NEWSLETTER

OF THE EUROPEAN MATHEMATICAL SOCIETY

European
Mathematical
Society

March 2020
Issue 115
ISSN 1027-488X

Features
Renormalisation of Stochastic PDEs
Approximate Groups

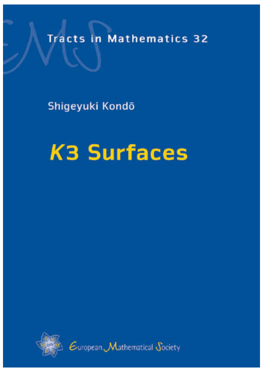
Interviews
Freeman Dyson
David Ruelle

Obituary
Hagen Neidhardt

Freeman Dyson (photo: Dan Komoda/
IAS, Princeton, NJ USA)

New books published by the
European Mathematical Society

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


Tracts in Mathematics 32

Shigeyuki Kondō

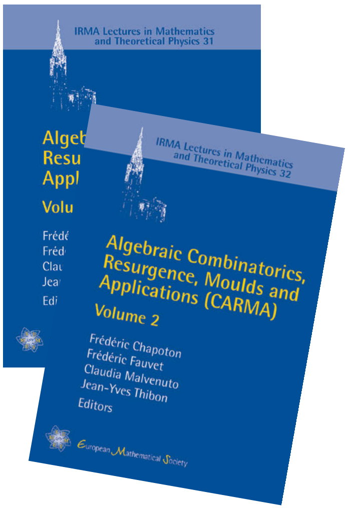
K3 Surfaces

European Mathematical Society

***K*3 Surfaces** (EMS Tracts in Mathematics, Vol. 32)
Shigeyuki Kondō (Nagoya University, Japan)

ISBN 978-3-03719-208-5. 2020. 252 pages. Hardcover. 17 x 24 cm. 78.00 Euro

*K*3 surfaces are a key piece in the classification of complex analytic or algebraic surfaces. The term was coined by A. Weil in 1958 – a result of the initials Kummer, Kähler, Kodaira, and the mountain K2 found in Karakoram. The most famous example is the Kummer surface discovered in the 19th century.
*K*3 surfaces can be considered as a 2-dimensional analogue of an elliptic curve, and the theory of periods – called the Torelli-type theorem for *K*3 surfaces – was established around 1970. Since then, several pieces of research on *K*3 surfaces have been undertaken and more recently *K*3 surfaces have even become of interest in theoretical physics.
The main purpose of this book is an introduction to the Torelli-type theorem for complex analytic *K*3 surfaces, and its applications. The theory of lattices and their reflection groups is necessary to study *K*3 surfaces, and this book introduces these notions. The book contains, as well as lattices and reflection groups, the classification of complex analytic surfaces, the Torelli-type theorem, the subjectivity of the period map, Enriques surfaces, an application to the moduli space of plane quartics, finite automorphisms of K3 surfaces, Niemeier lattices and the Mathieu group, the automorphism group of Kummer surfaces and the Leech lattice.
The author seeks to demonstrate the interplay between several sorts of mathematics and hopes the book will prove helpful to researchers in algebraic geometry and related areas, and to graduate students with a basic grounding in algebraic geometry.


IRMA Lectures in Mathematics and Theoretical Physics 31

IRMA Lectures in Mathematics and Theoretical Physics 32

Algebraic Combinatorics, Resurgence, Moulds and Applications (CARMA)

Volume 2

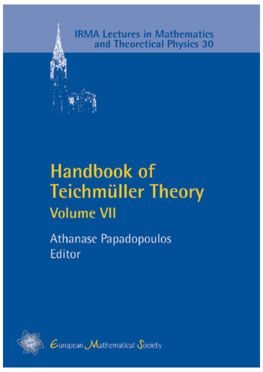
Frédéric Chapoton
Frédéric Fauvet
Claudia Malvenuto
Jean-Yves Thibon
Editors

European Mathematical Society

Algebraic Combinatorics, Resurgence, Moulds and Applications (CARMA). Volumes 1 and 2
(IRMA Lectures in Mathematics and Theoretical Physics, Vols. 31 and 32)
Edited by Frédéric Chapoton (Université de Strasbourg, France), Frédéric Fauvet (Université de Strasbourg, France), Claudia Malvenuto (Università di Roma La Sapienza, Italy) and Jean-Yves Thibon (Université Paris-Est Marne-la-Vallée, France)

Vol. 1: ISBN 978-3-03719-204-7. 2020. 354 pages. Hardcover. 17 x 24 cm. 58.00 Euro
Vol. 2: ISBN 978-3-03719-205-4. 2020. 396 pages. Hardcover. 17 x 24 cm. 58.00 Euro

This is a two-volume work comprising a total of 14 refereed research articles which stem from the CARMA Conference (Algebraic Combinatorics, Resurgence, Moulds and Applications), held at the Centre International de Rencontres Mathématiques in Luminy, France, from June 26 to 30, 2017.
The conference did notably emphasise the role of Hopf algebraic techniques and related concepts (e.g. Rota–Baxter algebras, operads, Ecalle's mould calculus) which have lately proved pervasive in combinatorics, but also in many other fields, from multiple zeta values to the algebraic study of control systems and the theory of rough paths.
The volumes should be useful to researchers or graduate students in mathematics working in these domains and to theoretical physicists involved with resurgent functions and alien calculus.


IRMA Lectures in Mathematics and Theoretical Physics 30

Handbook of Teichmüller Theory
Volume VII

Athanase Papadopoulos
Editor

European Mathematical Society

Handbook of Teichmüller Theory, Volume VII (IRMA Lectures in Mathematics and Theoretical Physics, Vol. 30)
Edited by Athanase Papadopoulos (Université de Strasbourg, France)

ISBN 978-3-03719-203-0. 2020. 626 pages. Hardcover. 17 x 24 cm. 88.00 Euro

The present, seventh volume of the Handbook of Teichmüller theory is divided into three parts.
The first part contains surveys on various topics in Teichmüller theory, including the complex structure of Teichmüller space, the Deligne–Mumford compactification of the moduli space, holomorphic quadratic differentials, Kleinian groups, hyperbolic 3-manifolds and the ending lamination theorem, the universal Teichmüller space, barycentric extensions of maps of the circle, and the theory of Higgs bundles.
The second part consists of three historico-geometrical articles on Tissot (a precursor of the theory of quasiconfomal mappings), Grötzsch and Lavrentieff, the two main founders of the modern theory of quasiconformal mappings.
The third part comprises English translations of five papers by Grötzsch, a paper by Lavrentieff, and three papers by Teichmüller. These nine papers are foundational essays on the theories of conformal invariants and quasiconformal mappings, with applications to conformal geometry, to the type problem and to Nevanlinna's theory. The papers are followed by commentaries that highlight the relations between them and between later works on the subject. These papers are not only historical documents; they constitute an invaluable source of ideas for current research in Teichmüller theory.

European Mathematical Society Publishing House – EMS Press
Technische Universität Berlin, Mathematikgebäude, Room MA266

Strasse des 17. Juni 136
10623 Berlin, Germany

orders@ems.press
ems-ph.org / ems.press

European Mathematical Society

Newsletter No. 115, March 2020

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

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

Published by the
EMS Publishing House
TU Berlin, Mathematikgebäude, Room MA266
Strasse des 17. Juni 137
10623 Berlin, Germany
homepages: ems-ph.org / ems.press

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

EMS Executive Committee

President

Prof. Volker Mehrmann
(2019–2022)
Technische Universität Berlin
Sekretariat MA 4-5
Straße des 17. Juni 136
10623 Berlin, Germany
e-mail: mehrmann@math.tu-berlin.de

Vice-Presidents

Prof. Armen Sergeev
(2017–2020)
Steklov Mathematical Institute
Russian Academy of Sciences
Gubkina str. 8
119991 Moscow
Russia
e-mail: sergeev@mi.ras.ru

Prof. Betül Tanbay
(2019–2022)
Department of Mathematics
Bogazici University
Bebek 34342 Istanbul
Turkey
e-mail: tanbay@boun.edu.t

Secretary

Prof. Sjoerd Verduyn Lunel
(2015–2022)
Department of Mathematics
Utrecht University
Budapestlaan 6
3584 CD Utrecht
The Netherlands
e-mail: s.m.verduynlunel@uu.nl

Treasurer

Prof. Mats Gyllenberg
(2015–2022)
Department of Mathematics
and Statistics
University of Helsinki
P. O. Box 68
00014 University of Helsinki
Finland
e-mail: mats.gyllenberg@helsinki.fi

Ordinary Members

Prof. Jorge Buescu
(2019–2022)
Department of Mathematics
Faculty of Science
University of Lisbon
Campo Grande
1749-006 Lisboa, Portugal
e-mail: jsbuescu@fc.ul.pt

Prof. Nicola Fusco
(2017–2020)
Dip. di Matematica e Applicazioni
Complesso Universitario di
Monte Sant' Angelo
Via Cintia
80126 Napoli
Italy
e-mail: n.fusco@unina.it

Prof. Stefan Jackowski
(2017–2020)
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa
Poland
e-mail: sjack@mimuw.edu.pl

Prof. Vicente Muñoz
(2017–2020)
Departamento de Algebra,
Geometría y Topología
Universidad de Málaga
Campus de Teatinos, s/n
29071 Málaga
Spain
e-mail: vicente.munoz@uma.es

Prof. Beatrice Pelloni
(2017–2020)
School of Mathematical &
Computer Sciences
Heriot-Watt University
Edinburgh EH14 4AS
UK
e-mail: b.pelloni@hw.ac.uk

EMS Secretariat

Ms Elvira Hyvönen
Department of Mathematics
and Statistics
P. O. Box 68
(Gustaf Hällströmin katu 2b)
00014 University of Helsinki
Finland
Tel: (+358) 2941 51141
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

2020

3–4 July
EMS Executive Committee Meeting, Bled, Slovenia

4–5 July
EMS Council Meeting, Bled, Slovenia

29 October
EMS 30 Years Anniversary Celebration
Edinburgh, UK

30 October–1 November
EMS Executive Committee Meeting
Edinburgh, UK

EMS Scientific Events

2020

6–10 April
Periods, motives and differential equations: between arithmetic and geometry
Institut Henri Poincaré, Paris, France

11–22 May
Recent trends in cryptology and cyber security
Kiev, Ukraine

25–29 May
Sub-Riemannian Geometry and Beyond, III.
Centro di Ricerca Matematica, Pisa, Italy

8–12 June
Conference on complex analysis and geometry
Institut de Mathématiques de Toulouse, France

29 June–3 July
Reductive Groups 2020
Bestwig, Germany

5–11 July
8th European Congress of Mathematics
Portorož, Slovenia

6–10 July
28th International Conference on Operator Theory
Timisoara, Romania

23–30 August
Helsinki Summer School on Mathematical Ecology and Evolution
Turku, Finland

14–18 September
IAMP-EMS summer school "Quantum information in many-body physics: a mathematical invitation"
Technical University of Munich, Germany

22–24 September
"The Unity of Mathematics", Conference in Memory of Sir Michael Atiyah
Isaac Newton Institute, Cambridge, UK

Report from the Executive Committee Meeting in Yerevan, Armenia 11–13th October 2019

Richard Elwes, EMS Publicity Officer and Sjoerd Verduyn Lunel, EMS Secretary

Last Autumn, the EMS Executive Committee gathered at Yerevan State University (YSU), on the generous invitation of the Armenian Mathematical Union (AMU). On Friday evening, the meeting was addressed by Yuri Movsisyan, President of the AMU, who told us about its history. Mathematics in Armenia dates back to the 7th century scholar Anania Shirakatsi whose textbook on Arithmetic ("Tvabanutyun") is preserved in Yerevan's Matenadaran (Institute of Ancient Manuscripts). The AMU, however, is of more recent birth, having been founded in 1991 by a group of mathematicians at YSU and the Academy of Sciences of Armenia. Its first President was Alexander Talalyan. Since 1993, the AMU has been an adhering organisation of the IMU, and since 2016 a member society of EMS. It currently has around 250 members throughout Armenia and the diaspora. As well as the annual AMU session, it often organises special events. Recently, 2018 was a notable year, with a series of international activities for researchers and students to mark the 120th anniversary of the leading Austrian-Armenian mathematician Emil Artin, the 90th anniversary of Sergey Mergelyan, and the 100th anniversary of Mkhitar Djrbashian.

Officers' reports and membership

After a welcome from the Chair, EMS President Volker Mehrmann, and some preliminary business, the meeting got underway with his report on his recent activities (most of which feature separately later in this report). He drew special attention to ongoing discussions about Open Access involving both EMS Press and the publishing houses of other learned societies, as a response to Plan S. (See Mehrmann et al, EMS Newsletter, December 2019.)

The EMS Treasurer, Mats Gyllenberg then reported on the state of the society's finances, including the arrangements with EMS Press (the newly rebooted EMS Publishing House based in Berlin, see next page). Overall the EMS finances continue to be healthy, although with expenditure for scientific projects in 2019 below the allocated budget, the EC approved his proposal to transfer funds into the EMS portfolio.

The EMS Secretary, Sjoerd Verduyn Lunel, then delivered his report, including on preparations for the next EMS Council (see below).

EMS Vice-President Betül Tanbay delivered her report, including in her capacity as liaison with the Inter-

From left to right: Yuri Movsisyan (President of the Armenian Mathematical Union), Sjoerd Verduyn Lunel (EMS Secretary), Stefan Jackowski (EMS Executive Committee), Armen Sergeev (EMS Vice-President), Betül Tanbay (EMS Vice-President), Volker Mehrmann (EMS President), Mats Gyllenberg (EMS Treasurer), Elvira Hyvönen (EMS Secretariat), Valentin Zagrebnov (Editor-in-Chief of EMS Newsletter).

national Mathematical Union. It was agreed in the ensuing discussion that she will also oversee the compilation of a celebratory booklet on the history and mission of the EMS to mark its 30th anniversary in 2020.

The Executive Committee approved the list of 124 new individual members (including several under the EMS's new lifetime membership scheme) and one new institutional member. It then discussed possible action against two member societies who are in arrears on their dues and non-responsive to the President's letters.

EMS website and news

With the renewed EMS publishing house (EMS Press) now up and running, its CEO André Gaul has performed a thorough analysis of the systems and tools it uses, including its online presence. With the EMS webpage also due for renewal, the EC made several significant decisions regarding the future. It agreed to adopt a single design and technology with two webpages, and to reorganise the present content. It agreed that the EMS Press should take the lead on technical side of the webpage renewal, and that it is now appropriate to reconfigure the society's various information channels: the news webpage, the quarterly e-news, and this EMS Newsletter. On this topic, it decided to transform the Newsletter into a new EMS Magazine concentrating on articles and interviews, and separate from the daily news that will continue to be available through the EMS webpage. The EMS Magazine will follow an 'online first' protocol: features will be published online immediately that they ready, and every three months an EMS Magazine will be compiled these already published articles.

The EC discussed a report from the Publicity Officer Richard Elwes (who had presented his apologies), which noted that the EMS now has over 5000 followers on Twitter (https://twitter.com/EMSnewsletter) and over 3000 on Facebook (https://www.facebook.com/EMSnewsletter/).

Scientific meetings

Since its inception in 1992, the quadrennial European Congress of Mathematics (ECM) has been the EMS's headline event. The eighth instalment will take place in Slovenia, in July 2020 (https://www.8ecm.si/). The President reported on his recent visit to the site, and the committee discussed the ongoing preparations for this important occasion.

Looking further ahead, the committee considered the two live bids to organize the 9th ECM in 2024. These will each present their bid to the EMS Council in 2020 (directly before ECM8), where a final decision will be made by a vote by the Council delegates.

Vice-President Armen Sergeev then reported on the third Caucasian Mathematics Conference (CMC-III) that took place in Rostov-on-Don (Russia) in August 2019 and updated the EC about plans for CMC-IV to be held in Yerevan in 2021. There are also discussions about the possibility of a similar series to be held in the Balkans.

The President gave an update on a planned Euro-Pacific conference in 2021, and a proposed joint meeting of the EMS with the Indian Mathematics Consortium (TIMC) in India, also in 2021.

Society matters

The EMS Council is our society's governing body, and meets every two years. Its next meeting is in July 2020 in Bled (Slovenia), immediately prior to the ECM. The EC discussed preparations for this, both of a practical nature, and in terms of policies to be put to the council for a vote. These include a proposal for a formal structure through which young mathematicians can gain a voice in the society, and for the possible creation of special interest groups within the EMS.

The EC further agreed to invite representatives of the American Mathematical Society and International Mathematical Union as guests at the Council and ECM, and to extend an invitation to the ECM to other societies with which the EMS has reciprocity agreements (Australia, Canada and Japan).

The EC also discussed preparation for the upcoming annual meeting of Presidents of EMS Member Societies, which will take place in March 2020 at CIRM (France).

Standing committees, projects, and publishing

The EC made several appointments to EMS committees in need of renewal, before considering reports from the chairs or liaison officers of the committees for Applied Mathematics, Developing Countries (which administers the programmes Simons For Africa and ERCE – Emerging Regional Centres of Excellence), Education, Ethics (a particular focus was the EMS Code of Practice, and the scope of its adherence among member societies), European Solidarity, Meetings, Publishing and Electronic Dissemination, and Women in Mathematics. Following the last of these, the EC agreed to allocate a specific budget for activities of the Women in Mathematics committee.

The EC then discussed several projects with which the EMS is involved including the online Encyclopedia of Mathematics (www.encyclopediaofmath.org) with which EMS Press is expecting to become involved, EU-MATHS-IN (European Service Network of Mathematics for Industry and Innovation), and the Global Digital Mathematics Library.

The President presented an update on the progress of EMS Press. Although the new organisation is up and running in Berlin, there will be a transition period while the previous business is wound up. Valentin Zagrebnov as Editor-in-Chief of the Newsletter then presented his report, which the committee received with thanks. A report from Klaus Hulek, Editor-in-Chief of Zentralblatt Math was also received, and the President updated the EC about the German government's plan to facilitate its transition to open access in 2021.

Funding, political, and scientific organisations

The President reported on the latest developments regarding Horizon 2020 and reiterated the importance of the mathematics community speaking with one voice in all discussions with decision-makers. The President then gave an update on developments at the ERC (European Research Council), with former EMS President Jean-Pierre Bourguignon coming to the end of his tenure as President. In the ensuing discussion the EC considered the funding needs of mathematics, and the ERC's approach to these.

The next ESOF (European Science Open Forum) meeting will be in 2020 in Trieste (simultaneous with and nearby to ECM8). It is expected that the EMS Committee on Raising Public Awareness of Mathematics will organize a session there.

The President gave a brief update on recent developments regarding FAIRMAT (FAIR Mathematical Data for the European Open Science Cloud) as well as Plan S on open access.

The EC discussed the EMS's relationship with other mathematical organisations, including the IMU (International Mathematical Union), ICIAM (International Council for Industrial and Applied Mathematics), CIMPA (Centre International de Mathématiques Pures et Appliquées), the Bernoulli Society, the Banach Center, TICMI (Tbilisi International Center of Mathematics and Informatics), Oberwolfach, ECMI (the European Consortium for Mathematics in Industry), and the Abel Prize.

Close

The Executive Committee's next meeting will be in March 2020 at CIRM (France), followed immediately by the annual meeting of Presidents of EMS Member Societies. The meeting then closed with expressions of gratitude to Yerevan State University, the Armenian Mathematical Union, and to its President Yuri Movsisyan, for their magnificent hospitality and excellent organisation.

Mathematics Subject Classification 2020*

Edward Dunne (Mathematical Reviews, Ann Arbor, USA) and Klaus Hulek (Leibniz Universität Hannover, Germany)

The latest revision of the Mathematics Subject Classification (MSC) has been published, replacing the 2010 Mathematics Subject Classification (referred to as MSC2010). Searchable versions are available from the zbMATH site: https://zbmath.org/classification/ and the MathSciNet site: https://mathscinet.ams.org/mathscinet/searchMSC.html.

Mathematical Reviews (MR) and zbMATH collaborate on maintaining the Mathematics Subject Classification, which is used by these reviewing services, publishers, funding agencies and others to categorise items in the mathematical sciences literature. It is a taxonomy created by and for mathematical researchers. Every ten years, the two editorial groups solicit input from the mathematics community. For the current revision, we received over 350 comments and suggestions from more than 100 different people. MR and zbMATH carefully considered this input from the community and used it in the preparation of our joint revision of the classification.

As anticipated, there are no changes at the two-digit level, but several at the three-digit level, and hundreds at the five-digit level. Nine new three-digit classes were added: **18M** Monoidal categories and operads; **18N** Higher categories and homotopical algebra; **53E** Geometric evolution equations; **57K** Low-dimensional topology in specific dimensions; **57Z** Relations of manifolds and cell complexes with science and engineering; **60L** Rough analysis; **62R** Statistics on algebraic and topological structures; **68V** Computer science support for mathematical research and practice, and **82M** Basic methods in statistical mechanics. For five-digit classes, 113 classes were retired and 486 new classes were introduced. The new MSC contains 63 two-digit classifications, 529 three-digit classifications, and 6006 five-digit classifications.

There were some general changes. Descriptions of classes were changed to be more useful when searching online or via database interfaces. Previous descriptions assumed the user was looking at a full list of the classifications, which would provide context. An example of the limitation is a search of MSC2010 for "optimization", which returns 18 matches, not counting essentially every class in **49** Calculus of variations and optimal control; optimization. There were three classes named "Flow control and optimization": **76B75**, **76D55**, and **76N25**. The three different contexts were incompressible inviscid fluids, incompressible viscous fluids, and compressible fluids and gas dynamics. Now they have descriptions with more detail, as in **76B75** Flow control and optimization for incompressible inviscid fluids. There were three classes just named "Optimization" in the areas **74P** Mechanics of deformable solids, **78M50** Optics, electromagnetic theory, and **80M50** Classical thermodynamics, heat transfer. Now they have descriptions that include the context, as in **78M50** Optimization problems in optics and electromagnetic theory.

In previous versions of the MSC, there were some "hyphen classes" of the form **XX–00** General reference works, **XX–01** Introductory expositions, **XX–02**

* This article also appeared in the March edition of the Notices of the AMS. https://www.ams.org/journals/notices/202003/rnoti-p410.pdf

Research exposition, **XX–03** History, **XX–04** Software, and **XX–06** Proceedings, conferences, collections, etc., along with other scattered hyphen classes. The use of hyphen classes has been made more uniform across the MSC, so that most two-digit classes now have these five subclasses. Some hyphen classes would be redundant and are omitted, such as the non-existent class **01-03**, since the two-digit class for "History of mathematics and mathematicians" does not need a subclass for history. The classes **-08** for Computational methods for problems from the parent class, **-10** for Mathematical modeling or simulation for problems from the parent class, and **-11** for Research data for problems from the parent class have been added where appropriate. For example, there is now the class **20-08** Computational methods for problems from group theory and the class **20-11** Research data for problems from group theory. An example of an omission of one of these new hyphen classes for reasons of redundancy is **65** Numerical analysis, which does not need the **-08** class for computational methods. Also, some classes have alternatives to **-08** with more detail, such as the eight five-digit classes in the three-digit class **14Q** Computational aspects in algebraic geometry. The hyphen classes **-10** mostly occur for applied classes, namely MSCs **70** through **94**, as in **70-10** Mathematical modeling or simulation for problems from mechanics of particles and systems.

The influences of data and computation on the mathematical sciences are reflected in the classes. In addition to the **-08** classes, and not including classes from **03** (Mathematical logic and foundations) or **68** (Computer science), there are 58 classes referring to computations, computational methods, or computers. For instance, for MSC2020, two new classes, **14Q25** Computational algebraic geometry over arithmetic ground fields and **14Q30** Computational real algebraic geometry were added to the three-digit class **14Q** Computational aspects in algebraic geometry, which had been added to the MSC in 1991. Similarly, two new classes were added under **37M** Approximation methods and numerical treatment of dynamical systems: **37M21** Computational methods for invariant manifolds of dynamical systems, **37M22** Computational methods for attractors of dynamical systems and **37M25** Computational methods for ergodic theory. For the **-11** classes, examples of the types of data envisioned include statistical data, mathematical tables, collections of mathematical objects and their properties, such as integer sequences (as found in the OEIS, for instance), or databases of modular forms or Calabi-Yau varieties. In addition to the **-11** classes, there are 31 classes with specific instances of data, including the new classes **62R10** Functional data analysis, **62R40** Topological data analysis and **68P27** Privacy of data.

Mathematical Reviews and zbMATH are now using MSC2020 as their classification schemes. We welcome and encourage the community to also adopt the MSC2020. It is available from msc2020.org in PDF or TeX. A SKOS version will be available later.

The classification is jointly published by the two organisations under a Creative Commons CC-BY-NC-SA license. Corrections to possible errors in the new system can be submitted by email to feedback@msc2020.org. All information about MSC2020 is jointly shared by MR and zbMATH.

The editors and staff at Mathematical Reviews and zbMATH express their gratitude to the numerous members of the community for their assistance in this lengthy revision process.

