor

ISBN 978-3-03719-157-6. 2016. 404 pages. Hardcover. 17 x 24 cm. 68.00 Euro

It has been known for some time that geometries over finite fields, their automorphism groups and certain counting formulae involving these geometries have interesting guises when one lets the size of the field go to 1. On the other hand, the nonexistent field with one element, \mathbb{F}_1 , presents itself as a ghost candidate for an absolute basis in Algebraic Geometry to perform the Deninger–Manin program, which aims at solving the classical Riemann Hypothesis.

This book, which is the first of its kind in the \mathbb{F}_1 -world, covers several areas in \mathbb{F}_1 -theory, and is divided into four main parts – Combinatorial Theory, Homological Algebra, Algebraic Geometry and Absolute Arithmetic. Topics treated include the combinatorial theory and geometry behind \mathbb{F}_1 , categorical foundations, the blend of different scheme theories over \mathbb{F}_1 which are presently available, motives and zeta functions, the Habiro topology, Witt vectors and total positivity, moduli operads, and at the end, even some arithmetic.

Each chapter is carefully written by experts, and besides elaborating on known results, brand new results, open problems and conjectures are also met along the way.

The diversity of the contents, together with the mystery surrounding the field with one element, should attract any mathematician, regardless of speciality.