Edward Dunne, Executive Editor,
Mathematical Reviews
Klaus Hulek, Editor-in-Chief, zbMATH

Renormalisation of Stochastic Partial Differential Equations

Yvain Bruned (University of Edinburgh, UK), Martin Hairer (Imperial College London, UK) and Lorenzo Zambotti (Sorbonne Université Paris, France)

We present the main ideas of the renormalisation of stochastic partial differential equations, as it appears in the theory of regularity structures. We informally discuss the regularisation of the noise, the transformation of the canonical model to the renormalised one, the space of the models and the underlying algebraic structure.

In the article [Hai14], the second author of this note introduced a theory of regularity structures (RS) in order to obtain for two important equations a notion of 'solution', as well as existence and uniqueness results, which had been open problems for decades. The first part of [Hai14] is a true *theory*, in the sense that it can be applied in the same way to a broad class of problems; however, the second part, that applies this theory to two concrete examples, contains more and more *ad hoc* arguments, which must be adapted if used in different contexts. Worse, for many other interesting equations, the approach of [Hai14] becomes intractable in practice because the combinatorial complexity of the objects involved can become arbitrarily large.

Fortunately, the situation has changed recently. The quartet of articles [Hai14, BHZ19, CH16, BCCH17] builds a fully automatic *black box* to obtain results of (local) existence and uniqueness (modulo an element of the 'renormalisation group' associated to the equation in question) for a broad class of stochastic partial differential equations (SPDEs), which includes

$$\partial_t u = \Delta u + (\partial_x u)^2 + \xi, \quad x \in \mathbf{R}, \qquad \text{(KPZ)}$$

$$\partial_t u = \Delta u + u\,\xi, \quad x \in \mathbf{R}^2, \qquad \text{(PAM)}$$

$$\partial_t u = \Delta u - u^3 + \xi, \quad x \in \mathbf{R}^3, \qquad (\Phi^4_3)$$

for $\xi \in \mathcal{D}'(\mathbf{R}^d)$ a random, stationary and possibly very irregular distribution (Schwartz generalised function). The main example of such a random distribution is given by *space-time white noise*, but the theory applies to a very large class of ξ.

These equations are called *singular*. Why? We can notice that it is possible to multiply a distribution $T \in \mathcal{D}'(\mathbf{R}^d)$ and a smooth function $\psi \in C^\infty(\mathbf{R}^d)$ in a canonical way, defining the product $\psi T = T\psi \in \mathcal{D}'(\mathbf{R}^d)$ by

$$(\psi T)(\varphi) = (T\psi)(\varphi) := T(\psi\varphi), \qquad \varphi \in C_0^\infty(\mathbf{R}^d).$$

But if $\psi \notin C^\infty(\mathbf{R}^d)$, this product is in general not well defined. Now, each of these equations contains some products between a distribution in $\mathcal{D}'(\mathbf{R}^d)$ and another distribution or function that is not sufficiently regular. More precisely:

- in KPZ (*Kardar-Parisi-Zhang*), u is no better than Hölder continuous in space, so the derivative $\partial_x u$ is a distribution and $(\partial_x u)^2$ is not well defined.
- in PAM (*Parabolic Anderson Model)*, ξ is a white noise in space, u is a non-smooth function, so $u\,\xi$ is not well defined.
- in (Φ^4_3), u is itself a distribution and so u^3 is not well defined.

In these equations, the notion of solution is therefore problematic, even before speaking of existence and uniqueness results.

Regularisation

To get around this problem, we can try to regularise the noise, solve the equation and then pass to the limit: let $\xi_\varepsilon = \varrho_\varepsilon * \xi$ be a regularisation of ξ, with $(\varrho_\varepsilon)_{\varepsilon>0}$ a family of even space-time mollifers, and let u_ε the solution of

$$\partial_t u_\varepsilon = \Delta u_\varepsilon + F(u_\varepsilon, \nabla u_\varepsilon, \xi_\varepsilon) \qquad (1)$$

where F is a non-linear function belonging to a suitable class of nonlinearities, which includes the nonlinearities of three equations above. The natural question is: what happens when $\varepsilon \to 0$? In order to control this limit, a natural approach is to look for a topology on the noises such that

1. the solution map $\Phi\colon \xi_\varepsilon \mapsto u_\varepsilon$ is continuous
2. $\xi_\varepsilon \to \xi$ when $\varepsilon \to 0$.

The first point requires a sufficiently strong topology, while the second requires a sufficiently weak topology. In fact, no solution seems possible if the regularity of ξ is too low, and even in the simplest case of stochastic *ordinary* differential equations it is a theorem that it is impossible to find a Banach space containing samples of the noise ξ and making the solution map continuous [Lyo91]. The analytic part of the regularity structures theory (RS) provides a framework for solving this problem by constructing, for a given equation,

- a metric space $(\mathcal{M}, \mathrm{d})$ called *space of models*
- a *canonical lift* of any smooth ξ_ε to a model $\mathbf{X}^\varepsilon \in \mathcal{M}$
- a *continuous function* $\boldsymbol{\Phi} : \mathcal{M} \to \mathcal{D}'(\mathbf{R}^d)$ such that $u_\varepsilon = \boldsymbol{\Phi}(\mathbf{X}^\varepsilon)$ solves the regularised equation (1), i.e., $\boldsymbol{\Phi}(\mathbf{X}^\varepsilon) = \Phi(\xi_\varepsilon)$.

This scheme is inspired by the theory of rough paths, initiated by Terry Lyons [Lyo98] and then developed, among others, by Massimiliano Gubinelli, whose ideas of controlled rough paths [Gub04] and branching rough paths [Gub10] served as a direct inspiration in the elaboration of regularity structures.

The RS theory identifies a class of equations, called *subcritical*, for which the canonical model $\mathbf{X}^\varepsilon \in \mathcal{M}$ encodes *a finite number of explicit multilinear functionals* obtained from the regularised noise ξ_ε by *pointwise multiplications* and *convolutions* with the heat kernel G or some derivatives of G, like for example $\partial_x G$. Among the components of the canonical model $\mathbf{X}^\varepsilon \in \mathcal{M}$ we can thus find

$$\xi_\varepsilon, \quad \xi_\varepsilon(G * \xi_\varepsilon)\,, \quad (\partial_x G * \xi_\varepsilon)^2, \quad \xi_\varepsilon\,(G * (\partial_x G * \xi_\varepsilon)^2). \qquad (2)$$

On the other hand, we do not have to consider *all* the possible functions of this type: for example, we typically do not expect (nor need) to make sense of ξ^2, so we do not consider ξ_ε^2 among the components of $\mathbf{X}^\varepsilon$.

To describe the functions that make up the components of $\mathbf{X}^\varepsilon$ we use a graphical notation: each function is represented by a rooted tree, where

- the edges correspond to convolutions with G (edges of type |) or $\partial_x G$ (edges of type **|**),
- each branching point corresponds to the pointwise product of the functions represented by the subtrees above the node in question.
- the noises are represented by nodes of type ○.

For example, the four functions in (2) are represented by the following trees:

$$○, \quad ⚲, \quad ∨, \quad ⋎. \tag{3}$$

Formally, we see $\mathbf{X}^\varepsilon$ as a linear map sending a space $\mathcal{H}$ of formal linear combinations of such trees into a space of distributions by writing $\mathbf{X}^\varepsilon(⚲) = \xi_\varepsilon(G * \xi_\varepsilon)$, etc. Note that the trees in (3) are naturally associated with a degree by applying the following rules: white noise has degree $-\frac{d}{2}$ with d the effective dimension of the corresponding space(-time), integration against the heat kernel increases degrees by 2, differentiation lowers degree by 1, and degrees are additive under multiplication. When $d = 3$ for example, we then have deg ○ $= -\frac{3}{2}$, deg ⚲ = deg ∨ $= -1$ and deg ⋎ $= -\frac{1}{2}$.

By simplifying a lot, we can say that convergence in $(\mathcal{M}, \mathrm{d})$ corresponds to the convergence of all these explicit functions as distributions. Note, however, that $\mathcal{M}$ is not a linear space: the topology of $\mathcal{M}$ encodes quantitative versions of statements of the type "close to the point z, the distribution $\mathbf{X}^\varepsilon(⚲)$ is well approximated by the distribution $\mathbf{X}^\varepsilon(◎)\mathbf{X}^\varepsilon(⚲)(z)$". (Note that the latter always makes sense since the argument of $\mathbf{X}^\varepsilon(⚲)$ is 'frozen' at the value z.) A major problem that appears in the examples (2) is that the products appearing in these expressions may diverge in the limit $\varepsilon \to 0$, e.g.,

$$\mathbf{E}[\xi_\varepsilon(G * \xi_\varepsilon)] = (\varrho_\varepsilon * G * \varrho_\varepsilon)(0) \to G(0) = +\infty\ ,$$

so that we do not expect in general that $\mathbf{X}^\varepsilon$ converges in $(\mathcal{M}, \mathrm{d})$ as $\varepsilon \to 0$.

Renormalisation

To overcome this problem, we must accept that it is necessary to *modify* (*renormalise*) some components of $\mathbf{X}^\varepsilon$ and define a new lift $\hat{\mathbf{X}}^\varepsilon \in \mathcal{M}$ of ξ_ε. For example, the canonical (pointwise) product $\xi_\varepsilon(G * \xi_\varepsilon)$, which diverges when $\varepsilon \to 0$ as we have just seen, can be replaced by

$$\begin{aligned}\mathbf{X}^\varepsilon\big(⚲\big) = \xi_\varepsilon(G * \xi_\varepsilon) \quad &\mapsto \quad \xi_\varepsilon(G * \xi_\varepsilon) - \mathbf{E}[\xi_\varepsilon(G * \xi_\varepsilon)] \\ &= \hat{\mathbf{X}}^\varepsilon\big(⚲\big).\end{aligned} \tag{4}$$

If, with appropriate modifications, we can build a lift $\hat{\mathbf{X}}^\varepsilon$ of ξ_ε such that

- we respect the non-linear constraints that define the space of models $\mathcal{M}$,
- the lift is 'admissible' in the sense that it respects the meaning of edges as convolution operators for planted trees, so one imposes for example that $\hat{\mathbf{X}}^\varepsilon(Y) = \partial_x G * \hat{\mathbf{X}}^\varepsilon(∨)$,
- we get a converging family in $(\mathcal{M}, \mathrm{d})$ when $\varepsilon \to 0$,

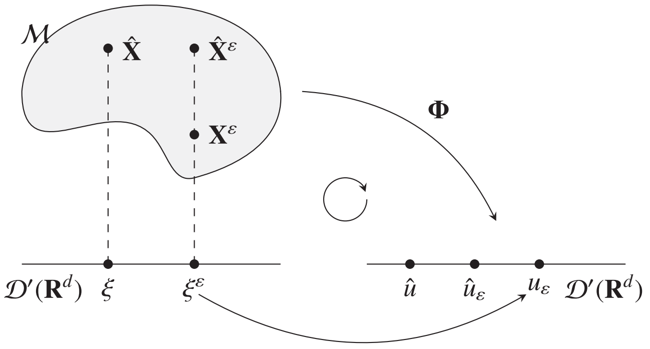


Figure 1. Illustration of the factorisation of the application $\xi_\varepsilon \mapsto u_\varepsilon$ into $\xi_\varepsilon \mapsto \mathbf{X}^\varepsilon \mapsto \mathbf{\Phi}(\mathbf{X}^\varepsilon) = u_\varepsilon$. In the space of the models $\mathcal{M}$, there are many possible lifts of $\xi_\varepsilon \in \mathcal{D}'(\mathbf{R}^d)$, e.g. the canonical model $\mathbf{X}^\varepsilon$ and the renormalised model $\hat{\mathbf{X}}^\varepsilon$; it is only the latter which converges to a model $\hat{\mathbf{X}}$, giving a lift of ξ.

then we can use the continuity of the solution map $\mathbf{\Phi}$ and get a family $\hat{u}_\varepsilon := \mathbf{\Phi}(\hat{\mathbf{X}}^\varepsilon)$ converging in $\mathcal{D}'(\mathbf{R}^d)$ to some limit $\hat{u}$ which may be a reasonable candidate for being 'the' solution we are looking for.

The changes in the components of $\mathbf{X}^\varepsilon$ cannot, of course, be totally arbitrary: the non-linear structure that we have already mentioned must be preserved, see also the discussion on page 10. The *renormalisation group* $\mathcal{G}_-$ that we describe in [BHZ19] is precisely the group of transformations of $\mathcal{M}$ that respect this structure and that furthermore preserve stationarity.

This procedure can be summarised in four steps:

- *Analytical step*: Construction of the space of models $(\mathcal{M}, \mathrm{d})$ and continuity of the solution map $\mathbf{\Phi} : \mathcal{M} \to \mathcal{D}'(\mathbf{R}^d)$, [Hai14].
- *Algebraic step*: Description of a group action on the space of models describing the transformation $\mathcal{M} \ni \mathbf{X}^\varepsilon \mapsto \hat{\mathbf{X}}^\varepsilon \in \mathcal{M}$ from the canonical model to the renormalised model, [BHZ19].
- *Probabilistic step*: Convergence in probability of the renormalised model $\hat{\mathbf{X}}^\varepsilon$ to a limit model $\hat{\mathbf{X}}$ in $(\mathcal{M}, \mathrm{d})$, [CH16].
- *Second algebraic step*: Identification of the renormalised equation satisfied by $\hat{u}_\varepsilon := \mathbf{\Phi}(\hat{\mathbf{X}}^\varepsilon)$, [BCCH17].

The final result is a *renormalised solution* $\hat{u} := \mathbf{\Phi}(\hat{\mathbf{X}})$, which is also the unique solution of a fixed point problem. Let us reiterate that all this works for very general noises, well beyond the Gaussian case.

Note here that the relation $\mathbf{\Phi}(\mathbf{X}^\varepsilon) = \Phi(\xi_\varepsilon)$ is broken by renormalisation, i.e., one has in general $\mathbf{\Phi}(\hat{\mathbf{X}}^\varepsilon) \neq \Phi(\xi_\varepsilon)$. At first glance one may be puzzled by this: have we really solved the original problem (5) or a completely different problem? The answer to this is somewhat subtle and requires us to realise that one rarely considers one single equation in isolation but is typically interested in solutions to a family of equations indexed by a number of constants (or possibly even functions). For example, in the case of the KPZ equation, we could consider the family of equations

$$\partial_t u = \partial_x^2 u + \lambda_1(\partial_x u)^2 - \lambda_2 + \xi\ ,$$

parametrised by $\lambda \in \mathbf{R}^2$. We should then view both the original 'naive' solution map Φ and the 'enhanced' solution map $\mathbf{\Phi}$ as depending not only on the noise ξ_ε (or model $\mathbf{X}^\varepsilon$), but also on the parameters λ describing a sufficiently large class of equations. It was then shown in [BCCH17] that the renormalisation group $\mathcal{G}_-$ already mentioned earlier does not only come with an action R on the space of models, but also with an action S on the parameter space of our class of equations, and these actions are intertwined in such a way that

$$\mathbf{\Phi}(\lambda, R^g\mathbf{X}) = \mathbf{\Phi}(S^g\lambda, \mathbf{X}) \;.$$

In particular, one can find elements $g_\varepsilon \in \mathcal{G}_-$ such that

$$\mathbf{\Phi}(\lambda, \hat{\mathbf{X}}^\varepsilon) = \mathbf{\Phi}(\lambda, R^{g_\varepsilon}\mathbf{X}^\varepsilon) = \mathbf{\Phi}(S^{g_\varepsilon}\lambda, \mathbf{X}^\varepsilon) = \Phi(S^{g_\varepsilon}\lambda, \xi_\varepsilon) \;.$$

One way of interpreting this is that the renormalisation procedure is nothing but a *change in parametrisation* for the family of solutions $\lambda \mapsto \Phi(\lambda, \xi_\varepsilon)$. We should then interpret our convergence as $\varepsilon \to 0$ not as the convergence of a single solution in this family, but as the simultaneous convergence of the entire family of solutions. In this sense, the limiting solution family $\lambda \mapsto \mathbf{\Phi}(\lambda, \hat{\mathbf{X}})$ should be viewed as the limit of the solution families $\lambda \mapsto \Phi(\lambda, \xi_\varepsilon)$ with the caveat that the parametrisation of this family has to be adjusted as $\varepsilon \to 0$ in order to get a non-degenerate parametrisation of the limiting family.

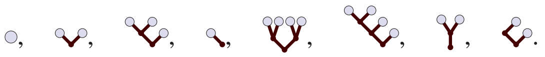
Note that this is precisely the same situation as arising in quantum field theory, where this change in parametrisation is the change from 'bare' to 'renormalised' coupling constants.

An example: KPZ

We consider the regularised version of the KPZ equation:

$$\partial_t u_\varepsilon = \partial_x^2 u_\varepsilon + \lambda_1(\partial_x u_\varepsilon)^2 + \lambda_2 + \xi_\varepsilon. \tag{5}$$

The (minimal) list of the trees representing the components of a model in $\mathcal{M}$ is in this case

 (6)

The renormalised version of the equation is then

$$\begin{aligned}\partial_t \hat u_\varepsilon &= \partial_x^2 \hat u_\varepsilon + \lambda_1(\partial_x \hat u_\varepsilon)^2 + \lambda_2 - \lambda_1^2 C_\varepsilon + \xi_\varepsilon,\\ C_\varepsilon &= \mathbf{E}\Big[(\partial_x G * \xi_\varepsilon)^2\Big] \sim \frac{1}{\varepsilon}.\end{aligned} \tag{7}$$

This makes it plain that (7) is nothing but (5), but with the ε-dependent change of parameters $(\lambda_1, \lambda_2) \mapsto (\lambda_1, \lambda_2 - \lambda_1^2 C_\varepsilon)$. The first mathematical article on KPZ was [BG97], where the solution is built via the Hopf-Cole transform, which is the simple remark that $z_\varepsilon := \exp(\hat u_\varepsilon)$ solves the *linear* equation

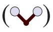
$$\partial_t z_\varepsilon = \partial_x^2 z_\varepsilon + z_\varepsilon\,(\xi_\varepsilon - C_\varepsilon) \;. \tag{8}$$

For this equation, one can show, in the particular case of regularisations ξ_ε that are white in time but coloured in space, that z_ε converges when $\varepsilon \to 0$ to a random function z, solution of the Itô equation

$$\partial_t z = \partial_x^2 z + z\,\xi.$$

We can then *define* $\hat u := \log z$ (after showing that $z > 0$ everywhere almost surely). Obviously, it is $\hat u_\varepsilon = \log z_\varepsilon$, solution of (7), which converges to $\hat u$, and not u_ε.

It is not before [Hai13] that a direct approach to (5)–(7) has been obtained which then allows us to deal with a much larger class of approximating equations. The reason why mathematicians have not been able to solve this equation for fifteen years is that it is not easy to deal with the convergence of $(\partial_x \hat u_\varepsilon)^2 - C_\varepsilon$ when $\varepsilon \to 0$. Thanks to the RS theory, we now know that it is enough to consider the convergence as a distribution of the family $\hat{\mathbf{X}}^\varepsilon(\tau)$ where τ varies over the family (6); for example

$\hat{\mathbf{X}}^\varepsilon($$) = (\partial_x G * \xi_\varepsilon)^2 - \mathbf{E}[(\partial_x G * \xi_\varepsilon)^2]$ (9)

which is the renormalised version of $(\partial_x G * \xi_\varepsilon)^2$. The continuity of the map $\mathbf{\Phi}$ allows us to conclude the convergence of $\hat u_\varepsilon := \mathbf{\Phi}(\hat{\mathbf{X}}^\varepsilon)$.

SPDEs with values in a manifold

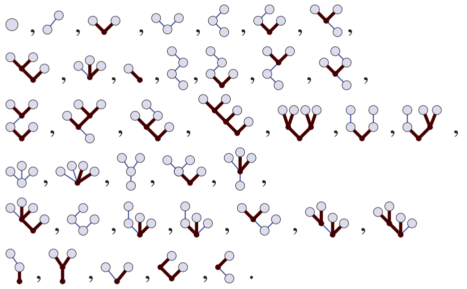
A recent application of the RS theory is the following: in [BGHZ19] the authors of this note with F. Gabriel have constructed a natural random dynamic on the space of loops in a Riemannian manifold with metric g. This evolution can be viewed as the solution to the SPDE given in local coordinates by

$$\partial_t u^\alpha = \partial_x^2 u^\alpha + \Gamma^\alpha_{\beta\gamma}(u)\,\partial_x u^\beta \partial_x u^\gamma + \sum_{i=1}^m \sigma_i^\alpha(u)\,\xi_i \;, \tag{10}$$

see Figure 2. Here, Γ denotes the Christoffel symbols of the metric g while the σ_i are any finite collection of smooth vector fields such that

$$\sum_i \sigma_i^\alpha(u)\sigma_i^\beta(u) = g^{\alpha\beta}(u) \;. \tag{11}$$

The list of trees indexing the components of a model in the space $(\mathcal{M}, \mathrm{d})$ associated to this class of equations is much longer. For example, the most relevant trees of negative degree are the following:

 (12)

In [BGHZ19], natural geometric quantities such as the scalar curvature play an important and fascinating role in the study of the equation (10). It was shown there that it is possible to perform the renormalisation of this equation in such a way that solutions perform under changes of variables as expected from the naïve application of the rules of calculus and such that the law of these solutions is independent of the choice of vector fields σ_i satisfying (11).

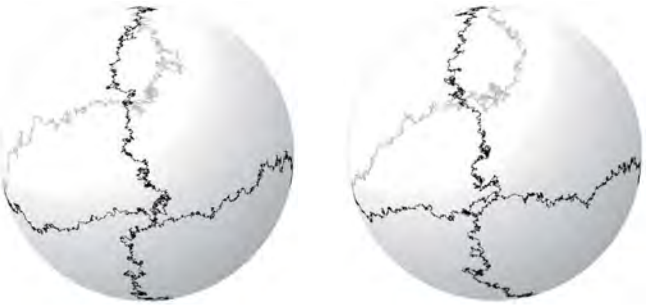


Figure 2. The solution of (10) **on the sphere at two successive times**

The algebraic structure

We can notice that the two examples of renormalised products that we discussed in (4)–(9) are simply given by the subtraction of a constant. In general, the renormalisation procedure (and therefore the transformation of $\mathbf{X}^\varepsilon$ to $\hat{\mathbf{X}}^\varepsilon$) is described in [BHZ19] by an operation of *recentering*. However, this recentering can be (much) more complicated than the simple subtraction of a constant; indeed, subtraction of a constant does not necessarily come from an 'admissible' transformation of the space of models, namely from the action of an element of the renormalisation group $\mathcal{G}_-$. It is shown in [BHZ19] that as long as the collection of trees $\mathcal{T}$ generating $\mathcal{H}$ has some properties natural in this context, there is a single (deterministic) $g_\varepsilon \in \mathcal{G}_-$, element of the renormalisation group such that if we set $\hat{\mathbf{X}}^\varepsilon(\tau) = \mathbf{X}^\varepsilon(g_\varepsilon\tau)$, then all components of $\hat{\mathbf{X}}^\varepsilon$ (corresponding to trees of negative degree, which are the only ones we ever considered in this note) have zero expectation. This is very similar to the 'BPHZ renormalisation' prescription found in the physics literature [BP57, Hep69, Zim69], so we call this particular choice of $\hat{\mathbf{X}}^\varepsilon$ the 'BPHZ lift' of the noise.

To describe the renormalisation group $\mathcal{G}_-$, we consider the algebra with unit $(\mathcal{H}_-, \cdot, \mathbf{1}_-)$ generated by the trees $\mathcal{T}_- \subset \mathcal{T}$ of negative degree (for example (6) for the KPZ equation or (12) for the loops in a manifold) and we realise $\mathcal{G}_-$ as the space of *characters* of $\mathcal{H}_-$, which are the algebra morphisms $g : \mathcal{H}_- \to \mathbf{R}$. To describe the group product in $\mathcal{G}_-$, we endow $\mathcal{H}_-$ with a structure of *coalgebra* with a *coproduct* $\Delta^- : \mathcal{H}_- \to \mathcal{H}_- \otimes \mathcal{H}_-$ which satisfies a property of *coassociativity*

$$(\Delta^- \otimes \mathrm{id})\Delta^- = (\mathrm{id} \otimes \Delta^-)\Delta^- \tag{13}$$

and a *counit* $\eta_- \in \mathcal{H}_-^*$ such that

$$(\eta_- \otimes \mathrm{id})\Delta^- = (\mathrm{id} \otimes \eta_-)\Delta^- = \mathrm{id} \tag{14}$$

on $\mathcal{H}_-$. The space $(\mathcal{H}_-, \cdot, \mathbf{1}_-, \Delta^-, \eta_-)$ is a *Hopf algebra*. The product in $\mathcal{G}_-$ is the dual of the coproduct in $\mathcal{H}_-$:

$$\mathcal{G}_- \times \mathcal{G}_- \ni (g_1, g_2) \mapsto g_1 \cdot g_2 \in \mathcal{G}_-,$$
$$(g_1 \star g_2)(h) := (g_1 \otimes g_2)\Delta^- h$$

for every $h \in \mathcal{H}_-$. The coassociativity (13) of Δ^- implies that this product is *associative*:

$$(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3),$$

and the counit η_- is the neutral element such that $\eta_- \star g = g \star \eta_- = g$ for every $g \in \mathcal{G}_-$, thanks to (14). Moreover, it is possible to show that every element of $\mathcal{G}_-$ has an inverse.

We have seen that a model $\mathbf{X} \in \mathcal{M}$ is determined by a linear map $\mathbf{X} : \mathcal{H} \to \mathcal{D}'(\mathbf{R}^d)$. Now if $\mathbf{X} \in \mathcal{M}$ is a model and $g \in \mathcal{G}_-$ is an element of the renormalisation group, we can define a new model $\mathbf{X}^g = R^g\mathbf{X} \in \mathcal{M}$ by

$$\mathbf{X}^g : \mathcal{H} \to \mathcal{D}'(\mathbf{R}^d), \qquad \mathbf{X}^g(\tau) := (g \otimes \mathbf{X})\Delta^- \tau\,, \tag{15}$$

where $\Delta^- : \mathcal{H} \to \mathcal{H}_- \otimes \mathcal{H}$ is defined very similarly to the coproduct of $\mathcal{H}_-$.

As already alluded to on page 8, the renormalisation group $\mathcal{G}_-$, which acts on the space of models $\mathcal{M}$, must preserve another underlying algebraic structure, described by another group called $\mathcal{G}_+$ and which allows us to describe the topology of the space $\mathcal{M}$. Similar to the construction of $\mathcal{G}_-$ and $\mathcal{H}_-$, we have a Hopf algebra $(\mathcal{H}_+, \cdot, \mathbf{1}_+, \Delta^+, \eta_+)$ generated by a collection $\mathcal{T}_+$ of trees, this time of *positive* degree, and the group $\mathcal{G}_+$ is described as the character group of $\mathcal{H}_+$. The group $\mathcal{G}_+$ acts on $\mathcal{H}$ similarly to above by $\tau \mapsto (\mathrm{id} \otimes g)\Delta^+\tau$ with $\Delta^+ : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}_+$ given by a formula very similar to that defining Δ^+. A linear map $\mathbf{X} : \mathcal{H} \to \mathcal{D}'(\mathbf{R}^d)$ then defines a model if there exists a $\mathcal{G}_+$-valued function $\mathbf{R}^d \ni x \mapsto f_x \in \mathcal{G}_+$ such that, for every $x \in \mathbf{R}^d$, the 'recentred' model $\mathbf{X}_x = (\mathbf{X} \otimes f_x)\Delta^+$ satisfies a bound of the type $|\mathbf{X}_x(\tau)(\varphi_x^\lambda)| \lesssim \lambda^{\deg \tau}$, whenever φ_x^λ is a scale λ approximation of a Dirac δ-distribution centred at x. Making this quantitative yields a topology on the space of models.

The fact that this topology is preserved by $\mathcal{G}_-$ is encoded in an action of $\mathcal{G}_-$ on $\mathcal{G}_+$, that is, a group morphism of $\mathcal{G}_-$ into the (outer) automorphisms of $\mathcal{G}_+$. The action of $\mathcal{G}_-$ on $\mathcal{G}_+$ is described by a map $\Delta^- : \mathcal{H}_+ \to \mathcal{H}_- \otimes \mathcal{H}_+$ which satisfies a property called *cointeraction*:

$$\mathcal{M}^{(13)(2)(4)}(\Delta^- \otimes \Delta^-)\Delta^+ = (\mathrm{id} \otimes \Delta^+)\Delta^-\,, \tag{16}$$

where $\mathcal{M}^{(13)(2)(4)}(\tau_1 \otimes \tau_2 \otimes \tau_3 \otimes \tau_4) := (\tau_1 \cdot \tau_3 \otimes \tau_2 \otimes \tau_4)$.

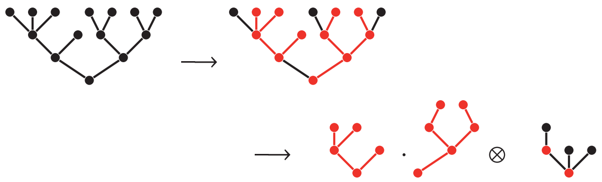
We now define the action of $\mathcal{G}_-$ on $\mathcal{G}_+$ like this: for $g_- \in \mathcal{G}_-$ and $g_+ \in \mathcal{G}_+$, $g_- \bullet g_+ \in \mathcal{G}_+$ is given by

$$(g_- \bullet g_+)(h_+) = (g_- \otimes g_+)\Delta^- h_+, \quad \forall\, h_+ \in \mathcal{H}_+.$$

We can easily see that the cointeraction property (16) defines an action:

$$g_- \bullet (\bar{g}_- \bullet g_+) = (g_- \star \bar{g}_-) \bullet g_+, \quad g_-, \bar{g}_- \in \mathcal{G}_-, \quad g_+ \in \mathcal{G}_+.$$

Let us conclude by giving a simplified description of the operations $\Delta^\pm$. Recall that the spaces $\mathcal{H}$, $\mathcal{H}_+$ and $\mathcal{H}_-$ are realised as vector spaces generated by (possibly collections of) *rooted and decorated trees*, see for example (6) or (12) above. The operations Δ^- and Δ^+ on such trees are both constructed by using an operation *of extraction and contraction* of subforests:

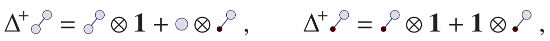


where

- we start from a tree or forest, drawn here in black on the left
- in the center, we select a subforest, colored in red
- on the right, the selected subforest is *extracted* in the left term of the tensor product, and *contracted* on the right. Note that in particular the total number of edges is always preserved by such operations.

The main difference between Δ^- and Δ^+ is in the selection of the subforests which are extracted: in the case of Δ^+, we extract only subforests consisting of a single tree that contains the root of the initial tree; in the case of Δ^-, we extract arbitrary subforests. In addition, the operation Δ^- only extracts subtrees of *negative* degree while Δ^+ only extracts those subtrees such that each 'trunk' adjacent to the root of the tree remaining on the right after contraction determines a subtree of *positive* degree.

Regarding the action of Δ^+, consider for example again the case of effective dimension 3, i.e., deg ○ $= -\frac{3}{2}$. In this case, one has for example



Δ^+ $=$ $\otimes \mathbf{1} +$ ○ $\otimes$,
Δ^+ $=$ $\otimes \mathbf{1} + \mathbf{1} \otimes$,

since these are the only ways in which we can extract/contract a subtree containing the root while being left on the right with a tree whose ‘branches’ touching the root are all of positive degree. A model $\mathbf{X}$ then must be such that there exists a function $x \mapsto f_x^{\bullet\!\diagup\!\circ}$ with the property that

$$\left|(\mathbf{X}{\circ\!\diagup\!\circ} + f_x^{\bullet\!\diagup\!\circ}\mathbf{X}\circ)(\varphi_x^\lambda)\right| \lesssim \lambda^{-1}\;, \qquad \left|(\mathbf{X}{\bullet\!\diagup\!\circ} + f_x^{\bullet\!\diagup\!\circ})(\varphi_x^\lambda)\right| \lesssim \lambda^{1/2}\;.$$

Note now that by admissibility, one must have $\mathbf{X}{\bullet\!\diagup\!\circ} = G * \mathbf{X}\circ = G * \xi$, which is a Hölder continuous function. Since the exponent $\frac{1}{2}$ appearing in the second bound above is positive, this *forces* to have $f_x^{\bullet\!\diagup\!\circ} = -(G * \xi)(x)$. The first identity is then precisely of the type “near x, $\mathbf{X}{\circ\!\diagup\!\circ}$ can be approximated by $(\mathbf{X}\circ) \cdot (\mathbf{X}{\bullet\!\diagup\!\circ})(x)$” as mentioned earlier on page 8.

Regarding the action of Δ^-, still in the same context, one has for example

$$\Delta^-{\circ\!\diagup\!\circ} = \mathbf{1} \otimes {\circ\!\diagup\!\circ} + {\circ\!\diagup\!\circ} \otimes \mathbf{1}\;, \quad \Delta^-{\circ\!\diagdown\!\circ\!\diagup\!\circ} = \mathbf{1} \otimes {\circ\!\diagdown\!\circ\!\diagup\!\circ} + {\circ\!\diagdown\!\circ\!\diagup\!\circ} \otimes \mathbf{1} + 2\,{\circ\!\diagup\!\circ} \otimes {\bullet\!\diagup\!\circ}\;.$$

(In principle, according to the description given above, one should add additional terms obtained by extracting and contracting single instances of the noise $\circ$, but we can ignore these since we will always consider centred noise.) We then see that if we want to construct the BPHZ lift of a noise ξ_ε, the first identity, combined with the BPHZ prescription that $\mathbf{E}\mathbf{X}^\varepsilon\tau = 0$ for $\deg\tau < 0$, forces us to choose a character g_ε such that $g_\varepsilon({\circ\!\diagup\!\circ}) = -\mathbf{E}\mathbf{X}^\varepsilon{\circ\!\diagup\!\circ}$, while the second identity then forces us to choose $g_\varepsilon({\circ\!\diagdown\!\circ\!\diagup\!\circ}) = -\mathbf{E}\mathbf{X}^\varepsilon{\circ\!\diagdown\!\circ\!\diagup\!\circ}$, yielding

$$\hat{\mathbf{X}}^\varepsilon{\circ\!\diagdown\!\circ\!\diagup\!\circ} = \mathbf{X}^\varepsilon{\circ\!\diagdown\!\circ\!\diagup\!\circ} - \mathbf{E}\mathbf{X}^\varepsilon{\circ\!\diagdown\!\circ\!\diagup\!\circ} - 2\mathbf{X}^\varepsilon{\bullet\!\diagup\!\circ} \cdot \mathbf{E}\mathbf{X}^\varepsilon{\circ\!\diagup\!\circ}\;.$$

The coassociativity and cointeraction properties seen above have a natural interpretation in terms of combinatorial operations on these trees and forests. Note that an algebraic structure very similar to our construction is known to arise in the numerical analysis of ordinary differential equations. There, this approach was pioneered by J. Butcher [But72] who pointed out that the natural composition operation for Runge–Kutta methods can be described by a Hopf algebra very similar to $\mathcal{H}_+$. More recently, it was pointed out by E. Hairer and his collaborators [CHV10] that an analogue of the Hopf algebra $\mathcal{H}_-$ has a natural interpretation as a ‘substitution operation’ for Runge–Kutta methods. The Hopf algebra $\mathcal{H}_+$ is also a generalisation of the so-called *Connes–Kreimer algebra* which was introduced in the 1990s to describe algebraically renormalisation in quantum field theory [CK98]. A review of this algebraic structure in various contexts is carried out in [CEFM11].

Bibliography

[BCCH17] Y. Bruned, A. Chandra, I. Chevyrev, and M. Hairer. Renormalising SPDEs in regularity structures. *ArXiv e-prints* (2017). To appear in J. Eur. Math. Soc. arXiv:1711.10239.

[BG97] L. Bertini and G. Giacomin. Stochastic Burgers and KPZ equations from particle systems. *Comm. Math. Phys.* **183**, no. 3, (1997), 571–607.

[BGHZ19] Y. Bruned, F. Gabriel, M. Hairer, and L. Zambotti. Geometric stochastic heat equations. *arXiv e-prints* (2019). arXiv:1902.02884.

[BHZ19] Y. Bruned, M. Hairer, and L. Zambotti. Algebraic renormalisation of regularity structures. *Invent. Math.* **215**, no. 3, (2019), 1039–1156. arXiv:1610.08468. doi:10.1007/s00222-018-0841-x.

[BP57] N. N. Bogoliubow and O. S. Parasiuk. Über die Multiplikation der Kausalfunktionen in der Quantentheorie der Felder. *Acta Math.* **97**, (1957), 227–266. doi:10.1007/BF02392399.

[But72] J. C. Butcher. An algebraic theory of integration methods. *Math. Comp.* **26**, (1972), 79–106. doi:10.2307/2004720.

[CEFM11] D. Calaque, K. Ebrahimi-Fard, and D. Manchon. Two interacting Hopf algebras of trees: a Hopf-algebraic approach to composition and substitution of B-series. *Adv. in Appl. Math.* **47**, no. 2, (2011), 282–308. arXiv:0806.2238. doi:10.1016/j.aam.2009.08.003.

[CH16] A. Chandra and M. Hairer. An analytic BPHZ theorem for Regularity Structures. *ArXiv e-prints* (2016). arXiv:1612.08138v5.

[CHV10] P. Chartier, E. Hairer, and G. Vilmart. Algebraic structures of B-series. *Found. Comput. Math.* **10**, no. 4, (2010), 407–427. doi:10.1007/s10208-010-9065-1.

[CK98] A. Connes and D. Kreimer. Hopf algebras, renormalization and noncommutative geometry. *Comm. Math. Phys.* **199**, no. 1, (1998), 203–242. arXiv:hep-th/9808042. doi:10.1007/s002200050499.

[Gub04] M. Gubinelli. Controlling rough paths. *Journal of Functional Analysis* **216**, no. 1, (2004), 86–140. doi:10.1016/j.jfa.2004.01.002.

[Gub10] M. Gubinelli. Ramification of rough paths. *Journal of Differential Equations* **248**, no. 4, (2010), 693–721. doi:10.1016/j.jde.2009.11.015.

[Hai13] M. Hairer. Solving the KPZ equation. *Ann. Math. (2)* **178**, no. 2, (2013), 559–664. arXiv:1109.6811. doi:10.4007/annals.2013.178.2.4.

[Hai14] M. Hairer. A theory of regularity structures. *Invent. Math.* **198**, no. 2, (2014), 269–504. arXiv:1303.5113. doi:10.1007/s00222-014-0505-4.

[Hep69] K. Hepp. On the equivalence of additive and analytic renormalization. *Comm. Math. Phys.* **14**, (1969), 67–69. doi:10.1007/BF01645456.

[Lyo91] T. Lyons. On the nonexistence of path integrals. *Proc. Roy. Soc. London Ser. A* **432**, no. 1885, (1991), 281–290.

[Lyo98] T. J. Lyons. Differential equations driven by rough signals. *Rev. Mat. Iberoamericana* **14**, no. 2, (1998), 215–310. doi:10.4171/RMI/240.

[Zim69] W. Zimmermann. Convergence of Bogoliubov’s method of renormalization in momentum space. *Comm. Math. Phys.* **15**, (1969), 208–234. doi:10.1007/BF01645676.

Yvain Bruned [yvain.bruned@ed.ac.uk] holds a doctorate in Mathematics from the University Paris 6 and is a lecturer at the University of Edinburgh. His main interests concern stochastic partial differential equations, Regularity Structures, Rough Paths and Hopf algebras.

Martin Hairer [m.hairer@imperial.ac.uk] obtained his PhD in mathematical physics from the University of Geneva and currently holds a chair for stochastic analysis at Imperial College London. His main mathematical interests lie in stochastic dynamic, stochastic partial differential equations, and the ergodic theory of stochastic processes.

Lorenzo Zambotti [zambotti@lpsm.paris] obtained his PhD from Scuola Normale Superiore in Pisa. He is currently head of the Laboratoire de Probabilités, Statistique et Modélisation in Paris, father of two children (Nicolò and Lidia) and supervisor of four PhD students (Jean-David, Florian, Lucas and David). In the spare time, he studies stochastic partial differential equations and stochastic analysis.

A Brief Introduction to Approximate Groups

Matthew C. H. Tointon (Pembroke College, University of Cambridge, UK)

We give a brief introduction to the notion of an approximate group and some of its numerous applications.

1 Approximately closed sets

Mathematicians are used to the notion of a subgroup of a group G as a subset containing the identity that is closed under taking products and inverses. However, it turns out that there are also circumstances in which we encounter subsets that are merely 'approximately closed'. Such sets arise in the study of *polynomial growth* in geometric group theory (which in turn has links to isoperimetric inequalities and random walks) and in the construction of *expander graphs* (which are important objects in computer science), but there are also numerous other examples.

A priori, there are several different ways to define approximate closure. One of these is the notion of a set of *small doubling*, with which we commence our discussion; another is the notion of an *approximate subgroup*, which we present in detail in Section 4. We shall see that these two notions are intimately linked.

We start by giving one interpretation of the phrase 'approximately closed'. Given subsets A, B of a group G, we set $AB = \{ab : a \in A, b \in B\}$ and $A^{-1} = \{a^{-1} : a \in A\}$. We also set $A^2 = AA$, $A^3 = AAA$, and so on. For additive abelian groups we write instead $A+B$, $-A$, $2A = A+A$, $3A = A+A+A$ and so on. To say that a finite subset A is closed under the group operation is then to say that $A^2 = A$. One property that could be interpreted as being an *approximate* version of closure is thus that A^2 is not too much bigger than A (we will discuss very briefly in Section 4 a possible extension to infinite subsets).

Let us consider for a moment the extreme values that $|A^2|$ can take. It is clear that $|A^2| \geq |A|$, with equality when A is a finite subgroup, for example. On the other hand, it is clear that $|A^2| \leq |A|^2$, with equality if $A = \{x_1, \ldots, x_r\}$ and G is the free group on the generators x_i.

Although it is extremal, the case in which $|A^2|$ is comparable to $|A|^2$ should not be thought of as atypical. Indeed, there is a fairly general phenomenon whereby if A is a suitably defined random set of size k inside some group then $\mathbb{E}[|A^2|] \geq ck^2$ for some constant c depending on the context. For example, if A is chosen uniformly from the interval $\{1, \ldots, n\} \subset (\mathbb{Z}, +)$ with n much larger than k then one can essentially take $c = \frac{1}{2}$ [4, Proposition 2.1.1]. This suggests that a condition of the type $|A^2| = o(|A|^2)$ is a stong constraint on the set A. We will consider this condition in its strongest form, in which

$$|A^2| \leq K|A| \tag{1}$$

for a given $K \geq 1$.

Definition 1. A set A satisfying (1) is called a *set of doubling at most K*, or simply a *set of small doubling*. The quantity $|A|^2/|A|$ is called the *doubling constant* of A. Similarly, a set A satisfying $|A^3| \leq K|A|$ is called a *set of tripling at most K*, or simply a *set of small tripling*. The quantity $|A|^3/|A|$ is called the *tripling constant* of A.

Since the inequality (1) is in some sense the opposite of what we would expect from a random set, it is reasonable to suppose that a set of small doubling should possess a certain amount of 'structure'. One of the principal goals of the theory of approximate groups is to describe this structure. In this article we give a brief overview of this theory; for more details, and for a more complete bibliography, the reader can consult the author's book [4].

We will often assume that the set A contains the identity and is *symmetric*, which is to say closed under taking inverses. For the majority of the results we present this is not a necessary hypothesis, but it simplifies the exposition and the notation.

2 First examples

A trivial family of examples of sets of small doubling is given by small sets: if $|A| \leq K$ then of course A satisfies $|A^2| \leq K|A|$. We will therefore focus on sets of size significantly larger than K. Finite subgroups also give easy examples of sets of small doubling. Note also that if a set A_0 has doubling constant at most K, and A is a subset of A_0 of *density* at most $\alpha \in [0, 1]$ (which is to say that $|A| \geq \alpha|A_0|$), then we have

$$|A^2| \leq |A_0^2| \leq K|A_0| \leq \frac{K}{\alpha}|A|,$$

and so the doubling constant of A is at most K/α. Thus, if A is sufficiently dense in some set of small doubling A_0 then A is also a set of small doubling. In particular, if H is a finite subgroup of G and the density in H of some subset $A \subset H$ is at least $1/K$ then the doubling constant of A is at most K. Freiman showed that for small enough K this essentially exhausts all of the examples of sets of doubling K. More precisely, he showed that if $|A^2| < \frac{3}{2}|A|$ then A^2 is a coset of a finite subgroup (see [4, Theorem 2.2.1]).

We now consider a more interesting example. Note first of all that if $B \subset \mathbb{Z}^d$ is a 'box' of the form

$$B = \{x \in \mathbb{Z}^d : |x_i| \leq L_i \text{ for } i = 1, \ldots, d\}$$

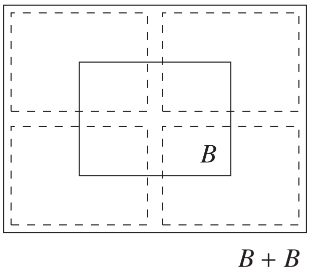
for some $L_i \in \mathbb{N}$ then

$$|B + B| \leq 2^d|B| \tag{2}$$

regardless of the values taken by the L_i. Boxes in $\mathbb{Z}^d$ are thus sets of small doubling. It is also easy to check that their homomorphic images are also sets of small doubling. To see this, first note that such a box B satisfies a stronger property than (2), in that there exists a set X satisfying $|X| = 2^d$ such that

$$B + B \subset B + X, \tag{3}$$

as illustrated in the following diagram.

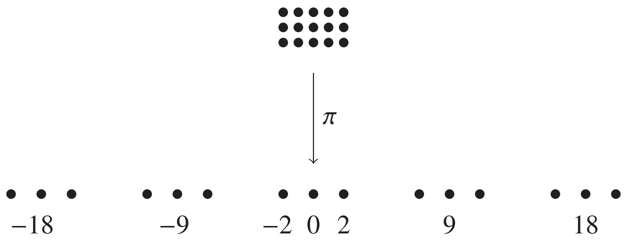


This means that if G is an abelian group and $\pi : \mathbb{Z}^d \to G$ is a homomorphism then $\pi(B) + \pi(B) \subset \pi(X) + \pi(B)$. In particular, $|\pi(B) + \pi(B)| \leq 2^d|\pi(B)|$, and so $\pi(B)$ has small doubling.

A homomorphic image of a box such as B is called a *progression*. More precisely, if $x_1, \ldots, x_d$ are elements of an abelian group and $L_1, \ldots, L_d \in \mathbb{N}$ then we set

$$P = P(x; L) = \{\ell_1 x_1 + \cdots + \ell_d x_d : |\ell_i| \leq L_i\}.$$

We call P a *progression*, and we call d the *rank* or the *dimension* of P. For example, in the following diagram we illustrate the progression $P(9, 2; 2, 1) \subset \mathbb{Z}$, viewed as $\pi(\mathbb{Z}^2 \cap ([-2, 2] \times [-1, 1]))$ with $\pi : \mathbb{Z}^2 \to \mathbb{Z}$ defined by $\pi(1, 0) = 9$ and $\pi(0, 1) = 2$.



To explain the term *progression*, note that if the rank of P is 1 then P is an arithmetic progression.

We have just seen that subgroups, progressions of bounded rank, and their dense subsets are all examples of sets of small doubling. The following remarkable theorem, due to Freiman in the case $G = \mathbb{Z}$ and Green and Ruzsa in the general case, shows that these are essentially the only examples in an abelian group.

Theorem 2 (Green–Ruzsa)**.** *Let G be an abelian group, and suppose that $A \subset G$ is a finite subset satisfying $|A + A| \leq K|A|$. Then there exist a finite subgroup H and a progression P of rank at most $r(K)$ such that A is a subset of $H + P$ of density at least $\delta(K)$.*

The proof is largely Fourier analytic, and gives explicit bounds on $r(K)$ and $\delta(K)$. Optimising these bounds continues to be an area of active research.

3 Plünnecke's inequalities and Ruzsa's covering lemma

The proof of Theorem 2 is too long to be included in this article, but we will illustrate two fundamental tools from the proof by considering the following special case.

Proposition 3 (Ruzsa)**.** *Let $m \in \mathbb{N}$, and let G be an abelian group in which each element has order at most m (such as $G = (\mathbb{Z}/m\mathbb{Z})^n$ for some $n \in \mathbb{N}$). Suppose that A is a finite symmetric subset of G such that $|A + A| \leq K|A|$. Then A is a subset of density at least $1/(m^{K^4}K)$ in some finite subgroup of G.*

The first tool we present is *Plünnecke's inequalities*, which were first proved by Plünnecke, then rediscovered and generalised by Ruzsa, and finally proved much more simply by Petridis.

Proposition 4 (Plünnecke–Ruzsa)**.** *Let G be an abelian group and suppose that A is a finite subset satisfying $|A + A| \leq K|A|$. Then $|mA - nA| \leq K^{m+n}|A|$ for every $m, n \in \mathbb{N}$.*

We will soon see concretely the role that this result plays in the proof of Proposition 3, but before that let us give a brief heuristic discussion of why one might expect such a result to be useful. First, note that if H is a subgroup then $mH = H$ for every $m \in \mathbb{N}$, a property that we use often without even thinking. Proposition 4 says that a set of small doubling satisfies an approximate version of this property: if A is a finite set satisfying $|A + A| \leq K|A|$ then, for every $m \in \mathbb{N}$, on the one hand the set mA is not much bigger than A, and on the other hand it is also of small doubling, in the sense that $|mA + mA| \leq K^{2m}|A| \leq K^{2m}|mA|$.

Another important tool featuring in the proof of Proposition 3 is the so-called 'covering lemma' of Ruzsa. We present a slightly simplified version of it here; see [1, Lemma 5.1] for a more general statement.

Lemma 5 (Ruzsa)**.** *Suppose A is a finite symmetric subset of a group G such that $|A^4| \leq K|A|$. Then there exists $X \subset G$ of size at most K such that $A^3 \subset XA^2$.*

Proof. Let $X \subset A^3$ be maximal such that the subsets xA with $x \in X$ are disjoint, noting that $|XA| = |X||A|$. Since $XA \subset A^4$, this implies that $|X||A| \leq K|A|$, and hence that $|X| \leq K$. Moreover, given $z \in A^3$ the maximality of X implies that there exist $x \in X$ and $a_1, a_2 \in A$ such that $za_1 = xa_2$, and hence $z = xa_2a_1^{-1} \in XA^2$. In particular, $A^3 \subset XA^2$ as required. □

Proof of Proposition 3. Proposition 4 implies that

$$|4A| \leq K^4|A|.$$

Lemma 5 therefore implies that there exists a set X of size at most K^4 such that $3A \subset X + 2A$. This implies by induction that $mA \subset (m-2)X + 2A$ for every $m > 3$. Writing $\langle B\rangle$ for the subgroup generated by a set B, we deduce in particular that $\langle A\rangle \subset \langle X\rangle + 2A$, and hence that $|\langle A\rangle| \leq |\langle X\rangle||2A| \leq m^{K^4}K|A|$, as required. □

4 Approximate groups

When G is not abelian, Proposition 4 no longer holds as stated. For example, if G is the free product $H * \langle x\rangle$ with x some element of infinite order, and if we take

$$A = H \cup \{x\}, \tag{4}$$

then $A^2 = H \cup xH \cup Hx \cup \{x^2\}$, hence in particular $|A^2| \le 3|A|$. On the other hand, $A^3 \supset HxH$ and $|HxH| = |H|^2$, so $|A^3| \ge \frac{1}{4}|A|^2$.

Nonetheless, it turns out that if we replace $|A + A| \le K|A|$ with a slightly stronger hypothesis then we can obtain a conclusion analogous to that of Proposition 4. In fact, there are at least two such possible ways in which to strengthen the condition of small doubling. The first is to replace it with the condition of small tripling: an argument of Ruzsa shows that if we assume $|A^3| \le K|A|$ instead of $|A^2| \le K|A|$ for a finite symmetric set A then we may conclude that $|A^m| \le K^{m-2}|A|$ for every $m \in \mathbb{N}$. In other words, unlike small doubling, small tripling permits us to bound the sizes of all of the sets $A^4, A^5, \ldots$.

The second possibility is to replace the condition $|A^2| \le K|A|$ by a property that we have already encountered in both Lemma 5 and (3): the existence of a set X of bounded size such that $A^2 \subset XA$, which easily implies that A has small doubling. It is this condition that underpins the following definition of an approximate subgroup, which is due to Tao.

Definition 6. A subset A of a group G is a *K-approximate (sub)group* if it is symmetric and contains the identity and there exists a set $X \subset G$ of size at most K such that $A^2 \subset XA$.

It is easy to see by induction that a K-approximate group A satisfies $A^m \subset X^{m-1}A$ for every $m \in \mathbb{N}$, so if A is finite then $|A^m| \le K^{m-1}|A|$ and once again we have an analogue of Proposition 4.

In fact, these two conditions – having small tripling and being an approximate group – are essentially equivalent for finite sets. We have just noted that if A is a finite K-approximate group then $|A^3| \le K^2|A|$, so A has small tripling. Conversely, for a finite symmetric set A satisfying $|A^3| \le K|A|$, the result of Ruzsa shows that $|A^4| \le K^2|A|$, and then Lemma 5 implies that A^2 is a K^4-approximate subgroup (we have $A^3 \subset XA^2$ by Lemma 5, and hence $A^4 = A^3A \subset XA^3 \subset X^2A^2$).

Note that one advantage of the notion of an approximate subgroup is that it can be applied without modification to arbitrary infinite subsets of groups, for which the notion of small tripling does not in general make sense. Indeed, infinite approximate groups have begun to be studied in certain contexts. However, at the time of writing the theory is far more advanced for finite approximate groups, and we will concentrate on them for the remainder of this article.

When introducing the definition of approximate groups, Tao showed that the study of sets of small doubling essentially reduces to the study of finite approximate groups. First, note that in example (4), A possesses a large subset that is a 1-approximate subgroup, namely H. Tao showed that this is a general phenomenon, in the sense that there exists $C > 0$ such that given any set $|A^2| \le K|A|$ there exists a K^C-approximate group $B \subset G$ of size at most $K^C|A|$ such that A is contained in a union of at most K^C left translates of B. One may thus replace the hypothesis $|A^2| \le K|A|$ by the hypothesis of being a K-approximate subgroup without really losing any generality, whilst gaining the ability to control the sizes of the sets $A^4, A^5, \ldots$

We close this section by noting that Ruzsa proved Lemma 5 several years before the introduction of Definition 6 by Tao. In that sense, Ruzsa's work can be thought of as a precursor to the notion of approximate group.

5 Basic properties

Here are two simple but useful properties of a subgroup H of G:

(1) If $\pi : G \to Z$ is a homomorphism then $\pi(H)$ is again a subgroup of Z.

(2) If $N < G$ is another subgroup then $H \cap N$ is also a subgroup.

It turns out that these properties have approximate analogues for approximate groups and sets of small tripling. For (1), if A is a K-approximate subgroup of G and $\pi : G \to Z$ is a homomorphism then it is trivially the case that $\pi(A)$ is a K-approximate subgroup of Z. Less obviously, an argument of Helfgott shows that if A is a finite symmetric subset of G then

$$\frac{|\pi(A)^m|}{|\pi(A)|} \le \frac{|A^{m+2}|}{|A|},$$

so in particular if $|A^3| \le K|A|$ then $|\pi(A)^3| \le K^3|\pi(A)|$. For (2), one can show for example that A and B are finite symmetric subsets of G then

$$\frac{|A^m \cap B^n|}{|A^2 \cap B^2|} \le \frac{|A^{m+1}|}{|A|}\frac{|B^{n+1}|}{|B|}$$

for every $m, n \ge 2$, and in particular if $|A^3| \le K|A|$ and $|B^3| \le L|B|$ then $|(A^2 \cap B^2)^3| \le (KL)^5|A^2 \cap B^2|$. Similarly, if A is a K-approximate group and B is an L-approximate group then $A^2 \cap B^2$ is a $(KL)^3$-approximate group. See [4, §2.6] for proofs and generalisations of these assertions.

We saw in the previous section that approximate groups and sets of small tripling are essentially equivalent notions. In this section we have seen that they satisfy the same basic properties, which renders them interchangeable in a number of arguments.

6 Approximate subgroups of non-abelian groups

One can generalise the concept of progression to certain non-abelian groups. For example, consider the *Heisenberg group* H defined by

$$H = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & n_2 & n_3 \\ 0 & 1 & n_1 \\ 0 & 0 & 1 \end{pmatrix} : n_i \in \mathbb{Z} \right\},$$

and set

$$Q = \left\{ \begin{pmatrix} 1 & \ell_1 & \ell_3 \\ 0 & 1 & \ell_2 \\ 0 & 0 & 1 \end{pmatrix} : \ |\ell_1| \le L_1, |\ell_2| \le L_1, |\ell_3| \le L_1L_2 \ \right\}.$$

It is an easy exercise to check that

$$Q^3 \subset \left\{ \begin{pmatrix} 1 & \ell_1 & \ell_3 \\ 0 & 1 & \ell_2 \\ 0 & 0 & 1 \end{pmatrix} : \begin{array}{l} |\ell_1| \le 3L_1, \\ |\ell_2| \le 3L_1, \\ |\ell_3| \le 8L_1L_2 \end{array} \right\},$$

and hence that $|Q^3| \le 72|Q|$ regardless of the values of L_1, L_2.

The key property of H that makes this true is that it is *nilpotent*. To define this, first define the *lower central series* of a group G to be the decreasing sequence of normal subgroups $G = G_1 > G_2 > \cdots$ defined recursively by setting $G_1 = G$ and $G_{n+1} = [G, G_n]$. A group G is then said to be *nilpotent* if there exists s such that $G_{s+1} = \{1\}$. The smallest s for which this holds is said to be the *step* or *class* of G. For the Heisenberg group H we have

$$H_2 = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad H_3 = \{1\},$$

so that H is 2-step nilpotent.

It turns out that we can define a progression in the same way as we did in the Heisenberg group in an arbitrary nilpotent group, as follows.

Definition 7. Let G be an s-step nilpotent group, let $x_1, \ldots, x_r \in G$, and let $L_1, \ldots, L_r \in \mathbb{N}$. Then we define $P(x; L) \subset G$ to be the set of those elements of G expressible as products of the elements $x_i^{\pm 1}$ in which each x_i and its inverse appear at most L_i times between them. We call $P(x; L)$ a *nilprogression* of *rank* r and *step* s.

One can show that if the L_i are large enough in terms of r and s then the nilprogression $P(x; L)$ is a K-approximate group of some K depending only on r and s.

The 'progression' Q is not exactly a nilprogression, but one can check that if we set

$$x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad x_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then $P(x; L) \subset Q \subset P(x; 5L)$, so Q is roughly equivalent to a nilprogression in some sense. See [4, Definition 5.6.2] for a generalisation of Q to arbitrary nilpotent groups, and [4, Proposition 5.6.4] for further details on this rough equivalence.

The following remarkable result of Breuillard, Green and Tao shows that nilprogressions are essentially the most general examples of sets of small doubling.

Theorem 8 (Breuillard–Green–Tao [1, Theorem 2.12])**.** *Let G be an arbitrary group and $A \subset G$ a finite subset such that $|A^2| \le K|A|$. Then G contains a subset P containing a finite subgroup H normalised by P, such that the image of P in $\langle P \rangle / H$ is a nilprogression of rank at most $r(K)$ and step at most $s(K)$, and such that $|P| \le t(K)|A|$. There also exists a set X of size at most $i(K)$ such that $A \subset XP$.*

In addition to the general theory of approximate groups, the proof of Theorem 8 uses tools from model theory introduced by Hrushovski, and arguments essentially due to Gleason arising from the solution to Hilbert's fifth problem in the 1950s.

The use of an ultrafilter in the model-theoretic arguments means that the proof of Theorem 8 gives no explicit bound on $i(K)$. For some applications of approximate groups, notably those to *growth* of groups that we present in Section 7, this does not pose a major problem. However, there are also applications of approximate groups, such as to *expansion*, in which it is important to have more explicit results than Theorem 8. Partly for this reason, numerous authors have given proofs of Theorem 8 that offer explicit bounds on $i(K)$ in return for restricting attention to certain specific classes of groups. There are such results, for example, in the case of soluble groups, residually nilpotent groups, and certain linear groups. In the next section we will discuss briefly how some of these results for linear groups are used in the construction of expanders.

7 Applications to growth and expansion in groups

In this section we describe two of the most spectacular applications of approximate groups. We begin with applications to *growth* of finitely generated groups, a notion that is in turn linked to random walks, geometric group theory and differential geometry. After that we will discuss applications to *expansion*, a notion which appears in several branches of mathematics and has numerous applications, particularly in theoretical computer science.

Let G be a finitely generated group and S a finite symmetric generating subset. The *growth* of G refers to the speed with which the cardinality of the sets $S^1, S^2, \ldots$ grows. It is not difficult to show that if G is *virtually nilpotent* – that is to say, if G contains a nilpotent subgroup of finite index – then there exist $C, d \ge 0$ such that $|S^n| \le Cn^d$ for every $n \in \mathbb{N}$. In that case we say that G has *polynomial growth*. A fundamental theorem of Gromov says that the converse also holds: every finitely generated group of polynomial growth is virtually nilpotent.

It turns out that approximate groups can be used to prove Gromov's theorem. In fact, Breuillard, Green and Tao used Theorem 8 to prove a refined version of Gromov's theorem. For example, the quantitative statement of Gromov's theorem implicitly requires the generating set to be of bounded cardinality, but in the Breuillard–Green–Tao version this hypothesis is not necessary.

The observation that allows one to reduce Gromov's theorem to Theorem 8 is that the condition

$$|S^n| \le n^d |S| \tag{5}$$

implies that there exists $K \ge 1$ depending only on d, and an integer m satisfying $\sqrt{n} \le m \le n$, such that $|S^{2m}| \le K|S^m|$. In other words, (5) implies that there exists m not too small such that S^m is a set of small doubling. Thus, approximate groups appear very naturally in the study of groups of polynomial growth. We refer the reader to [4, Chapter 11] and the references therein for more details and further applications in this direction.

Another important application of approximate groups is the construction of *expander graphs*. An *expander graph* is a graph that is both sparse and highly connected. Precisely, given a subset A of a finite graph Γ, we define the *boundary* ∂A of A by setting $\partial A = \{x \in \Gamma \setminus A : (\exists a \in A)(x \sim a)\}$, and we define the *(vertex) Cheeger constant* $h(\Gamma)$ of Γ by setting

$$h(\Gamma) = \min_{|A| \le |\Gamma|/2} \frac{|\partial A|}{|A|}.$$

Given $\varepsilon > 0$ and $d \in \mathbb{N}$, a family X of finite graphs is said to be a *family of (ε, d)-expanders* if $h(\Gamma) \ge \varepsilon$ for every $\Gamma \in X$, if $\sup_{\Gamma \in X} |\Gamma| = \infty$, and if each vertex of each graph in X has degree at most d. Note that if a finite graph Γ is complete then $h(\Gamma) \ge 1$; the upper bound on the degrees rules out this trivial situation, and is the sense in which expanders are sparse.

To see why such graphs are interesting, note that sparsity and high connectivity are both desirable properties of communication and transport networks, yet are intuitively difficult to achieve simultaneously.

One of the objectives, and one of the difficulties, in the theory of expander graphs is their construction. One fruitful approach is based on group theory and the notion of a *Cayley graph*. Given a finitely generated group G and a finite symmetric generating set S, the *Cayley graph* $\Gamma(G, S)$ has the elements of G as its vertices, and has x and y joined by an edge if there exists $s \in S$ such that $xs = y$.

It turns out that certain results using techniques from the theory of approximate groups can be applied in the construction of expander Cayley graphs. For example, for $SL_n(\mathbb{K})$ we have the following theorem, which was announced independently (within four hours of one another!) by Breuillard–Green–Tao and Pyber–Szabo, Helfgott having already treated the cases $d = 2, 3$ for $\mathbb{K} = \mathbb{F}_p$ with p prime.

Theorem 9 ([2, Theorem 1.5.1])**.** *Let $\mathbb{K}$ be a finite field and let $n \geq 2$. Let A be a generating set of $SL_n(\mathbb{K})$. Suppose that $\varepsilon > 0$ is small enough in terms of n. Then either $|A^3| \geq |A|^{1+\varepsilon}$, or $|A| \geq |SL_n(\mathbb{K})|^{1-c_n\varepsilon}$, with c_n a certain constant depending only on n.*

It turns out that using Theorem 9 and an ingenious argument of Bourgain and Gamburd one can show that certain Cayley graphs of $SL_n(\mathbb{F}_p)$ are expander graphs. For further details on this argument and its history the reader can consult Tao's book [2].

Bibliography

[1] E. Breuillard, B. J. Green, and T. Tao. The structure of approximate groups. *Publ. Math. IHES*, 116:115–221, 2012.

[2] T. Tao. *Expansion in finite simple groups of Lie type*, volume 164 of *Graduate Studies in Mathematics*. Amer. Math. Soc., Providence, RI, 2015.

[3] M. C. H. Tointon. Raconte-moi ... les groupes approximatifs. *Gaz. Math.*, 160:53–59, 2019. In French.

[4] M. C. H. Tointon. *Introduction to approximate groups*, volume 94 of *London Mathematical Society Student Texts*. Cambridge Univ. Press, 2020.

Matthew Tointon [mcht2@cam.ac.uk] is the Stokes Research Fellow at Pembroke College, University of Cambridge. His book 'Introduction to Approximate Groups' has recently appeared in the LMS Student Texts series, published by Cambridge University Press.

This is a translation of the author's article 'Raconte-moi ... les groupes approximatifs', which appeared in the Gazette des mathématiciens *in April 2019* [3]. *It appears here with the kind permission of the* Gazette.

A Discussion with Freeman Dyson

Michael Th. Rassias (University of Zürich, Switzerland)

Note: Just a few days before this article was printed, we were all saddened by Freeman Dyson's passing on February 28, 2020. The article below is published in its original form.

Freeman Dyson presenting his new book *Maker of Patterns.* (Photo: Dan Komoda/Institute for Advanced Study, Princeton, NJ, USA)

Freeman J. Dyson, born in 1923 in Crowthorne in Berkshire, England, is a world-famous American theoretical physicist and mathematician, whose academic stature is that of a historical figure of science. At the beginning of his career he worked as a civilian scientist for the Royal Air Force in World War II. In 1945 he obtained his B.A. degree in mathematics from Cambridge University. He had a job as an instructor at Imperial College from 1945–1946, and in 1947 he went to Cornell University as a graduate student, where he worked with Hans Bethe and Richard Feynman. Subsequently, he was a member of the Institute for Advanced Study, Princeton, from 1948–1949 and a research fellow at the University of Birmingham from 1949–1951. He then became professor at Cornell University, where he remained until 1953. Surprisingly, he was made professor at Cornell notwithstanding the fact that he did not have and never actually obtained a Ph.D. (a topic also discussed with him below). In 1953 he became a permanent professor at the Institute for Advanced Study, Princeton, where he has remained throughout the rest of his career.

Freeman Dyson has made numerous profound contributions in a broad spectrum of subjects of mathematics and physics, among which is the unification of the three versions of quantum electrodynamics invented by Richard Feynman, Julian Schwinger and Shin'ichirō Tomonaga. His work and lectures on Feynman's theories played an integral role in making them understandable to physicists of the time, and this helped Feynman's work to be accepted by the academic community. His work on this subject impressed J. Robert Oppenheimer and had an impact on him being offered a permanent position at the Institute for Advanced Study, Princeton.

Among his participation in many diverse and important projects, it is also worth mentioning that in 1958 he was a member of the design team under Edward Teller for a small and really safe nuclear reactor used throughout the world in hospitals and universities for the production of medical isotopes.

Dyson's passion has always been to explore problems through which mathematics can be usefully applied. His span of scientific interests and his everlasting appetite for exploration have lead him to investigate problems not only in mathematics, physics and their interconnections, but also in other subjects such as biology.

During his career, he has been bestowed with a plethora of awards and distinctions, including becoming a Fellow of the Royal Society (1952), receiving the Lorentz Medal (1966), the Wolf Prize (1981), the Enrico Fermi Award (1993), the Templeton Prize (2000), the Henri Poincaré Prize (2012), to name just a few.

Honoured and humbled to be surrounded by such pillars of science during my time as a visiting researcher at the Program in Interdisciplinary Studies of the Institute for Advanced Study, Princeton, I had the great privilege of first meeting Freeman Dyson in around 2015. Since then, I have had the opportunity to spend some time with him, hoping to absorb some of his wisdom. Inspired by his accomplishments, and always spellbound by his beautiful tales of the numerous interesting events of his life, the idea arose for the following discussion to be shared with the readers of the EMS Newsletter.

You started your academic career as a pure mathematician, worked with Davenport for a while and among other things proved Minkowski's conjecture in four dimensions using methods from various areas of mathematics. You later turned to physics. At which age did you decide to become a mathematician?

I met Davenport during the year 1945–1946 when I had a job at Imperial College as an instructor. He was at University College, so I was not officially his student. He generously supplied me with problems to work on, hard enough to be challenging but not impossibly hard. First was the Siegel conjecture that every algebraic number can be approximable by rational (p/q) with accuracy not better than q to the power two-plus-epsilon. I failed to prove it and the conjecture was later proved by Klaus Roth. Second was the Minkowski conjecture in four dimensions, which I succeeded in proving, and used as a thesis for a research fellowship at Trinity College Cambridge. I remained a life-long friend of Davenport.

I think my choice of pure mathematics for a career was mostly the result of reading *Men of Mathematics* by

Freeman Dyson giving a lecture at the Institute for Advanced Study. (Photo: Dan Komoda/Institute for Advanced Study, Princeton, NJ, USA)

Eric Bell at the age of 13. I was doubly lucky, as Bell's book was newly published in 1937, and it was given to me as a high-school prize by Winchester College. The book is a collection of mathematical biographies, bringing mathematicians to life as real people, and explaining their work with enough technical detail to bring their ideas to life.

What made you later move towards physics?
The move to physics happened when I moved to Trinity College in 1946. There I met Nicholas Kemmer, a world-class theoretical physicist who was also a dedicated teacher. He taught me most of what I needed to know to become a physicist. I saw that my nineteenth-century mathematics would be useful for practical problems in physics, while I remained ignorant of the more abstract ideas that were then dominating pure mathematics. It would be much more exciting to join the crowd exploring the mysteries of nuclear and particle physics than to remain in the small world of number theory. As a physicist I had no difficulty in finding funds to visit the United States where the particle physics revolution was already in full swing.

Was there a specific paper, book, lecture, or even a theorem you came across that had a lasting impact on you to the extent that it made you chose to become a scientist, rather than – say – a musician like your father?
The book that most influenced my choice of career was *Men of Mathematics*. My father was a composer and conductor and administrator. He became director of the Royal College of Music in 1938. He had the wisdom to see that I had no musical talent and never tried to push me into music. He always encouraged me to follow my own path in science.

You never followed a doctoral program in order to obtain a Ph.D. In this subject you also have some interesting views which are fairly divergent from the norm.
I was lucky to be educated in England at a time when the Ph.D. was not required as an entrance ticket to an academic career. I was always opposed to the Ph.D. system as it became more and more rigid in later years. It was a system designed for a small population of German students in the nineteenth century and was well suited to their needs. It is totally unsuited to the needs of a large and diverse population of students in the twenty-first century. It is especially harmful to women, who have to deal with the biological clock of child bearing while the rigid and lengthy Ph.D. system is eating up their best years. It is one of the main reasons why talented women drop out of academic careers. It is also harmful to young people of all genders who do not happen to belong to wealthy or professional-class families. It has the effect of increasing and perpetuating the inequality between rich and poor in modern societies.

Is there a mathematician who influenced you the most? Either through your mutual collaboration or interaction or even by studying his/her work? I remember you mentioning A. Besicovitch in the past as one such case, who happened to also be a close friend of yours.
The mathematician who influenced me most was Besicovitch. I was lucky to arrive at Trinity College as an undergraduate at age 17 in 1941, when there were hardly any advanced students. The old and famous mathematicians, Hardy, Littlewood, Besicovitch, lavished their time and attention on the few advanced students who were there. I quickly became a personal friend of the famous mathematicians and especially with Besicovitch, who was the owner of the billiard table. I played billiards mostly with Besicovitch, but also with Hardy. Besicovitch gave me hard mathematical problems to work on and took me with him for long walks around Cambridge, on which only Russian was spoken.

Being an analyst and analytic number theorist, I was fascinated when you first told me in the past that you actually knew G.H. Hardy rather well and had even spent time with him playing billiards at Cambridge. Would you like to share some memories from your time with him, as he is known for his particular personality.
Hardy gave wonderful lectures on function theory and analysis to a group of four students sitting around a small table. He prepared his lectures with great care, so that the discussion came to a dramatic climax just as the hour ended. He included stories about the personal lives and idiosyncrasies of the famous mathematicians that he had known. He talked fast and with a wealth of detail, so that I had to listen to every word. He spoke for three hours a week without ever repeating a lecture. He was fiercely opposed to the Tripos examination system that dominated Cambridge in those days just as the Ph.D. system does today. He tried and failed to abolish the Tripos just as I tried and failed to abolish the Ph.D.

You also think that Hardy is partly to be blamed for Ramanujan's death, if I remember well?
The story of Ramanujan's illness only became clear after his death. What is clear is that he died of amoebic hepatitis contracted in India before he came to England. Amoebic hepatitis was a well-known disease, which any doctor specialised in tropical medicine would have recognised. It was already then a curable disease with an

From left to right: Enrico Bombieri, Freeman Dyson, Dan Rockmore, Robbert Dijkgraaf. (Photo: Andrea Kane/Institute for Advanced Study, Princeton, NJ, USA)

effective chemical antidote. Hardy was responsible for Ramanujan's well-being when he became sick in England. Hardy never had him examined by a specialist in tropical medicine. The local doctors in Cambridge misdiagnosed his disease as tuberculosis and treated it with standard tuberculosis treatment, which was obviously ineffective. Hardy saw Ramanujan chronically sick for several years but never seemed to take the problem seriously. He enjoyed Ramanujan as a brilliant mind and an active collaborator, but did not care for him as a human being. That is a harsh verdict, but I think it is justified by the evidence.

On a humorous note, if – like in the case of Ramanujan – there were a supreme being that could hand you solutions to important problems in your sleep, and say that you could have only one such dream, the solution to which problem would you like to see?

I find it unattractive to have a dream giving me the solution of a deep mathematical or physical problem such as the Riemann hypothesis or the value of the fine structure constant. That would be too cheap. Nature gave us these problems as tests of our imagination, and to have them cheaply solved would be a loss of the mystery and beauty of Nature. So I would choose a historical question that deals with events that are lost in the past. Where and when did the first life appear on our planet? Where and when did the first human language emerge?

For a brief period of your life you lived in Zürich, where you also got to know W. Pauli. Would you like to say a few words about your interaction with him?

I was lucky to live in Zürich in the summer of 1951 when Pauli and I were the only two regular visitors at the ETH institute of theoretical physics. Pauli liked to go for walks after lunch and often invited me to join him. He loved to talk about all kinds of problems from physics to psychoanalysis, and I loved to listen. Among many other topics, we discussed the question whether the perturbation series expressing the interactions between particles in quantum electrodynamics are convergent or divergent. If the series converges, it proves the theory to exist as a well-defined mathematical object. If the series diverges, it proves that the theory is ill-defined and mathematically non-existent. I then believed that the series converged and Pauli believed that it diverged. As a result of our conversations, I found a simple proof that Pauli was right and I was wrong. I was profoundly grateful to Pauli for forcing me to confront the unwelcome truth.

Since Pauli was a quantum physicist, this reminded me of another topic. What are your views on the possibility of creation of quantum computers, as well as on the advent of areas such as quantum cryptography in our efforts to be protected against the possible use of quantum computers towards breaking current cryptosystems?

Quantum computers is not the right name for them. The right name is quantum subroutines. They are physical objects with quantum behaviour that processes information faster than classical objects can do. They must be connected to classical computer systems that provide input and output and interaction with human operators. The quantum subroutines are theoretically powerful and will probably be practically useful. They still need a massive engineering development before we can set limits to their capabilities. One of the important applications will be to cryptography. A quantum crypto-system will be theoretically more secure than a classical crypto-system. But that does not mean that the quantum crypto-system is more secure in the real world. In the real world, crypto-systems are usually broken by exploiting human

Freeman Dyson (left) at his office at the Institute for Advanced Study, Princeton, with Michael Th. Rassias, ca. March 2017.

errors in the day-to-day operations of the users. Human errors will probably be as prevalent in quantum systems as they are in classical systems. So long as humans are involved in the practical use of crypto, no system will be secure against hackers.

An amusing thing you mentioned to me in a past discussion of ours related to the important physicist E. Teller, whom you also knew, was that to be with Teller one had to know how to act with children. Why is that?
Edward Teller worked with me on the design of a nuclear reactor called TRIGA, which was much safer than other reactors. Teller was a brilliant scientist with an abundant supply of ideas. He was also a prima donna who threw temper tantrums like a five-year-old if anyone dared to oppose him. So our collaboration worked very well. Every day Edward would suggest a new crazy idea, I would explain why his idea would not work, and he would throw a tantrum. Then the next day that idea was forgotten and a new crazy idea was suggested. In this way we converged on a design that actually worked. The collaboration worked well because I had a lot of experience dealing with five-year-old kids at home. The reactor was a commercial success and we sold 75 of them, some of them still working sixty years later.

From all the people you have met in your life, who has astonished you the most?
As it happens, the two people who impressed me the most were both scientists, Richard Feynman and Stephen Hawking. Both were physicists. This is probably not an accident. They lived at a time when physics was attracting a large fraction of the most brilliant young people, with new experiments and theories and revolutionary discoveries rushing ahead. Now, seventy years later, physics has slowed down, while astronomy and biology have speeded up. Now I talk with astronomers and biologists more than I talk with physicists.

What is the first thing that comes to mind when you are thinking of the word "physics"?
When I think of physics today, I think of the monstrous instruments like the Large Hadron Collider which cost billions of dollars to build and can only do one experiment in ten years. I also think of fashionable theories that are never tested because they do not make verifiable predictions. If I were young today, I would not choose physics as my line of work.

One may state that mathematics has witnessed great expansion during the last, say, one hundred years, with many different areas emerging and various methods discovered, bridging seemingly different fields. How do you see the future of mathematics in that respect? Do you think that interdisciplinarity might be the theme of the future, for example?
The most beautiful feature of mathematics is its unpredictability. Progress comes in big jumps, sometimes unifying the whole subject with new ideas, sometimes diversifying the whole subject with new problems. The only thing I know for sure about the future is that the next big jump will be a surprise. I do not try to guess how it will go.

Many scientists from a broad spectrum of areas have expressed various views, opinions and even fears about the possible future consequences of the advancement of Artificial Intelligence (AI), in connection to the so-called "AI-control problem". As someone who has witnessed paradigm shifts in science which defined new eras, what are your views about the possible important advances in AI which might affect human lives altogether?
Artificial Intelligence is a huge subject and I cannot summarise the prospects for its future. The clearest view of it was published in the book *The Human Use of Human Beings*' by Norbert Wiener in 1950. Wiener showed amazing insight in his vision of the good and bad effects of AI. He predicted the failure of our society to find benefits to humanity from the good effects and remedies for the evil. Seventy years later, his verdict, that humans competing with machines will become slaves, is being proved correct. His remedies are nowhere being applied on a scale adequate to the size of the problems. I cannot do better in defining the problems than Wiener did in 1950.

An Interview with David Ruelle

Hans Henrik Rugh (Université Paris-Saclay, Orsay, France

Translation by Rafael Sasportes of the original article titled "Un interview de David Ruelle", published in La Gazette des Mathématiciens, July 2019. The permission of Hans Henrik Rugh, David Ruelle and the Société Mathématique de France is gratefully acknowledged.

David Ruelle's work covers various fields bordering on physics and mathematics. Some of his best-known results are found in his quantum field theory work on the asymptotic condition (Haag–Ruelle theory), in statistical mechanics in the works which describe "the" natural definition of equilibrium states and Gibbs states for infinite systems (DLR equations: Dobrushin–Lanford–Ruelle), in dynamical systems and turbulence in a proposition with F. Takens on the role of strange attractors to explain turbulence, in differential dynamical systems: SRB states (Sinai–Ruelle–Bowen), the notions of transfer operators and dynamical zeta functions, and also work on out of equilibrium statistical mechanics. He wrote books still considered founding references of their fields: *Statistical Mechanics, Rigorous Results* (1969) and *Thermodynamic Formalism* (1978). Among his books for the general public are *Chance and Chaos* (1991) and *The Mathematician's Brain* (2007).

Dear David Ruelle, when and how did you become interested in science?

I was very curious from an early age. But while some friends were aces at predicting football results or collected license plate numbers, I was curious about the nature of things. I identified plants using a small scientific book on botany, I did fun (and a little dangerous) chemistry experiments in the basement of my house. I also read parts of the *Positive Philosophy Course* from Auguste Comte and from the *Ethics* of Spinoza. I quickly understood that the title *Ethica Ordine Geometrico Demonstrata* was an illusion: we are a long way away from Euclid's logic. However, I have great personal sympathy for Spinoza, who earned his living by trimming optical lenses and was rejected by his Jewish community for his free thinking. For the rest, I read any scientific and mathematics books that fell into my hands.

At the beginning of your career, how did you judge the scientific environments that you encountered in different countries?

I started my university studies at an engineering school in Mons, the Belgian provincial city where I lived. The courses were, by the way, excellent. Then I continued studying physics and maths at the Free University of Brussels. I studied quantum mechanics with J. Géhéniau, who knew it well, although it was not obvious at the time. I also had time for non-university activities (in particular anti-militarist ones). From Brussels I went to Zürich to work with W. Pauli, who Géhéniau knew. Pauli died shortly after (late 1958), and I became part of a small group who had gathered around Res Jost. I have little enthusiasm for the notions of master and student in science, but I readily admit that the personality of Res Jost was decisive for my beginnings in research (into quantum field theory). Later I changed direction and benefitted a lot from my contacts with other scientists, for example by reading and rereading articles by S. Smale, R.L. Dobrushin and Ia.G. Sinai, and also by interacting with younger colleagues like Oscar Lanford, Jean-Pierre Eckmann and Giovanni Gallavotti. But it's in Zürich that I started a career as a researcher and a life outside of Belgium.

Being a foreigner in the country where you live is a situation well known to many colleagues: you cannot really be politically active and you are exposed to xenophobia by some. I lived as a foreigner in Switzerland, in the United States and in France for a quarter of a century. You get used to it: you are silent and you don't think less of it. This has undoubtedly strengthened my natural tendency to try to understand things and people rather than judging that this is good and this is bad.

At the beginning of my scientific career I saw Niels Bohr, I attended classes by Heisenberg and Pauli and I knew the latter personally. It was the end of a great period for physics. As far as I am concerned, I have become increasingly oriented towards theoretical physics problems, which are mathematical problems with a particular flavour.

Here I would like to say a few words about the changing atmosphere of scientific research. Quantitatively, there has been a huge increase in the number of researchers within a century. Qualitatively, what was above all a vocation (supported materially by teaching tasks or other sources of income) has become a profession like any other. Instead of individuals seeking to understand the nature of things, there are a host of postdocs seeking a research subject. The financial scope of research has become major, and the role of scientific administrators (often former researchers) has become dominant. The result is a new standard of research: the need to publish in prestigious journals, the obligation to study postdocs applications, etc. Unfortunately, these obligations discourage exceptional scientists, who are often the most original and the best. That said, contemporary research has yielded extraordinary results in many areas.

You have written a few popular science articles and books, often marked by a rather philosophical approach. How do you see the interaction between philosophy and science?

Galileo wrote that the great book of nature was written in mathematical language. It's very well expressed, but if we look at things four centuries later, we see them as a little more complicated. We can say that human mathematics results from the interaction of the human brain with the physical universe in which we live. An axiomatic presentation of mathematics (Zermelo–Fraenkel–Choice) eliminates the physical universe and at the same time the human brain. It should also be noted that understanding the physical universe requires only a part of mathematics based on ZFC. My colleague Giovanni Gallavotti believes that physics can do without the Axiom of Choice (this does not prevent the fact that the inclusion of the Axiom of Choice makes the presentation of mathematics much more natural). In fact, when we work to rewrite the great book of nature in mathematical language, we are led to natural mathematical choices different from those of the usual mathematics based on ZFC. This is not a new thing: the beginnings of geometry (based on the observation of the physical world) imposed the primacy of the real numbers field over other fields.

If we want to understand the nature of things, it seems that we have to start with the study of philosophy. But if we look at the situation more closely, we see that philosophy breaks up in a multitude of doctrines which bring no certainty. The near certainties we have come from maths and science. It should be added that these are quasi-certainties on a human level at a period close to the year 2000, and that the expression of these quasi-certainties is largely based on the use of natural languages such as English and French. It should also be noted that in science and in the practice of mathematics, as in this discussion, the use of natural languages is poorly formalised.

I do not despise philosophy and I have read the dialogues of Plato with pleasure. I am very aware of the evolution of human thought that has led to our current understanding of the nature of things.

To what extent does what we know of the nature of things depend on the human nature of our intelligence? The problem is most affordable in mathematics, which can be formally formulated without resorting to natural languages.

Another question is to know what it is in the personal philosophy of the builders of science that guides them towards their discoveries.

The interaction between mathematics and physics obviously plays an important role in your work. How do you see the structure of mathematics and its use in the description of natural sciences?

Mathematics can be formalised using the Zermelo–Fraenkel–Choice axioms, which de facto form the basis of current mathematics. We can organise known human results within the framework of the "fundamental structures of analysis" as N. Bourbaki does. But this structuring is far from the ZFC axioms. Other structures use categories, morphisms and functors, etc. Is there a natural structure of mathematics?

Part of the answer could be provided by computers. There are already very reliable *formal computer proofs*. These computer proofs are logically long, but their accuracy depends on a logical kernel which is a carefully checked short program. If we admit that the basic axioms of mathematics are non-contradictory, formal computer proofs are much more reliable than traditional human proofs. What computers lack is creativity: guessing new results and guessing a way to prove them. Some believe that the creative power of the human brain can never be replaced by "a machine" (a computer). But this belief has no serious scientific basis. In short, it is possible that a natural structure of mathematics could emerge from computer-created mathematics, but that is by no means certain. For now we only know human mathematics.

However, human mathematics is partly guided by our efforts to interpret the physical world around us. My personal research work falls within this framework, that of mathematical physics. As it currently exists, mathematical physics includes quite diverse things, such as string theory, whose relationship with the physical world is not guaranteed. My interests have mainly focused on statistical physics, which is the study of material systems with a large number of particles, such as liquids and gases. It turns out that we can define so-called *equilibrium* states for these systems, characterised by variables such as temperature, entropy, etc. Ludwig Boltzmann (with Maxwell, Gibbs and others) understood what an equilibrium state is: it is a specific probability measure over a space with large dimension. This measure corresponds to a given interaction between the particles of the system.

We will not try to summarise the theory of equilibrium states (statistical mechanics of equilibrium) here. Let's just say it is a mathematically difficult but natural theory, it introduces important mathematical concepts like entropy, and there are still poorly understood phenomena like phase transitions. An important notion that I have studied (with R.L. Dobrushin and O. Lanford) is that of *Gibbs state*.

Let's move on to a mathematical problem unrelated to the statistical mechanics of equilibrium: hyperbolic differentiable dynamical systems. For these systems, Ia.G. Sinai has constructed what he calls *Markov partitions* which allow an application of the methods of statistical equilibrium mechanics. It turns out that Gibbs states are a wonderful tool for an in-depth study of the theory of (uniformly) hyperbolic systems. Hyperbolic dynamical systems appear in the study of hydrodynamic turbulence (D. Ruelle and F. Takens). We thus see that there is a purely mathematical link (via Gibbs states) between two very different physical problems: the statistical mechanics of equilibrium and hydrodynamic turbulence. How is that possible?

In my opinion, the study of mathematical physics leads to the introduction of fruitful mathematical concepts, like entropy or Gibbs states. These concepts would be much more difficult to find in a Bourbaki-style mathematical approach based on the analysis of structures. There is here an element to answering the question: is there a natural structure of mathematics?

In the area of dynamical systems, part of the terminology has been imported from statistical mechanics. What is the explanation for this?

I had to work on both sides of the border between physics and mathematics. I will not list these works here. But it turns out that I contributed to the terminology of differentiable dynamical systems. For instance, I introduced the term "thermodynamic formalism" – this is the title of a book I published in 1978. I also introduced the term "pressure" for a function that appears in ergodic theory; frankly the proper term in statistical mechanics should be "free energy", but the word pressure seemed more acceptable to mathematicians. I should also mention the expression "strange attractor", which has been very successful and seems to have appeared for the first time in an article published by Floris Takens and myself in 1971. The intention of the article was to clarify a small mathematical point concerning hydrodynamic turbulence. I thought the article would go unnoticed and be immediately forgotten, instead of which it has been cited to date 3874 times. Vanitas vanitatum!

One question I have worked on is that of SRB states for differentiable dynamical systems. The initials SRB correspond to Sinai, Ruelle, and Bowen, but one should also add F. Ledrappier, J.M. Strelcyn, L.-S. Young and a few others. My interaction with Sinai and Bowen was a great source of job satisfaction for me: everyone just wanted to understand a problem, not to show that he was superior to his colleagues. Yasha Sinai was a great force in Russian mathematics. As for Rufus Bowen, who died at 31, his clarity of mind was extraordinary, and a difficult problem suddenly became simple when he explained it. I also had a lot of fun at the IHÉS interacting with Viviane Baladi and Hans Henrik Rugh on issues of differentiable dynamics.

You have been a member of several academies for a good number of years. What do you think of the role of academies and their function of scientific assessment?

For science to progress, the value of scientific work must be constantly assessed. This assessment takes several forms: selection of articles in peer-reviewed scientific journals, scientific honours, etc. Any form of assessment has an element of power, and power corrupts. It is therefore desirable that this power is not absolute, and that there is a balance of these assessment powers. At the moment, it seems to me that there is a problem in the growing role of professional scientific administrators, and also in the biased or incompetent attribution of certain great scientific prizes. Any power of scientific assessment can be criticised, it is the case of scientific honours like the election to an academy. As much as the way academies work deserves to be discussed, the abolition of these would only encourage other instances of power, without this benefitting science.

Personally, I am a member of several academies, including the Paris Academy of Sciences, where I play a modest role. It is clear in my mind that slightly different circumstances could have led to me not becoming an academy member. That said, the greatest benefit I have derived from the academy is to have rubbed shoulders with a generation of great mathematicians: H. Cartan, J. Leray, J.-P. Serre, L. Schwartz, J. Dieudonné, R. Thom, J. Tits, G. Choquet and others.

Who are the most memorable scientific minds in your career?

During my military service as a private in the Belgian army, I was in a room with two illiterates: one had never learned to read, the other had forgotten how to. It was an intellectually disadvantaged environment. However, I met other privates there who were remarkable men. In a military environment, one of whose mission was to break personalities, these men, either by courage, trickery or cheating, did not break. In my scientific career too, I have met remarkable individuals. Often when I have to make a decision, I think of this or that person, and I wonder what he or she would have done in this situation. Important scientists are not necessarily remarkable people in my opinion. Many are specialists with limited intellectual ambitions, such as becoming a head mathematician. Grothendieck, on the other hand, said: I am a generalist, not a specialist.

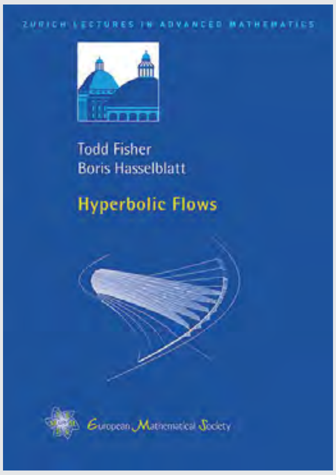
Alexandre Grothendieck had an extraordinary personality. He wrote a *praise for incest*. His relationships with the women who shared his life could be extremely tense. He was firmly anti-militarist and had anarchist tastes. Mathematics played a central role in his life at certain times, meditation and religion at other times. I was around Grothendieck for several years and I was fascinated by the way he worked, including his changes in orientation. He faced general human problems in an original way. You can follow or not follow his choices, but when I have to make a decision I often wonder what Grothendieck would have done in my place.

As rich as Grothendieck's life seems to me, including its contradictions, the corrected version that is often made of it now seems false and lacklustre. Grothendieck would be a chief mathematician with politically correct ideas (by today's standards) and a few errors that must be excused because he was a genius.

Remarkable scientific minds have very diverse intellectual personalities, and it is this diversity that allows them new approaches to scientific problems. But it seems to me that remarkable scientific minds are often guided by the search for a general view of the nature of things and the universe in which we live. This was certainly the case with Newton, who, in addition to his contributions to mathematics and physics, devoted great efforts to alchemy and theology. Spinoza, Newton or Grothendieck's efforts to understand the nature of things have sometimes led to remarkable discoveries, sometimes not. During conversations with Murray Gell-Mann I was impressed by his knowledge of languages and biology, here was someone who sought a general understanding of the nature of things, and not just of one area of physics. These examples show that trying to guide research by administrative standards can only impoverish our knowledge of the world.

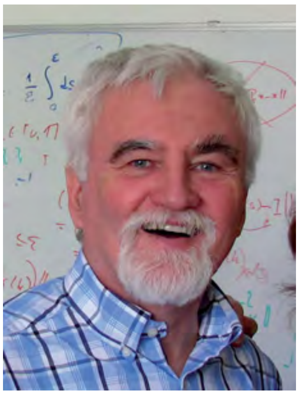
My curiosity about the nature of things has never been limited to my professional scientific work. Among other things, I have spent time hiking, alone or with my wife, in remote corners of Mexico, Bolivia, or elsewhere. In the scientific field I have had the satisfaction of gaining a certain understanding of scientific fields such as the statistical mechanics of equilibrium or the theory of chaos, or of clarifying small questions like the lemma of Asano–Ruelle (concerning the zeros of complex quadratic polynomials with two variables). I have admired the mathematical way in which minds like those of Bowen and Sinai work. I have also been able to see remarkable spirits acting in ordinary life, such as Mark Kac full of humour, Joel Lebowitz always generous, or J. Robert Oppenheimer colder and for whom I had less sympathy. But sympathy or not, the different ways in which great scientific minds work have always fascinated me.

Hans H. Rugh wrote his PhD thesis in Copenhagen, Denmark, under the supervision of Predrag Cvitanović. He has since held full-time positions in Warwick, England, as well as in Cergy-Pontoise, France. At present he is professor at the University of Paris-Saclay, at the Mathematics Institute at Orsay.


Zürich Lectures in Advanced Mathematics
Todd Fisher
Boris Hasselblatt
Hyperbolic Flows
European Mathematical Society

Hagen Neidhardt (1950–2019) – His Work and Legacy

Jussi Behrndt (TU Graz, Austria), Pavel Exner (Doppler Institute, Prague, Czechia), Takashi Ichinose (Kanazawa University, Japan), Mark M. Malamud (People's Friendship University of Russia, Moscow, Russia) and Valentin A. Zagrebnov (Institut de Mathématiques de Marseille, France)



Our friend and co-author, brilliant mathematician Hagen Neidhardt, passed away on 23 March 2019 at the age of 68. Author of more than 150 research papers, Hagen was a world-renowned expert in the areas of functional analysis, operator theory and mathematical physics, where he made a number of highly original contributions.

Hagen Ernst Neidhardt was born on 20 November 1950 in the provincial town of Gefell (Thuringia) in the German Democratic Republic (GDR). His father, Hubertus Neidhardt, was director at the Engineering School for Textile Technology, Reichenbach/Vogtland. His mother Ruth Neidhardt (née Löffler) was a clerk at Vogtlandstoffe VEB Kombinat Wool and Silk Meerane.

Hagen was passionate about mathematics from a very young age. On one occasion he came across a mathematics enyclopedia his parents had been planning to give him as a Christmas present that year, and by the time Christmas came around, it was clear to his parents that he had already worked through the entire book. His whole life beat to the rhythm of mathematics.

School, University, Karl Weierstraß Institute

Neidhardt's special talent and inclination towards mathematics were recognized early on by parents and teachers. Hagen attended a local primary school in Gefell from 1957 to 1967, after which he moved on to advanced high schools in Schleiz and Reichenbach (Vogtland).

At only 17 years of age, Hagen left his childhood home for good. In 1967, he moved to the Faculty of Workers and Peasants (ABF) at Martin Luther University Halle-Wittenberg for two years preparation for studying in the Soviet Union. The Institute for Preparation for Studying Abroad in Halle (Saale) prepared delegated students from all over the GDR for studying abroad. Hagen was preparing for his studies in the USSR at the Leningrad State University (LSU).

Six years later, on 28 February 1975, Hagen graduated with distinction from the Faculty of Physics of the LSU and was awarded the diploma in mathematical physics. His tutor and promotor of his diploma thesis on the *scattering theory* was Professor Mikhail Shlemovich Birman.

Hagen Neidhardt, Dubna (1989)

This background and his time with Professor Birman, who was then the head of the Leningrad Mathematical Physics Seminar, were decisive for the mathematical orientation of the young Hagen Neidhardt. This became the spectral theory of operators and, in particular, the scattering theory, which were the main topics of the seminar at that time, with participation of Ludwig D. Faddeev, Olga A. Ladyzhenskaya and Boris S. Pavlov.

Almost immediately after his return to the GDR, on 4 March 1975, Hagen took up a junior position in the Karl Weierstraß Institute of Mathematics in Berlin. There he wrote his first research paper in 1976: "Zwei-Raum-Verallgemeinerung des Theorems von Rosenblum und Kato" on spectral analysis of the scattering theory, motivated by one of Birman's publications. This paper appeared in *Mathematische Nachrichten* 84(1978) 195–211 and signified one of the preferred directions of Hagen's scientific interests. He returned to this question in the paper "A nuclear dissipative scattering theory" (*J. Operator Theory* 1985), and then in "A Converse of the Kato-Rosenblum Theorem" in the same journal (1991). The last paper, where he revisited this problem, was published in 2017.

In the meantime, Hagen started to work on his Ph.D. thesis. His supervisor was Professor Hellmut Baumgärtel, a leading expert in the mathematical scattering theory. Although this topic offered enough scope to be worth continuing, Hagen was attracted to another project related to the solution of the non-autonomous Cauchy problem with the help of extension to evolution semigroups. This method was advocated by Howland (1974) and Evans (1976). In "Integration von Evolutionsgleichungen mit Hilfe von Evolutionshalbgruppen" (Dissertation, AdW der DDR, Berlin 1979, defended on 5 April 1979) Hagen generalised this approach to an arbitrary Banach space. The main result, published in "On abstract linear evolution equations. I" (*Mathematische Nachrichten* 1981), proved the one-to-one correspondence between a set of evolution semigroups and strongly continuous solution operators (propagators) for non-autonomous Cauchy problem. The Howland–

Evans–Neidhardt approach is now well known for both parabolic and hyperbolic cases. They were scrutinised by Hagen in two papers, "On abstract linear evolution equations. II" and "III" in 1981–82. He returned to the elucidation of the difficult hyperbolic case versus Schrödinger evolution in "Linear non-autonomous Cauchy problems and evolution semigroups" (*Adv. Diff. Equations* 2009). Hagen liked the evolution semigroups approach to the non-autonomous Cauchy problem and returned to applications of this method many times, in particular, in the framework of product formula approximations for propagators. One of the very last of his papers on this subject: "Convergence rate estimates for Trotter product approximations of solution operators for non-autonomous Cauchy problems" appeared only recently in *Publ. RIMS Kyoto Univ*. 2020.

Joint Institute for Nuclear Research, Dubna

A new chapter in Hagen's scientific evolution opened in the second half of the eighties, when he arrived with his family for a scientific visit (15 September 1986–14 September 1990) to the Joint Institute for Nuclear Research (JINR) in Dubna, USSR. There he first returned to the "spectral shift" problem that was studied in Leningrad by L.S. Koplienko, one of Birman's students. Note that this problem can be traced back to M.G. Krein (1953, 1962), who introduced the terms "spectral shift function" and "trace formula". Let $\{H, H_0\}$ be a pair of self-adjoint operators on a separable Hilbert space $\mathfrak{h}$ which differ by a nuclear operator. M.G. Krein has proved the existence of a summable real function $\xi(\cdot)$ defined on $\mathbb{R}^1$ such that for a certain class of functions $\psi(\cdot)$ the relation

$$\operatorname{Tr}(\psi(H) - \psi(H_0)) = \int_{\mathbb{R}^1} d\lambda\, \xi(\lambda)\, \partial_\lambda \psi(\lambda)$$

holds. The function $\xi(\cdot)$ is called the *spectral shift function* of the pair $\{H, H_0\}$ and the relation itself, the *trace formula*. In his paper "Spectral Shift Function and Hilbert-Schmidt Perturbation: Extensions of Some Work of L.S. Koplienko" (*Mathematische Nachrichten* 138(1):7–25, 1988), Hagen made an important step forward in this problem. Then, in 1987–1990, he generalised the trace formula for non-unitary and non-self-adjoint operators and showed that a summable real spectral shift function can be introduced for a pair of contractions, or dissipative operators, such that the trace formula holds if they differ by an operator which is *slightly* more compact than a trace class operator.

These results constituted a part of Hagen's dissertation of *Doctor scientiarum naturalium* awarded on 30 June 1987 by the Akademie der Wissenschaften der DDR. The formula proved by him is now known as the *Koplienko–Neidhardt Trace Formula*.

Hagen Neidhardt was very friendly with colleagues and always open to new ideas. In the Laboratory of Theoretical Physics of JINR, he was a member of the Mathematical Physics Group headed by Werner Timmermann and then by Pavel Exner. The problems discussed at the group seminar inspired Hagen to new projects.

Pavel Exner and Hagen Neidhardt, Kanazawa (2010).

One of these was motivated by the question from quantum statistical mechanics and brought a new object to his attention: the Gibbs semigroup, i.e., strongly continuous semigroups $\{e^{-tA}\}_{t\geq 0}$ with values in the *-ideal of trace-class operators $\mathcal{C}_1(\mathfrak{h})$ on a separable Hilbert space $\mathfrak{h}$ for $t>0$. The question was whether the well-known strongly convergent *Trotter product formula*

$$\lim_{n\to\infty} \left(e^{-tA/n} e^{-tB/n}\right)^n = e^{-tH}, \qquad t > 0,$$

converges in the *trace-norm* topology to semigroup with some generator H if B is generator of a strongly continuous semigroups. In the paper "The Trotter–Kato product formula for Gibbs semigroups" with V. Zagrebnov (*Commun. Math. Phys*. 1990) this question was answered affirmatively in a general framework of non-exponential Kato functions.

This paper triggered an important long-term research project on the *product formulae* approximations in the trace-norm and the operator-norm topologies for semigroups, unitary groups and for propagators that involved Hagen Neidhardt and his co-authors P. Exner, T. Ichinose and V. Zagrebnov.

In addition to his research work, Hagen actively participated in the life of the community concentrated

Valentin Zagrebnov, Hagen Neidhardt and Jürgen Voigt, QMath7, Prague (1998).

around the mathematical physics group of the Laboratory of Theoretical Physics. He attended conferences that were the beginning of what was later known as the "Mathematical Results in Quantum Physics" (or QMath) series, and helped to organise the third one in 1989, dedicated to the memory of M.G. Krein. He also co-edited this proceedings conference volume of QMath3, which appeared under the title *Order, Disorder and Chaos in Quantum Systems* as Volume 46 in the Birkhäuser series "Operator Theory: Advances and Applications" (Basel 1990).

Back to Berlin

In September 1990, Hagen returned with his family to Berlin. It was not an easy time for them. One of the results of the German "reunification" was the demise of the Karl Weierstraß Institute of Mathematics, with all of its employees having been made redundant. For two years in 1992–1993 he worked at the Technical University of Berlin, and from the 1st of January 1994 to 31 December 1999 he was a research associate at the University of Potsdam. These difficulties neither discouraged him, nor did they reduce his enthusiasm for doing mathematics.

At that time he often visited the Mediterranean University of Marseille-Luminy to continue the collaboration with V. Zagrebnov on the Trotter–Kato product formula and operator-norm convergence. They also started a new project on singular perturbations, regularisation and extension theory; let us quote a few principal papers in this connection: "Towards the right Hamiltonian for singular perturbations via regularization and extension theory" (1996), "Does each symmetric operator have a stability domain?"(1998), "On semibounded restrictions of self-adjoint operators"(1998). These results motivated an important article with P. Exner and V. Zagrebnov, "Potential approximations to δ': an inverse Klauder phenomenon with norm-resolvent convergence"(2001).

During the nineties, Hagen also collaborated closely with J. Brasche on Krein's extension theory and singularly continuous spectrum of self-adjoint extensions, as well as on the inverse spectral theory for self-adjoint extensions. Once more, the research did not consume all of his energy. During his stay at Potsdam University he organised, in collaboration with M. Demuth, P. Exner and V. Zagrebnov, the fifth issue of the QMath conference series in Blossin in the Berlin suburbs, effectively giving the series a new lease of life; he also co-edited the conference proceeds appearing as Volume 70 of the indicated Birkhäuser edition.

Back to the Weierstraß Institute

In January 2000 Hagen Neidhardt succeeded in returning to his mathematical *alma mater*, reborn under the name Weierstraß Institute for Applied Analysis and Stochastic (WIAS). As usual, he was full of plans and enthusiasm.

The Trotter–Kato product formulae activity for semigroups progressed successfully in collaboration with Valentin Zagrebnov, leading to the operator-norm convergence with the rate estimate subsequently extended to symmetrically-normed ideals, and with T. Ichinose, V. Zagrebnov to fractional conditions, "Trotter–Kato product formula and fractional powers of self-adjoint generators" (*J. Funct. Anal.* 2004). A few interesting results together with P. Exner, T. Ichinose and V. Zagrebnov were also established for the unitary case in "Zeno product formula revisited" (*Integral Equations and Operator Theory* 2007) and in "Remarks on the Trotter–Kato product formula for unitary groups" (Integral Equations and Operator Theory 2011).

Shigetoshi Kuroda and Hagen Neidhardt, Prague (2006)

During one of his visits to Marseille-Luminy, Hagen came across the activity concerning the non-equilibrium steady states (NESS) in quantum many-body systems, popular there at that time. He quickly realised that there was room here for the application of his expertise in the scattering theory. This was the beginning of his fruitful collaboration with J. Rehberg, H. Kaiser and M. Baro, see e.g.: "Macroscopic current induced boundary conditions for Schrödinger-type operators" (*Integral Equ. Oper. Theory* 2003), "Dissipative Schrödinger–Poisson systems" (*J. Math. Phys.* 2004), "A quantum transmitting Schrödinger–Poisson system" (*Rev. Math. Phys*. 2004) and "Classical solutions of drift–diffusion equations for semiconductor devices: The two-dimensional case" (*Nonlinear Analysis* 2009).

At the same time, Hagen never ceased to pay attention to the "purely" mathematical aspect of the NESS and its possible applications, as seen in the papers (with H. Cornean and V. Zagrebnov) "The effect of time-dependent coupling on non-equilibrium steady states" (*Annales Henri Poincaré* 2009), "The Cayley transform applied to non-interacting quantum transport" (*J. Funct. Anal.* 2014) and "A new model for quantum dot light emitting-absorbing devices: proofs and supplements" (*Nanosystems* 2015).

Note that the last two papers were part of the thesis of his Ph.D. student Lukas Wilhelm (WIAS Berlin).

A similar inclination was shown by Hagen in the papers "Non-equilibrium current via geometric scatterers" (*J. of Phys. A* 2014) with P. Exner, M. Tater and V. Zagrebnov and "A model of electron transport through a boson cavity" (*Nanosystems* 2018) with A. Boitsev, J. Brasche and I. Popov. The mathematical background of this model was developed within Hagen's important project on *boundary triplet* technique in the paper "Boundary triplets, tensor products and point contacts to reservoirs" (*Annales Henri Poincaré* 2018) by the same authors including M. Malamud. There the boundary triplet technique was employed. In this paper, a model of electron transport through a quantum dot assisted by a cavity of photons is proposed. In this model, the boundary operator is chosen to be the well-known Jaynes–Cummings operator which is regarded as the Hamiltonian of the quantum dot.

The beginning of the collaboration between Hagen and Mark Malamud dates back to the end of the nineties. Originally it was influenced by Hagen's interest in extensions of a symmetric operator with a gap and his joint results with S. Albeverio and J. Brasche. This collaboration started with an attempt to apply the technique of boundary triplets and the corresponding Weyl functions to the problem of existence (and description) of self-adjoint extensions with prescribed spectrum within a gap. Their result, obtained together with S. Albeverio and J. Brasche, was published in "Inverse spectral theory for symmetric operators with several gaps: scalar type Weyl functions" (*J. Funct. Anal*. 2005).

Mark Malamud and Hagen Neidhardt, Prague (2009)

Later on, Hagen (together with J. Behrndt and M. Malamud) applied the Weyl function technique to investigating scattering matrices of two resolvent comparable self-adjoint operators, i.e., operators with a trace-class resolvent difference. In this direction they published two papers "Scattering matrices and Weyl functions" (*Proc. Lond. Math. Soc.* 2008) and "Scattering matrices and Dirichlet-to-Neumann maps" (*J. Funct. Anal.* 2017). There the scattering matrix of two resolvent comparable self-adjoint extensions of a symmetric (not necessarily densely defined) operator with equal deficiency indices has been expressed by means of the limit values of the Weyl function on the real axis and a boundary operator. The abstract result was then applied to various different realisations of the Schrödinger operator, where the Weyl function is closely related to the classical Dirichlet-to-Neumann map.

In 2007 the assertion of the first paper for the scattering matrix was generalised to the case of a pair of self-adjoint and maximal dissipative extensions of a symmetric operator with finite deficiency indices in "Scattering theory for open quantum systems with finite rank coupling" (*Math. Phys. Anal. Geom.* 2007).

Using the formula for the scattering matrix, the authors recovered a connection, first discovered by V.M. Adamyan and D.Z. Arov, between the Lax–Phillips scattering matrix and the characteristic function of the maximal dissipative operator. Moreover, it was shown there that the Lax–Phillips scattering matrix coincides with the lower diagonal entry of the scattering matrix of the pair of two self-adjoint extensions, with one of them being a minimal self-adjoint dilation of the dissipative operator under consideration.

Let us next mention another of Hagen's joint papers with M. Malamud, "Perturbation determinants for singular perturbations" (*Russian J. of Math. Phys*. 2014). Here the boundary triplets technique was applied to perturbation determinants (PD) for pairs of resolvent comparable operators. Treating both operators as proper extensions of a certain symmetric (not necessarily densely defined) operator and choosing a boundary triplet, a PD is expressed via the Weyl function and boundary operators. In applications, it allows one to express a PD of two boundary value problems (BVPs) directly in terms of boundary conditions and the Weyl function. In particular, a PD for two BVPs for Schrödinger operators in a domain with smooth compact boundary via the Dirichlet-to-Neumann map is explicitly computed.

Finally, the series of Hagen's publications in collaboration with M. Malamud and V. Peller deserve a mention: "Trace formulas for additive and non-additive perturbations" (*Advances in Math.* 2015), "Analytic operator Lipschitz functions in the disc and trace formulas for functions of contractions" (*Func. Anal. and Appl.* 2017), and "Absolute continuity of spectral shift" (*J.Funct.Analysis* 2019).

As is clear from their titles, the papers are devoted to the Krein-type trace formulae for pairs of resolvent comparable operators. Here Hagen returned to the subject of his Dr.Sc. dissertation (1987). In particular, it was shown that a pair of contractions (maximal dissipative operators) admits a (non-unique) complex valued summable spectral shift function (SSF), i.e. their resolvent difference outside the unit disc admits a Krein-type representation. Besides, the SSF can be selected to have non-negative (or non-positive) imaginary part whenever the first (second) operator is unitary. A particular case of the later result, where the resolvent difference belongs to the ideal which is slightly narrower than the trace class one and defect operators are of the trace class, was analysed by Hagen (jointly with V.M. Adamyan) in "On the summability of the spectral shift function for pair of contractions and dissipative operators" (*J. Oper. Theory* 1990) .

In the two last papers it was also shown that the maximal class of functions for which the Krein-type trace formula holds is the class of the operator Lipschitz functions, which are analytic in the unit disc.

Note that the problem of description of the maximal class of functions for which the trace formula holds for any pair of self-adjoint operators with trace class dif-

Takashi Ichinose, Hagen Neidhardt, Valentin Zagrebnov, Prague (2009).

ference was posed by M.G. Krein in 1964, and was then solved by V. Peller in 2016. Thus Hagen, jointly with M. Malamud and V. Peller, obtained a solution of the version of the M.G. Krein problem for pairs of contractions (maximal dissipative operators).

Note that Hagen constructed the first example of a pair of contractions which does not admit a real valued locally summable SSF in the paper: "Scattering matrix and spectral shift of the nuclear dissipative scattering theory" (*Operators in indefinite metric spaces, scattering theory and other topics*, Birkhäuser Verlag, Basel 1987). Conversely, in the last paper of the series (*J. Funct. Analysis* 2019) it was proved that a real valued SSF, which is A-integrable (in the sense of A.N. Kolmogorov), always exists.

Note also that in *J. Funct. Analysis* 2019 the authors solved in passing M.S. Birman problem: to find a proof of absolute continuity of a spectral shift measure relied on the theory of double operator integrals. Birman's interest has been inspired by his (joint with M.Solomyak) approach to SSF. The authors' proof is based on S. Nagy-Foias result on ac-continuity of the spectral measure of a minimal unitary dilation of a simple contraction.

Hagen's role as a QMath conference co-organiser was not exhausted by the two events mentioned above. In 2012 he came to rescue when the original plan ran into trouble, and it was his work which made the meeting at the Humboldt University in Berlin possible. As in the previous cases, he co-edited the proceedings volume of QMath12, which was published this time by World Scientific in 2014.

Another of Hagen's projects starting in the same year was the book *Trotter–Kato product formulae*. It was planned for the Springer Lecture Notes in Mathematics series and is actually still in progress.

Farewell in 2016

After his retirement from WIAS in 2016, Hagen was still active and kept a "corner" at the institute to host his visitors and collaborators. With his student Artur Stephan and V. Zagrebnov, Hagen returned to the *evolution semigroup* approach to the construction of *solution operator* (propagator) for the non-autonomous Cauchy problem in Hilbert and Banach spaces. In fact, this idea goes back to his Ph.D. thesis from 1979 about the Howland–Evans–Neidhardt approach to the solution of abstract non-autonomous Cauchy problems. A new aspect was to use the full power of the Trotter product formula approximations for evolution semigroups and their one-to-one correspondence with propagators to produce product formula approximations for the latter.

The one-to-one correspondence allowed control over the rate of convergence of approximants for propagator: "Convergence rate estimates for Trotter product approximations of solution operators for non-autonomous Cauchy problems" (first in archive: arXiv:1612.06147 (2016) and finally in the *Publications of Research Institute for Mathematical Sciences, Kyoto* 2020).

The main results appeared in the series of papers "On convergence rate estimates for approximations of solution operators for linear non-autonomous evolution equations" (*Nanosystems: mathematics* 2017), "Remarks on the operator-norm convergence of the Trotter product formula" (*Integral Equations and Operator Theory* 2018), "Trotter Product Formula and Linear Evolution Equations on Hilbert Spaces" (*Analysis and Operator Theory*, vol.146, 2019).

Beyond Mathematics

Hagen was an extraordinary person.

He loved mathematics as his first priority. When visiting any new place on earth for scientific collaboration, he did not seem all that interested in taking time out to do sightseeing, etc.; what he wanted to do was mathematics. So the colleague who had invited him would have to preach at him to take a break and do something else, otherwise he would just keep sitting in front of his PC and doing mathematics for the duration of his visit.

Second, he loved Nature: he loved hiking, he loved mountains, preferably as high as possible. He enjoyed setting himself a challenge, be it fitness training, mountaineering, or swimming through a dam or very far from the coast of the Mediterranean Sea in Marseille.

Hagen read several daily newspapers every day, and he declared: "A high level of general education is to be inter-

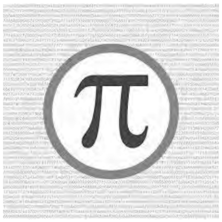
Hagen Neidhardt in Kanazawa (2010).

ested in politics and sports, but also in the small things of everyday life." Hagen had an extraordinary memory for time – for example, he had absolutely no problem recalling key sporting events and the winners. He also liked to watch live football matches at the Berlin stadium.

Hagen was rational and objective, but he could be very funny as well. He had the knack of being able to reverse the mood in "unpleasant" situations by his good, amusing comments, but he could also become emotional and philosophical. He was impressed by the way that time progresses. Hagen enjoyed music, for example classical music by Tchaikovsky, but also modern interpreters such as ABBA. He loved space and everything about space travel and technology; sometimes he had tears in his eyes while watching a rocket launch. But he also found joy in the simple things like the view from the terrace into the greenery. Hagen was a family man. When Hagen and Hiltrud celebrated their silver wedding anniversary, he declared: "Dear Hille, I love you more than my mathematics." Hagen loved his children and always stood by them with support and advice, without ever making empty promises. He very much admired his first granddaughter Sophie. He had started teaching her the digits of π.

Now you can see π on the gravestone of Hagen Neidhardt (20.11.1950–23.03.2019) in the Städtische Friedhof Pankow-Buch.

We are greatly privileged to have been friends and collaborators of Hagen. We miss him so much.



Heritage of European Mathematics

Gösta Mittag-Leffler and Vito Volterra 40 Years of Correspondence

Edited by Frédéric Jaëck Laurent Mazliak Emma Sallent Del Colombo Rossana Tazzioli

European Mathematical Society

The Mathematics of Bitcoin

Cyril Grunspan (De Vinci Research Center, Pôle Léonard de Vinci, Courbevoie, France) and Ricardo Pérez-Marco (CNRS, IMJ-PRG, Sorbonne Université, Paris, France)

1 Introduction to Bitcoin

Bitcoin is a new decentralised payment network that started operating in January 2009. This new technology was created by a pseudonymous author, or group of authors, called Satoshi Nakamoto, in an article that was publically released [1] in the cypherpunk mailing list. The cypherpunks are anarchists and cryptographers who have been concerned with personal privacy in the Internet since the 90s. This article follows on from a general presentation of Bitcoin by the second author [2]. We refer to this previous article for general background. Here we focus on mathematics being a feature of the security and effectiveness of Bitcoin protocol.

Roughly speaking, the Bitcoin's protocol is a mathematical algorithm on a network which manages transaction data and builds majority consensus among the participants. Thus, if a majority of the participants are honest, then we get an honest *automatic* consensus. Its main feature is *decentralisation*, which means that no organisation or central structure is in charge. The nodes of the network are voluntary participants that enjoy equal rights and obligations. The network is open and anyone can participate. Once launched, the network is resilient and unstoppable. It has been functioning permanently without significant interruption since January 2009.

The code and development are open. The same code has been reused and modified to create hundreds of other cryptocurrencies based on the same principles. The security of the network relies on strong cryptography (several orders of magnitude stronger than the cryptography used in classical financial services). For example, classical hash functions (SHA256, RIPEMD-160) and elliptic curve digital signatures algorithm (ECDSA) are employed. The cryptography used is very standard and well known, so we will not dwell on the mathematics of these cryptographic tools, but interesting cryptographical research is motivated by the special features of other cryptocurrencies.

Nodes and mining

The bitcoin network is composed of nodes that correspond to the bitcoin program running on different machines and communicate with their neighbours. Properly formatted bitcoin transactions flood the network, and are checked, broadcasted and validated continuously by the nodes which follow a precise set of rules. There is no way to force the nodes to follow these rules. Incentives are created so that any divergence from the rules is economically penalised, thus creating a virtuous cycle. In this way, the network is a complex dynamical system and it is far from obvious that is is stable. The stability of this system is a very interesting and fundamental mathematical problem. In this study, we will encounter special functions, martingale theory, Markov chains, Dyck words, etc.

Figure 1. The bitcoin logo

Nodes in the network broadcast transactions and can participate in their validation. The process of validating transactions is also called "mining" because it is related to the production of new bitcoins. The intuition behind bitcoin is that of a sort of "electronic gold", and the rate of production of bitcoins is implemented in the protocol rules. On average, every 10 minutes a block of transactions is validated and new bitcoins are minted in a special transaction without bitcoin input, called the coinbase transaction. At the beginning, 50 ₿ were created in each block, and about every 4 years (more precisely, every 210.000 blocks), the production is divided by 2. This event is called a "halving". So far, we have had two halvings, and the production is currently of 12.5 ₿ per 10 minutes, or 1.800 ₿ per day. The next halving will occur in April–May 2020. This geometric decrease of the production limits the total amount of bitcoins to 21 million. Currently, about 18 million have already been created. Each block containing the validated transactions can contain about 3 to 4 thousand transactions and has a size of about 1 Mb. These blocks are linked together cryptographically, and the set of all these blocks forms the "blockchain" that contains the full history of bitcoin transactions. This data is stored efficiently, and the current blockchain is only about 260.000 Mb. The cryptographical link between blocks is provided by the mining/validation procedure that is based on a hash function and a "Proof of Work". It costs computation power to validate a block and this is what ensures that the data cannot be tampered with or corrupted. In order to modify a single bit of a block, we must redo all computations that have been used to build all the subsequent blocks until the last current one. Currently the computation power needed to change the last few blocks of the more than 600 thousand composing the blockchain is beyond the capabilities of any state or company.

The mining/validation procedure is a sort of decentralised lottery. A miner (this is a node engaging in validating transactions) packs together a block of floating, not yet validated transactions, and builds a header of this block that contains a hash of the previous block header. The hash algorithm used is SHA-256 (iterated twice), that outputs 256 bits. Mathematically, a hash function is a deterministic one way function: it is easy to compute, but practically impossible to find pre-images or collisions (two files giving the same output). It also enjoys pseudo-random properties, that is, if we change a bit of the input, the bits of the output behave as uncorrelated random variables taking the values 0 and 1 with equal probabilities. The mining procedure consists of finding a hash that is below a pre-fixed threshold, which is called the *difficulty*. The difficulty is updated every two weeks (or more precisely every 2016 blocks) so that the rate of validation remains at 1 block per 10 minutes. The pseudo-random properties of the hash function ensure that the only way to find this hash is to probe many hashes, therefore changing a parameter in the header (the nonce). The first miner to find a solution makes the block public, and the network adopts the block as the last block in the blockchain.

It can happen that two blocks are simultaneously validated in different parts of the network. Then a competition follows between the two candidates, and the first one to have a mined block on top of it wins. The other one is discarded and is called an *orphan* block. The blockchain with the larger amount of work (which is in general the longer one) is adopted by the nodes.

When a transaction is included in the last block of the blockchain, we say that it has one confirmation. Any extra block mined on top of this one gives another confirmation to the transaction and engraves it further inside the blockchain.

This apparently complicated procedure is necessary to ensure that neither the network nor the blockchain can be corrupted. Any participant must commit some computer power in order to participate in the decision of validation. The main obstacle for the invention of a decentralised currency was to prevent a double spend without a central accounting authority. Hence, the first mathematical problem that Nakamoto considers in his founding article [1] is to estimate the probability of a double spend. In the following we consider this and other stability problems, and mathematically prove the (almost general) stability of the mining rules.

2 The mining model

We consider a miner with a fraction $0 < p \leq 1$ of the total hashrate. His profit comes from the block rewards of his validated blocks. It is important to know the probability of success when mining a block. The average number of blocks per unit of time that he succeeds in mining is proportional to his hashrate p. The whole network takes on average $\tau_0 = 10$ min to validate a block, hence our miner takes on average $t_0 = \frac{\tau_0}{p}$. We consider the random variable $\mathbf{T}$ giving the time between blocks mined by our miner. The pseudo-random properties of the hash function show that mining is a Markov process, that is, memoryless. It is then an elementary exercise to show from this property that $\mathbf{T}$ follows an exponential distribution,

$$f_{\mathbf{T}}(t) = \alpha e^{-\alpha t}$$

where $\alpha = 1/t_0 = 1/\mathbb{E}[\mathbf{T}]$. If the miner starts mining at $t = 0$, and if we denote $\mathbf{T}_1$ the time needed to mine a first block, then $\mathbf{T}_2, \ldots, \mathbf{T}_n$ the inter-block mining times of successive blocks, then the Markov property shows that the random variables $\mathbf{T}_1, \mathbf{T}_2, \ldots, \mathbf{T}_n$ are independent and are all identically distributed following the same exponential law. Therefore, the time needed to discover n blocks is

$$\mathbf{S}_n = \mathbf{T}_1 + \mathbf{T}_2 + \ldots + \mathbf{T}_n \,.$$

The random variable $\mathbf{S}_n$ follows the n-convolution of the exponential distribution and, as is well known, this gives a Gamma distribution with parameters (n, α),

$$f_{\mathbf{S}_n}(t) = \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t}$$

with cumulative distribution

$$F_{\mathbf{S}_n}(t) = \int_0^t f_{\mathbf{S}_n}(u)du = 1 - e^{-\alpha t} \sum_{k=0}^{n-1} \frac{(\alpha t)^k}{k!} \,.$$

From this we conclude that if $\mathbf{N}(t)$ is the process counting the number of blocks validated at time $t > 0$, $\mathbf{N}(t) = \max\{n \geq 0; \mathbf{S}_n < t\}$, then we have

$$\mathbb{P}[\mathbf{N}(t) = n] = F_{\mathbf{S}_n}(t) - F_{\mathbf{S}_{n+1}}(t) = \frac{(\alpha t)^n}{n!} e^{-\alpha t} \,,$$

and $\mathbf{N}(t)$ follows a Poisson law with mean value αt. This result is classical, and the mathematics of bitcoin mining, as well as other cryptocurrencies with validation based on proof of work, are mathematics of Poisson processes.

3 The double spend problem

The first crucial mathematical problem that deserves attention in the bitcoin protocol is the possibility of realisation of a double spend. This was the major obstacle to overcome for the invention of decentralised cryptocurrencies, thus it is not surprising that Nakamoto addresses this problem in Section 11 of his founding article [1]. He considers the situation where a malicious miner makes a payment, then in secret tries to validate a second conflicting transaction in a new block, from the same address, but to a new address that he controls, which allows him to recover the funds.

For this, once the first transaction has been validated in a block in the official blockchain and the vendor has delivered the goods (the vendor will not deliver unless some confirmations are visible), the only possibility consists of rewriting the blockchain from that block. This is feasible if he controls a majority of the hashrate, that is, if his relative hashrate q satisfies $q > 1/2$, because then he is able to mine faster than the rest of the network, and he can rewrite the last end of the blockchain as he desires. This is the reason why decentralised mining is necessary so that no one controls more than half of the mining power. But even when $0 < q < 1/2$ he can try to attempt a double spend and will succeed with a non-zero probability. The first mathematical problem consists of computing the probability that the malicious miner succeeds in rewriting the last $n \geq 1$ blocks. We assume that the remaining relative hashrate, $p = 1 - q$, consists of honest miners following the protocol rules.

This problem is similar to the classical gambler's ruin problem. Nakamoto observes that the probability of catching up n blocks is

$$q_n = \left(\frac{q}{p}\right)^n \qquad \text{(Nakamoto)}$$

The modelisation of mining shows that the processes $\mathbf{N}(t)$ and $\mathbf{N}'(t)$ counting the number of mined blocks at time t by the honest and malicious miners, respectively, are independent Poisson processes with respective parameters α et α' satisfying

$$p = \frac{\alpha}{\alpha + \alpha'} \,, \quad q = \frac{\alpha'}{\alpha + \alpha'} \,.$$

The random variable $\mathbf{X}_n = \mathbf{N}'(\mathbf{S}_n)$ of the number of blocks mined by the attacker when the honest miners have mined their n-th block follows a negative binomial variable with parameters (n, p) ([3]), thus, for an integer $k \geq 1$ we have

$$\mathbb{P}[\mathbf{X}_n = k] = p^k q^k \binom{k+n-1}{k} .$$

Nakamoto, in section 11 of [1], abusively approximates $\mathbf{X}_n = \mathbf{N}'(\mathbf{S}_n)$ by $\mathbf{N}'(t_n)$ where

$$t_n = \mathbb{E}[\mathbf{S}_n] = n\mathbb{E}[\mathbf{T}] = \frac{n\tau_0}{p}$$

This means that he considers the classical approximation of a negative binomial variable by a Poisson variable. Rosenfeld observes in [4] that the negative binomial variable seems to be a better approximation. We proved in [3] that this was indeed the case, and we could find the exact formula for the double spend probability after z confirmations (z is the classical notation used by Nakamoto for the number of confirmations).

Theorem 1 ([3], 2017)**.** *After z confirmations, the probability of success of a double spend by attackers with a relative hashrate of* $0 < q < 1/2$ *is*

$$P(z) = I_{4pq}(z, 1/2)$$

where $I_x(a,b)$ is the incomplete regularised beta function

$$I_x(a,b) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(1-t)^{b-1}\, dt .$$

Bitcoin security depends on this probability computation. It is not just a theoretical result. It allows the estimation of the risk of a transaction to be reversed and the number of confirmations required to consider it definitive. For example, if $q = 0.1$, after 6 confirmations, the probability of a double spend is smaller than 1 % (for complete tables see [5]).

In his founding article, Nakamoto tried to compute this probability from his approximate argument and ran a numerical simulation. He convinced himself that the probability converges exponentially to 0 when the number of confirmations z goes to infinite (as he states "we can see the probability drop off exponentially with z"). The numerical simulation is not a proof, but this statement is repeated over and over again, however never proved before 2017. With the previous exact formula, using classical methods (Watson Lemma), we can prove the following Corollary:

Corollary 2. *Let $s = 4pq < 1$. When $z \to +\infty$ the probability $P(z)$ decays exponentially, and, more precisely,*

$$P(z) \sim \frac{s^z}{\sqrt{\pi(1-s)z}} .$$

One can obtain higher order asymptotics in the classical way or by using equivalent combinatorical methods as in [6].

We can be more precise by looking at the time it takes for the honest network to mine z blocks. A longer duration than the average $\tau_1 = z\tau_0$ leaves extra time for the attacker to build his replacement blockchain, and with this conditional knowledge the probability changes. If we define $\kappa = \frac{\tau_1}{z\tau_0}$, we can compute this probability $P(z,\kappa)$ and we can also obtain an exact formula using the regularised incomplete Gamma function

$$Q(s,x) = \frac{\Gamma(s,x)}{\Gamma(x)}$$

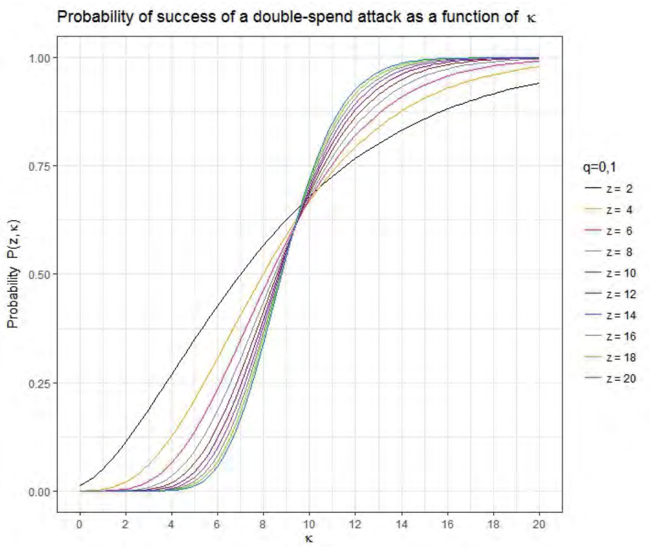


Figure 2. Probabilities $P(z,\kappa)$ for $q = 0.1$ and distinct values of z

where

$$\Gamma(s,x) = \int_x^{+\infty} t^{s-1} e^{-t}\, dt$$

is the incomplete Gamma function.

Theorem 3. *We have*

$$P(z,\kappa) = 1 - Q(z, \kappa\, z\, q/p) + \left(\frac{q}{p}\right)^z e^{\kappa\, z\, \frac{p-q}{p}} Q(z, \kappa\, z) ,$$

Figure 2 shows the graphs of $\kappa \mapsto P(z,\kappa)$ for different values of z.

4 Mining profitability

After studying the security of the protocol, the next important problem is its stability. For a decentralised protocol it is fundamental that the interests of the individuals are properly aligned with the protocol rules. In particular, the maximal gain of miners should be achieved when following the protocol rules. This is far from obvious, and we know from the study of unstable dynamical systems that this is hard to achieve. It is somewhat surprising that this has been empirically verified since Bitcoin's inception.

For example, it is by no means obvious that is in the best interest of a miner to immediately publish a block that he has validated. He can keep it secret and secretly push his advantage, but then he runs the risk that another miner publishes a validated block and the public blockchain adopts it, thus losing his reward. This type of scenario has been discussed since 2012 in bitcointalk forum, created by Nakamoto in 2010.

To answer this question, we first need to develop a proper profitability model. As in any business, mining profitability is accounted by the "Profit and Loss" per unit of time. The profits of a miner come from the block rewards that include the coinbase reward in new bitcoins created, and the transaction fees of the transactions in the block. The profitability at instant $t > 0$ is given by

$$\mathbf{PL}(t) = \frac{\mathbf{R}(t) - \mathbf{C}(t)}{t}$$

where $\mathbf{R}(t)$ and $\mathbf{C}(t)$ represent, respectively, the rewards and the cost of the mining operation up to time t. If we don't consider transaction fees, we have

$$\mathbf{R}(t) = \mathbf{N}(t)\, b$$

where $b > 0$ is the coinbase reward. If we include transaction fees, the last equation remains true, taking the average reward using the classical Wald theorem.

The random variable $\mathbf{C}(t)$ representing the cost of mining operations is far more complex to determine, since it depends on external factors (such as electricity costs, mining hardware costs, geographic location, currency exchange rate, etc). But, fortunately, we don't need it in the comparison of the profitability of different mining strategies, as we explain next.

The mining activity is repetitive and the miners return to the same initial state after some time, for instance, to start mining a fresh block. A mining strategy is composed by cycles where the miner invariably returns to the initial state. It is a "game with repetition" similar to those employed by profit gamblers in casino games (when they can spot a weakness that makes the game profitable). For example, an honest miner starts a cycle each time the network, he or someone else, has validated a new block.

We denote by $\boldsymbol{\tau}$ the duration of the cycle, and we are interested in *integrable* strategies for which $\mathbb{E}[\boldsymbol{\tau}] < +\infty$ (this means that the cycles almost surely up in finite time). Then it is easy to check, using the law of large numbers and Wald theorem, that the long term profitability is given a.s. by the limit

$$\mathbf{PL}_\infty = \lim_{t\to+\infty} \frac{\mathbf{R}(t) - \mathbf{C}(t)}{t} = \frac{\mathbb{E}[\mathbf{R}] - \mathbb{E}[\mathbf{C}]}{\mathbb{E}[\boldsymbol{\tau}]}.$$

As observed before, the second cost term is hard to compute, but the revenue term, that we call *revenue ratio*, is in general computable

$$\boldsymbol{\Gamma} = \frac{\mathbb{E}[\mathbf{R}]}{\mathbb{E}[\boldsymbol{\tau}]}.$$

For example, for an honest miner we have $\mathbb{E}[\mathbf{R}] = p.0 + q.b = qb$ and $\mathbb{E}[\boldsymbol{\tau}] = \tau_0$, and therefore

$$\boldsymbol{\Gamma}_H = \frac{qb}{\tau_0}.$$

We have the fundamental theorem on comparison of mining strategies with the same cost ratio. This is the case when both strategies use the full mining power at all time.

Theorem 4 ([7], 2018)**.** *We consider two mining strategies ξ and η with the same cost by unit of time. Then ξ is more profitable than η if and only if*

$$\boldsymbol{\Gamma}_\eta \leq \boldsymbol{\Gamma}_\xi.$$

5 Protocol stability

We can now mathematically study the protocol stability. The following remarkable result (remarkable because it is hard to imagine how Nakamoto could have foreseen it) validates the proper adjustment of the protocol:

Theorem 5 ([7], 2018)**.** *In the absence of difficulty adjustment, the optimal mining strategy is to immediately publish all mined blocks as soon as they are discovered.*

Remember that the difficulty of mining adjusts about every two weeks, so at the same time we spot a weakness of the protocol that we discuss below.

This theorem holds true for any hashrate of the miner and without any assumption of the type of miners present in the network. It does not change anything that eventually there are some dishonest miners in the network.

The proof is simple and a good example of the power of martingale techniques. For a constant difficulty, the average speed of block discovery remains constant and the counting process $\mathbf{N}(t)$ is a Poisson process with intensity $\alpha = \frac{p}{\tau_0}$ where p is the relative hashrate of the miner. The cycle duration $\boldsymbol{\tau}$ is a stopping time and the revenue per cycle equals to $\mathbf{R} = \mathbf{N}(\boldsymbol{\tau})$. Its mean value is then obtained using Doob's stopping time to the martingale $\mathbf{N}(t) - \alpha t$. Finally, we get $\boldsymbol{\Gamma} \leq \boldsymbol{\Gamma}_H$.

But the bitcoin protocol does have a difficulty adjustment algorithm that is necessary, in particular during the development phase. Theorem 5 shows that this is the only vector of attack. This difficulty adjustment provides a steady monetary creation and ensures that the interblock validation time stays at around 10 minutes. A minimum delay is necessary to allow a good synchronisation of all network nodes. If the hashrate accelerates without a difficulty adjustment, then the nodes will desynchronize, and many competing blockchains will appear, leaving a chaotic state.

6 Profitability of rogue strategies

In view of Theorems 4 and 5, and in order to decide if a mining strategy is more profitable than the honest strategy, we need only compute the revenue ratio $\boldsymbol{\Gamma}$ with the difficulty adjustment integrated. Selfish mining (SM strategy 1) is an example of rogue strategy. Instead of publishing a new block, the miner keeps the block secret and tries to build a longer blockchain, increasing its advantage. When he makes it public, he will orphan the last mined honest blocks and will reap the rewards. To be precise, the attack cycles are defined as follows: the miner starts mining a new block on top of the official blockchain. If an honest miner finds a block first, then the cycle ends and he starts over. Otherwise, when he is the first to find a block, he keeps mining on top of it, and keeping it secret. If before he mines a second block the honest network mines one public block, then he publishes his block immediately, thus trying to get a maximum proportion $0 < \gamma < 1$ of honest miners to adopt his block. The propagation is not instantaneous and the efficiency depends on the new parameter γ which represents his good connectivity to the network. A competition follows, and if the next block is mined on top of the honest block, then the selfish miner looses the rewards of this block and the attack cycle ends. If he, or his allied honest miners, mine the next block, then they publish it and the attack cycle ends again. If the attacker succeeds in mining two consecutive secret blocks at the beginning, then he continues working on his secret blockchain until he has only one block of advantage with respect to the public blockchain. In this case, he doesn't run any risk of being joined by the public blockchain and publishes all his secret blockchain, thus reaping all the rewards and ending the attack cycle again. In few words, the rogue miner spends most of his time replacing honest blocks by those that he has mined in advance and kept secret. The mean duration $\mathbb{E}[\boldsymbol{\tau}]$ of the attack cycle is obtained as a variation of the following result about Poisson processes.

Proposition 6 (Poisson races)**.** *Let* $\mathbf{N}$ *and* $\mathbf{N}'$ *be two independent Poisson processes with respective parameters* α *and* α'*, with* $\alpha' < \alpha$ *and* $\mathbf{N}(0) = \mathbf{N}'(0) = 0$*. Then, the stopping time*

$$\boldsymbol{\sigma} = \inf\{t > 0; \mathbf{N}(t) = \mathbf{N}'(t) + 1\}$$

is almost surely finite, and we have

$$\mathbb{E}[\boldsymbol{\sigma}] = \frac{1}{\alpha - \alpha'}\,, \quad \mathbb{E}[\mathbf{N}'(\boldsymbol{\sigma})] = \frac{\alpha'}{\alpha - \alpha'}\,, \quad \mathbb{E}[\mathbf{N}(\boldsymbol{\sigma})] = \frac{\alpha}{\alpha - \alpha'}\,.$$

The proof is a simple application of Doob's stopping time theorem. Here, $\mathbf{N}$ and $\mathbf{N}'$ are the counting processes of blocks mined by the honest miners and the attacker. To finish, we must compute the intensities α and α'. At the beginning we have $\alpha = \alpha_0 = \frac{p}{\tau_0}$ and $\alpha' = \alpha_0' = \frac{q}{\tau_0}$, where p is the apparent hashrate of the honest miners and q the one of the attacker. But the existence of a selfish miner perturbs the network and slows down the production of blocks. Instead of having one block for each period τ_0, the progression of the official blockchain is of $\mathbb{E}[N(\boldsymbol{\tau}) \vee N'(\boldsymbol{\tau})]$ blocks during $\mathbb{E}[\boldsymbol{\tau}]$. After validation of 2016 official blocks, this triggers a difficulty adjustment that can be important. The new difficulty is obtained from the old one by multiplication by a factor $\delta < 1$ given by

$$\delta = \frac{\mathbb{E}[N(\boldsymbol{\tau}) \vee N'(\boldsymbol{\tau})]\,\tau_0}{\mathbb{E}[\boldsymbol{\tau}]}.$$

After the difficulty adjustment, the new mining parameters are $\alpha = \alpha_1 = \frac{\alpha_0}{\delta}$ and $\alpha' = \alpha_1' = \frac{\alpha_0'}{\delta}$. The stopping time $\boldsymbol{\tau}$ and the parameter δ can be computed using the relation $|N(\boldsymbol{\tau}) - N'(\boldsymbol{\tau})| = 1$. This can be used to compute the revenue ratio of the strategy [7]. This analysis can also be checked by mining simulators.

An alternative procedure consists of modelling the network by a Markov chain, where the different states correspond to a different degree of progress by the selfish miner. Each transition corresponds to a revenue increase $\boldsymbol{\pi}$ and $\boldsymbol{\pi}'$ for the honest and selfish miner. By another application of the law of large numbers, we prove that the long-term apparent hashrate of the strategy, defined as the proportion of mined blocks by the selfish miner compared to the total number of blocks, is given by the formula

$$q' = \frac{\mathbb{E}[\boldsymbol{\pi}']}{\mathbb{E}[\boldsymbol{\pi}] + \mathbb{E}[\boldsymbol{\pi}']}.$$

The expectation is taken as relative to the stationary probability that exists because the Markov chain is transitive and recurrent. Indeed, the Markov chain is essentially a random walk on $\mathbb{N}$ partially reflexive on 0. The computation of this stationary probability proves the following theorem:

Theorem 7 ([8], 2014)**.** *The apparent hashrate of the selfish miner is*

$$q' = \frac{((1+pq)(p-q)+pq)q - (1-\gamma)p^2q(p-q)}{p^2q + p - q}$$

The results from [7] and [8] obtained by these different methods are compatible. The revenue ratio $\mathbf{\Gamma}_1$ and the apparent hashrate q' are related by the following equation:

$$\mathbf{\Gamma}_1 = q'\frac{b}{\tau_0}$$

But the first analysis is finer, since it does explain the change of profitablity regime after the difficulty adjustment. In particular, it allows us to compute the duration before running into profitability for the attacker. The selfish miner starts by losing money, then after the difficulty adjustment that favours him, starts making profits. For example, with $q = 0.1$ and $\gamma = 0.9$, he needs to wait 10 weeks in order to be profitable. This partly explains why such an attack has never been observed in the bitcoin network.

Theorem 4 gives an explicit semi-algebraic condition on the parameters, namely $q' > q$, that determines the values of the parameters q and γ for which the selfish mining strategy is more profitable than honest mining.

Theorem 5 shows that the achilles heel of the protocole is the difficulty adjustment formula. This formula is supposed to contain the information about the total hashrate, but in reality it ignores the orphan blocks. The authors propose a solution that incorporates this count, and this solves the stability problem of the protocol [7].

There are other possible block-withholding strategies that are variations of the above strategy [9]. These are more agressive strategies. In the initial situation where the attacker succeeds in being two blocks ahead, instead of publishing the whole secret chain when he is only one block ahead, he can wait to be caught up to release his blocks and then start a final competition between the two competing chains. The attack cycle ends when the outcome is decided. This is the "Lead Stubborn Mining" (LSM, strategy 2). In this strategy it is important that the miner regularly publishes his secret blocks with the same height of the official blockchain, to attract part of the honest miners in order to take out hashrate from the pool of honest miners. Also in this way, even if he loses the final competition he will succeed in incorporating some of his blocks in the official blockchain and reap the corresponding rewards.

Another even more agressive variation consists of waiting not to be caught up, but to be behind one block. This is the "Equal Fork Stubborn Mining Strategy" (EFSM, strategy 3). Here again, it is important to publish secret blocks regularly. Finally, the authors have considered another more agressive variation where the stubborn miner follows EFSM but then doesn't stop when he is one block behind. He keeps on mining until his delay becomes greater than a threshold A or until he successfully comes from behind, catches up and finally takes the advantage over the official blockchain.

This strategy seems desperate because the official blockchain progress is faster, on average. But in the case of catching up, the selfish miner wins the jackpot of all the blocks he replaces. This is the "A-Trailing Mining" strategy (A-TM, strategy 4). The authors of [9] conduct a numerical study of profitability by running a Montecarlo simulation and compare the profitability of the different strategies for different parameter values (q, γ). But we can find closed form formulas for

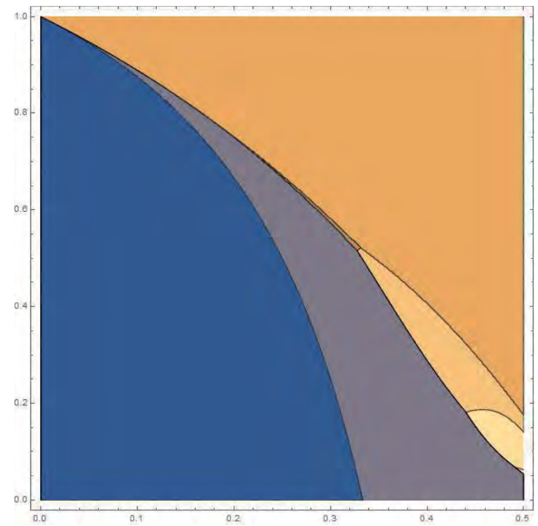


Figure 3. Comparison of HM, SM, LSM, EFSM and A-TSM

the revenue ratio of all these strategies using the precedent martingale approach.

Theorem 8 ([7, 10–12])**.** *We have*

$$\frac{\boldsymbol{\Gamma}_1}{\boldsymbol{\Gamma}_H} = \frac{(1+pq)(p-q)+pq-(1-\gamma)p^2(p-q)}{p^2q+p-q}$$

$$\frac{\boldsymbol{\Gamma}_2}{\boldsymbol{\Gamma}_H} = \frac{p+pq-q^2}{p+pq-q} - \frac{p(p-q)f(\gamma,p,q)}{p+pq-q}$$

$$\frac{\boldsymbol{\Gamma}_3}{\boldsymbol{\Gamma}_H} = \frac{1}{p} - \frac{p-q}{pq}f(\gamma,p,q)$$

$$\frac{\boldsymbol{\Gamma}_4}{\boldsymbol{\Gamma}_H} = \frac{1+\frac{(1-\gamma)p(p-q)}{(p+pq-q^2)[A+1]}\left(\left([A-1]+\frac{1}{p}\frac{P_A(\lambda)}{[A+1]}\right)\lambda^2-\frac{2}{\sqrt{1-4(1-\gamma)pq}+p-q}\right)}{\frac{p+pq-q}{p+pq-q^2}+\frac{(1-\gamma)pq}{p+pq-q^2}(A+\lambda)\left(\frac{1}{[A+1]}-\frac{1}{A+\lambda}\right)}$$

with

$$f(\gamma,p,q) = \frac{1-\gamma}{\gamma}\cdot\left(1-\frac{1}{2q}\left(1-\sqrt{1-4(1-\gamma)pq}\right)\right)$$

and

$$\lambda = q/p, q \quad [n] = \frac{1-\lambda^n}{1-\lambda} \quad \textit{for } n\in\mathbb{N},$$

$$P_A(\lambda) = \frac{1-A\lambda^{A-1}+A\lambda^{A+1}-\lambda^{2A}}{(1-\lambda)^3}.$$

We can plot the parameter regions where each strategy is the best one (Figure 3). The Catalan numbers appear naturally in the computations.

$$C_n = \frac{1}{2n+1}\binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}.$$

For this reason, their generating function appears in the formulas

$$C(x) = \sum_{n=0}^{+\infty} C_n x^n = \frac{1-\sqrt{1-4x}}{2x}$$

We observe that $\sqrt{1-4pq} = p-q$ and $C(pq) = 1/p$, and this justifies the definition of new probability distributions that arise in the proofs.

Definition 9. A discrete random variable X taking integer values follows a Catalan distribution of the first type if we have, for $n \geq 0$,

$$\mathbb{P}[X=n] = C_n p(pq)^n.$$

It follows a Catalan distribution of the second type if $\mathbb{P}[X = 0] = p$ and for $n \geq 1$,

$$\mathbb{P}[X=n] = C_{n-1}(pq)^n.$$

It follows a Catalan distribution of the third type if $\mathbb{P}[X = 0] = p$, $\mathbb{P}[X = 1] = pq + pq^2$ and for $n \geq 2$,

$$\mathbb{P}[X=n] = pq^2C_{n-1}(pq)^{n-1}.$$

7 Dyck words

We can recover these results by a direct combinatorical approach representing each attack cycle by a Dyck word.

Definition 10. A Dyck word is a word built from the two letter alphabet $\{S, H\}$ which contains as many S letters as H letters, and such that any prefix word contains more or equal S letters than H letters. We denote $\mathcal{D}$ the set of Dyck words, and for $n \geq 0$, $\mathcal{D}_n$ the subset of Dyck worlds of length $2n$.

The relation to Catalan numbers is classical: the cardinal of $\mathcal{D}_n$ is C_n. We can encode attack cycles by a chronologic succession of block discoveries (disregarding if it is made public or not). For a selfish block we use the letter S (for "selfish") and for the honest blocks the letter H (for "honest").

The link between the selfish mining strategy and Dyck words is given by the following proposition:

Proposition 11. *The attack cycles of the SM strategy are H, SHH, SHS, and SSwH where $w \in \mathcal{D}$.*

At the end of the cycle, we can summarise and count the total number of official blocks, say L, and how many of these blocks were mined by the attacker, say Z. Then, for strategy 1 (SM), the random variable $L-1$ follows a Catalan distribution of the third type, and except for some particular cases (when $L < 3$), we always have $L = Z$. The apparent hashrate q' is then given by the formula:

$$q' = \frac{\mathbb{E}[Z]}{\mathbb{E}[L]}$$

We can then directly recover Theorem 7 by this simpler combinatorical procedure [12]. The other rogue strategies can be studied in a similar way. The Catalan distribution of the first type arises in the study of the strategy EFSM (strategy 3), and the one of the second type for the strategy LSM (strategy 2). We can then recover all the results given by the Markov chain analysis. Unfortunately, we cannot recover the more finer results obtained by martingales techniques.

This sort of analysis applies to other Proof of Work cryptocurrencies, and to Ethereum, which has a more complex reward system and a different difficulty adjustment formula [13].

8 Nakamoto double spend revisited

We come back to the fundamental double spend problem from the Nakamoto bitcoin paper discussed in Section 3. In that

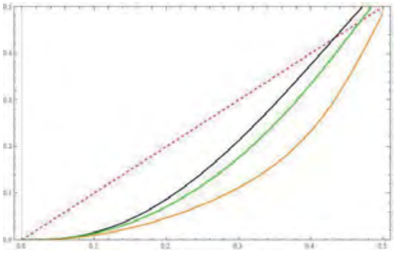


Figure 4. Graph of Γ_A, for $z = 2$, $v = b$ and $A = 3, 5, 10$

section, we computed the probability of success of a double spend. But now, with the profitability model knowledge from Section 4, we can study its profitability and get better estimates on the number of confirmations that are safe to consider a paiement definitive. The double spend strategy as presented in [1] is unsound because there is a non-zero probability of failure, and in that case, if we keep mining in the hope of catching up from far behind the official blockchain, we have a positive probability of total ruin. Also, the strategy is not integrable, since the expected duration of the attack is infinite. Thus, we must obviously apply a threshold to the unfavourable situation where we are lagging far behind the official blockchain.

We assume that the number of confirmations requested by the recipient of the transaction is z and we assume that we are never behind $A \geq z$ blocks of the official blockchain. This defines an integrable strategy, the A-Nakamoto double spend strategy. Putting aside technical details about premining, the probability of success of this strategy is a modification of the probability from Theorem 1.

Theorem 12 ([14], 2019)**.** *After z confirmations, the probability of success of an A-Nakamoto double spend is*

$$P_A(z) = \frac{P(z) - \lambda^A}{1 - \lambda^A}$$

where $P(z)$ is the probability from Theorem 1 and $\lambda = q/p$.

If v is the amount to double spend, then we can compute the revenue ratio $\mathbf{\Gamma}_A = \mathbb{E}[\mathbf{R}]/\mathbb{E}[\boldsymbol{\tau}]$.

Theorem 13 ([14], 2019)**.** *With the previous notations, the expected revenue and the expected duration of the A-Nakamoto double spend strategy is*

$$\begin{aligned}\mathbb{E}[\mathbf{R}_A]/b &= \frac{qz}{2p} I_{4pq}(z, 1/2) - \frac{A\lambda^A}{p(1-\lambda)^3[A]^2} I_{(p-q)^2}(1/2, z) \\ &\quad + \frac{2 - \lambda + \lambda^{A+1}}{(1-\lambda)^2[A]} \frac{p^{z-1}q^z}{B(z,z)} + P_A(z)\left(\frac{v}{b} + 1\right) \\ \mathbb{E}[\mathbf{T}_A]/\tau_0 &= \frac{z}{2p} I_{4pq}(z, 1/2) + \frac{A}{p(1-\lambda)^2[A]} I_{(p-q)^2}(1/2, z) \\ &\quad - \frac{p^{z-1}q^z}{p(1-\lambda)\,B(z,z)} + \frac{1}{q}\end{aligned}$$

with the notation $[n] = \frac{1-\lambda^n}{1-\lambda}$ for an integer $n \geq 0$, and B is the classical Beta function.

In principle, a powerful miner does not have an interest in participating in a large double spend, since doing so will undermine the foundations of his business. For a small miner with relative hashrate $0 < q << 1$ we can estimate from which amount a double spend can be profitable. For this we only need to use the inequality from Theorem 4: $\mathbf{\Gamma}_A \geq \mathbf{\Gamma}_H = qb/\tau_0$, and take the asymptotics $q \to 0$ (with A and z being fixed, but the final result turns out to be independent of A).

Corollary 14. *When $q \to 0$, the minimal amount v for an Nakamoto double spend with $z \geq 1$ confirmations is*

$$v \geq \frac{q^{-z}}{2\binom{2z-1}{z}} b = v_0 \ .$$

For example, in practice, with a 10% hashrate, $q = 0.01$, and only one confirmation, $z = 1$, we need to double spend more than $v_0/b = 50$ coinbases. With the actual coinbase reward of $b = 12.5$ ₿ and the actual prize over 8.300 euros, this represents more than 5 million euros.

Hence, for all practical purposes and normal amount transactions, only one confirmation is enough to consider the transaction definitive.

Conclusions

Bitcoin provides a good example of the universality of mathematical applications and its potential to impact our society. With the glimpse we have given, we hope to have convinced our colleagues that the Bitcoin protocol also motivates some exciting Mathematics.

Bibliography

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," www.bitcoin.org/bitcoin.pdf, released on November 1st 2008 on the USENET Cryptography Mailing List "Bitcoin P2P e-cash paper".

[2] R. Pérez-Marco, "Bitcoin and decentralized trust protocols," *Newsletter European Mathematical Society*, vol. 21, no. 100, pp. 31–38, 2016.

[3] C. Grunspan and R. Pérez-Marco, "Double spend races," *Int. Journal Theoretical and Applied Finance*, vol. 21, no. 08, 2018.

[4] M. Rosenfeld, "Analysis of hashrate-based double spending," arXiv:1402.2009, 2014.

[5] C. Grunspan and R. Pérez-Marco, "Satoshi risk tables," arXiv:1702.04421, 2017.

[6] E. Giogladis and D. Zeilberger, "A combinatorial-probabilistic analysis of bitcoin attacks," *Journal of Difference Equations and its Applications*, vol. 25, no. 1, 2019.

[7] C. Grunspan and R. Pérez-Marco, "On the profitability of selfish mining," arXiv:1805.08281, 2018.

[8] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, pp. 95–102, June 2018.

[9] K. Nayak, S. Kumar, A. K. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 305–320, 2015.

[10] C. Grunspan and R. Pérez-Marco, "On the profitability of stubborn mining," arXiv:1808.01041, 2018.

[11] C. Grunspan and R. Pérez-Marco, "On the profitability of trailing mining," arXiv:1811.09322, 2018.

[12] C. Grunspan and R. Pérez-Marco, "Bitcoin selfish mining and Dyck words," arXiv:1811.09322, 2019.

[13] C. Grunspan and R. Pérez-Marco, "Selfish mining in Ethereum," arXiv:1904.13330, 2019.

[14] C. Grunspan and R. Pérez-Marco, "On profitability of nakamoto double spend," arXiv:1912.06412, 2019.

The authors [cyril@grunspan.net, ricardo.perez.marco@gmail.com] did study at Lycée Louis-le-Grand with the late Prof André Warusfel, and are alumni of the École Normale Supérieure of Paris. They are pioneers in mathematical research in Bitcoin and other cryptocurrencies and organize regularly the Paris cryptofinance seminar since 2016.

ICMI Column

Jean-Luc Dorier (Université de Genève, Switzerland)

News in brief

The congress **ICME14** will be held in Shanghai, 12–19 July 2020. All information can be found at www.icme14.org. On 12 July the Early Career Day for young researchers and the General Assembly of ICMI, where the new EC will be elected for the period 1.1.2021–31.12.2023, will be held simultaneously.

The **ICMI awards** will be officially presented at the opening ceremony.

- *Felix Klein awards*:
  2017: Deborah Ball, 2019: Tommy Dreyfus
- *Hans Freudenthal awards*:
  2017: Terezinha Nunes, 2019: Gert Schubring
- *Emma Castelnuevo award* 2019: NCTM (National council of teachers of mathematics).

ICME15 will take place in Sydney, Australia on 7–14 July 2024.

The **ICMI Study 25** conference on "Teachers of Mathematics Working and Learning in Collaborative Groups" will be held in Lisbon, Portugal on 3–7 February 2020. See http://icmistudy25.ie.ulisboa.pt/.

The study volume for **ICMI Study 24** on "School Mathematics Curriculum Reforms: Challenges, Changes and Opportunities" is in preparation. The aim is to present the volume at ICME14.

CANP was launched by ICMI in 2010, with the support of UNESCO and IMU, to strengthen the educational capacity of all those involved in teacher preparation and professional development, creating sustained and effective regional networks of teachers, mathematics educators and mathematicians, and also linking them to international support (see https://www.mathunion.org/icmi/activities/developing-countries-support/capacity-networkingproject-canp). Within one decade, CANP has become a major ICMI-IMU project in developing countries.

The CEMAS network (Communidad de Educación Matemática de América del Sur) was created during CANP5, which was held in Lima, Peru in February 2016, for the Andean countries (Bolivia, Ecuador, Peru) and Paraguay. And, in September 2019, it organised the first EIII CEMAS (Encuentro Internacional de Iniciativas Innovadoras) with the generous support of the Consejo Nacional de Ciencia y Tecnología (CONACYT) of Paraguay. It gathered more than 200 passionate participants: primary and secondary teachers coming from all Paraguayan regions, student teachers, teacher educators and researchers in mathematics education and in mathematics. The three days, perfectly organised, offered a very rich and intense programme combining eight plenary lectures covering both general themes and the presentation and analysis of specific innovative and research projects, most of them carried out in the region, and four 1h45 slots for parallel sessions proposing workshops on diverse topics.

The event concluded with a round table, where participants discussed regional problems with the invited international experts. In fact, among the 20 presenters, 7 were from Paraguay, 9 from Peru, Ecuador and Chile, and four from Brazil, France, Mexico and USA. Unfortunately, Angel Ruiz from Costa Rica, past vice-president of ICMI and organiser of CANP 2, and Beatriz Macedo from Uruguay, who had supported the launching of CANP when she was working at UNESCO, could not attend. This was also the case for Yuriko Baldin Yamamoto, who has been the ICMI liaison officer or CANP 5 and accompanied the CEMAS network since 2016.

ERME Column

Jason Cooper (Weizmann Institute of Science, Israel)

ERME topic conferences

European Society for Research in Mathematics Education (ERME) Topic Conferences (ETC) are organised on a specific research theme or themes related to the work of thematic working groups at CERME conferences. Their aim is to extend the work of the group or groups in specific directions, with clear value to the mathematics education research community. We announce an upcoming ETC:

INDRUM – International Network for Didactic Research in University Mathematics

INDRUM2020, to be held 27–29 March in Bizerte, Tunisia, is the third conference of the International Network for Didactic Research in University Mathematics. Initiated by an international team of researchers in didactics of mathematics, INDRUM aims to contribute to the development of research in didactics of mathematics at all levels of tertiary education, with particular concern for the development of new researchers in the field and for dialogue with mathematicians (https://hal.archives-ouvertes.fr/INDRUM). The themes addressed at INDRUM2020 cover teacher and student practices and the teaching and learning of specific mathematical topics at undergraduate and post-graduate level, as well as across disciplines. The target audience of the conference is researchers in didactics of mathematics, but also mathematicians, teachers and researchers who are interested in these issues. The programme of the conference comprises: a plenary talk by Carl Winsløw (University of Copenhagen, Denmark); an expert panel discussion on higher education in the "digital age"; four thematic working groups; short communications in parallel; a poster exhibition; and a training session for young researchers. The main language of the conference is English, with an option of presenting a paper in French or Arabic, provided slides or a handout in English are provided. INDRUM2020 is an ERME topic conference. The event will be preceded on 26 March by a special day in honour of Viviane Durand-Guerrier, who is a former ERME President (2013–2017). For more information see: https://indrum2020.sciencesconf.org.

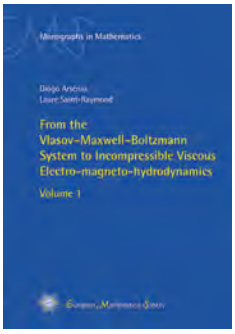
Thomas Hausberger (INDRUM2020 IPC Chair),
Marianna Bosch (IPC Co-chair)

CERME Thematic Working Groups

The European Society for Research in Mathematics Education (ERME) holds a bi-yearly conference (CERME), in which research is presented and discussed in Thematic Working Groups (TWG). The initiative of introducing the working groups, which we began in the September 2017 issue, will continue in the following issue of the newsletter.

Jason Cooper is an associate staff scientist at the Weizmann Institute's Department of Science Teaching. His research concerns various aspects of teacher knowledge, including roles of advanced mathematical knowledge in teaching mathematics and contributions of research mathematicians to the professional development of mathematics teachers.

Book Reviews


Monographs in Mathematics
Diogo Arsénio
Laure Saint-Raymond
From the Vlasov–Maxwell–Boltzmann System to Incompressible Viscous Electro-magneto-hydrodynamics
Volume 1
European Mathematical Society

Diogo Arsénio
Laure Saint-Raymond
From the Vlasov–Maxwell–Boltzmann System to Incompressible Viscous Electro-magneto-hydrodynamics, Volume 1

EMS Publishing House, 2019
418 p.
ISBN 978-3-03719-193-4

Reviewer: Alain Brillard

The Newsletter thanks zbMATH and Alain Brillard for the permission to republish this review, which originally appeared as Zbl 1427.76001.

The book is devoted to the analysis of viscous hydrodynamics limits mainly from a fundamental point of view. A second book will indeed follow the present one with applications. The present book is divided in two parts and twelve chapters. Three appendices complete the book.

The first part contains three chapters respectively devoted to the presentation of Vlasov–Maxwell–Boltzmann system and its properties, and to the corresponding mathematical framework. It gathers weak stability results for the limiting macroscopic systems. The second part presents the formal limits which are deduced from this Vlasov–Maxwell–Boltzmann system according to different scalings.

Chapter 1 starts with the Vlasov–Maxwell–Boltzmann system which describes viscous and incompressible magnetohydrodynamics. It is written as

$$\begin{aligned}
&\partial_t f + v\cdot\nabla_x f + \frac{q}{m}(E + v\wedge B)\cdot\nabla_v f = Q(f,f),\\
&\mu_0\epsilon_0\partial_t E - rotB = -\mu_0 q\int_{\mathbb{R}^3} f v dv,\\
&\partial_t B + rotE = 0,\\
&\operatorname{div} E = \frac{q}{\epsilon_0}\left(\int_{\mathbb{R}^3} f dv - 1\right),\\
&\operatorname{div} B = 0,
\end{aligned}$$

where f is the density of charged particles which depends on the time $t \in (0,\infty)$, on the position x and on the velocity v, q is the charge, m is the mass, E is the electric field, B is the magnetic field, Q is Boltzmann collision operator, μ_0 is the vacuum permeability and ϵ_0 is the vacuum permittivity. Because the charged ions may be positive or negative, the Vlasov–Boltzmann equation may be split in two equations

$$\partial_t f^+ + v\cdot\nabla_x f^+ + \frac{q^+}{m^+}(E+v\wedge B)\cdot\nabla_v f^+ = Q(f^+,f^+)+Q(f^+,f^-)$$

for the cations and

$$\partial_t f^- + v\cdot\nabla_x f^- - \frac{q^-}{m^-}(E+v\wedge B)\cdot\nabla_v f^- = Q(f^-,f^-)+Q(f^-,f^+)$$

for the anions, the integral

$$\int_{\mathbb{R}^3} q f v dv$$

being replaced in Ampère and Gauss equations by

$$\int_{\mathbb{R}^3}(q^+f^+ - q^-f^-)vdv \quad\text{or}\quad \int_{\mathbb{R}^3}(q^+f^+ - q^-f^-)vdv,$$

respectively. The Boltzmann collision operator is taken as

$$Q(f,h) = \int_{\mathbb{R}^3}\int_{\mathbb{S}^2}(f(v')h(v'_*) - f(v)h(v_*))b(v-v_*,\sigma)d\sigma dv_*$$

where

$$v' = \frac{v+v_*}{2} + \frac{|v-v_*|}{2}\sigma, \qquad v'_* = \frac{v+v_*}{2} - \frac{|v-v_*|}{2}\sigma.$$

The collision kernel b depends on the relative velocity $|z|$ and on the deviation angle θ as

$$b(|z|,\cos\theta) = \frac{\beta}{\sin\epsilon}\frac{\partial\beta}{\partial\theta}|z|,$$

where β is the impact parameter. The authors will not assume the usual simplifying cutoff hypothesis for the collision kernel. The authors then derive that the entropy dissipation is non negative, which leads to Boltzmann H-theorem and that the entropy

$$\int_{\mathbb{R}^3} f\log f dv$$

is at least formally a Lyapunov function for the Boltzmann equation. They also prove the entropy inequality. The authors finally explain that they will consider renormalized solutions to the Vlasov–Maxwell–Boltzmann system, although their existence is not yet proved. They indeed explain the difficulty to prove the convergence to renormalized solutions of approximate solutions to the Vlasov–Maxwell–Boltzmann system. Such approximate solutions instead converge to measure-valued renormalized solutions with the introduction of Young measures.

Chapter 2 starts with the description of incompressible viscous regimes. The authors write the Boltzmann equation in adimensional variables as

$$S_t\partial_t f + v\cdot\nabla_x f = \frac{1}{Kn}Q(f,f),$$

where Kn is Knudsen number equal to the ratio λ_0/l_0 between the mean free path λ_0 and the observation length scale l_0, St is Strouhal number equal to l_0/c_0t_0 with c_0 the speed of sound and t_0 the unit time. The authors also introduce Mach number as $Ma = u_0/c_0$ where u_0 is the bulk velocity. They consider hydrodynamics limits obtained when Kn goes to 0 (hence $Ma \to 0$) and they take the density f in the form $f = M(1 + Mag)$ where M is the global normalized Maxwellian equilibrium of density 1, bulk velocity 0 and temperature 1 defined as:

$$M(v) = \frac{1}{(2\pi)^{\frac{3}{2}}}e^{-\frac{|v|^2}{2}}.$$

They rewrite the Vlasov–Maxwell–Boltzmann system assuming that Kn, St and Ma are of the same order ϵ. A parameter δ appears which has to be compared to this order ϵ. Changing also the units of E and B, the authors get the problem

$$\begin{aligned}
&\epsilon\partial_t f + v\cdot\nabla_x f + (\alpha E + \beta v\wedge B)\cdot\nabla_v f = \frac{1}{\epsilon}Q(f,f),\\
&f = M(1+\epsilon g),\\
&\gamma\partial_t E - rotB = -\frac{\beta}{\epsilon^2}\int_{\mathbb{R}^3} f v dv,\\
&\gamma\partial_t B + rotE = 0,\\
&\operatorname{div} E = \frac{\alpha}{\epsilon^2}\left(\int_{\mathbb{R}^3} f dv - 1\right),\\
&\operatorname{div} B = 0,
\end{aligned}$$

for one species and

$$\begin{aligned}
&\epsilon\partial_t f^{\pm} + v\cdot\nabla_x f^{\pm} \pm (\alpha E + \beta v\wedge B)\cdot\nabla_v f^{\pm}\\
&\qquad = \frac{1}{\epsilon}Q(f^{\pm},f^{\pm}) + \frac{\delta}{\epsilon^2}Q(f^{\pm},f^{\mp}),\\
&f^{\pm} = M(1+\epsilon g^{\pm}),\\
&\gamma\partial_t E - rotB = -\frac{\beta}{\epsilon^2}\int_{\mathbb{R}^3}(f^+ - f^-) v dv,\\
&\gamma\partial_t B + rotE = 0,\\
&divE = \frac{\alpha}{\epsilon^2}(\int_{\mathbb{R}^3}(f^+ - f^-)dv - 1),\\
&divB = 0
\end{aligned}$$

for two species. They formally derive the asymptotic systems according to the orders of this parameter δ. They conclude Chapter 2 with the formal derivations of the asymptotic systems in the case of two species.

In Chapter 3, the authors analyze the well-posedness of three asymptotic problems which have been formally derived in Chapter 2: an incompressible quasi-static Navier-Stokes–Fourier–Maxwell–Poisson system, the two-fluid incompressible Navier-Stokes–Fourier–Maxwell system with Ohm's law and the two-fluid incompressible Navier-Stokes–Fourier–Maxwell system with solenoidal Ohm's law. The chapter starts with the incompressible quasi-static Navier-Stokes–Fourier–Maxwell-Poisson system written as

$$\begin{aligned}
&\partial_t u + u\cdot\nabla_x u = -\nabla_x p + E + \rho\nabla_x\theta + u\wedge B,\\
&\operatorname{div} u = 0,\\
&\partial_t(\frac{3}{2}\theta - \rho) + u\cdot\nabla_x(\frac{3}{2}\theta - \rho) - \frac{5}{2}\kappa\Delta_x\theta = 0,\\
&\Delta_x(\rho+\theta) = \rho,\\
&rotB = u,\\
&\operatorname{div} E = \rho,\\
&\partial_t B + rotE = 0,\\
&\operatorname{div} B = 0.
\end{aligned}$$

Initial conditions $(\rho^{in}, u^{in}, \theta^{in}, B^{in})$ are added. The authors first prove a global energy inequality assuming that (ρ, u, θ, B) is a smooth solution to this problem. They define the notion of weak or Leray solution and they prove the existence of such a weak solution under hypotheses on the initial data. They then move to the Navier-Stokes–Fourier–Maxwell system with Ohm's law and the two-fluid incompressible Navier-Stokes–Fourier–Maxwell system with solenoidal Ohm's law. They prove that a smooth solution (u, E, B) to these problems satisfies a global conservation of energy. They quote from the literature the existence of large global solutions in the 2D case to the Navier-Stokes-Maxwell system, or a local small solution to this problem in the 3D case. Chapter 3 ends with the proof of weak-strong stability and existence results for dissipative solutions to these two systems.

Part II begins with Chapter 4 which is devoted a deeper analysis of two asymptotic systems. The authors first define the notion of renormalized solutions to the Vlasov–Maxwell–Boltzmann system with one or two species, first for the Vlasov–Boltzmann equation

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

assuming that the given force F satisfies at least

$$F, \nabla_v\cdot F \in L^1_{\text{loc}}(dtdx; L^1(M^\alpha dv)) \quad \text{for all} \quad \alpha > 0,$$

where M is the global asymptotic Maxwellian equilibrium. Assuming now classical hypotheses on the kernel b, on F and on the initial data, the authors recall the existence of a renormalized solution to the Vlasov-Boltzmann equation which further satisfies a local conservation of mass property and the global entropy inequality. The authors then define the notion of renormalized solution to the Vlasov–Maxwell–Boltzmann system with one or two species and they analyze macroscopic conservation laws within this context. In the case of the Navier-Stokes–Fourier–Maxwell-Poisson system, the authors assume the existence of a renormalized solution to the one species Vlasov–Maxwell–Boltzmann system and they prove a weak relatively compactness result in $L^1_{\text{loc}}(dtdx)$ for special macroscopic fluctuations of the density, bulk velocity and temperature and under hypotheses on the initial data. The limit is a weak solution to the Navier-Stokes–Fourier–Maxwell-Poisson system. The proof of this result is postponed to Chapter 11. In the case of the Navier-Stokes–Fourier–Maxwell system with solenoidal Ohm's law, the authors also assume the existence of renormalized solutions to the Vlasov–Maxwell–Boltzmann system with two species. They again prove a weak relatively compactness result is $L^1_{\text{loc}}(dtdx)$ and that the limit is a non-positive solution to the Navier-Stokes–Fourier–Maxwell system with solenoidal Ohm's law. They here assume that the initial data satisfy different hypotheses among which a "well-prepared" hypothesis. A quite similar weak relatively compactness result is proved in the case of Navier-Stokes–Fourier–Maxwell system with Ohm's law and the proofs of these results are postponed to Chapter 12.

In Chapter 5, the authors prove weak compactness results for fluctuations in the case of the Vlasov-Boltzmann equation or Vlasov–Maxwell–Boltzmann system with one species. The authors first derive the relation between the entropy bounds and the entropy dissipative bounds. They present a decomposition of the linearized collision operator and properties of the linear collision operator. The chapter ends with improved integrability results on the velocity for the fluctuations.

In Chapter 6, the authors derive lower-order linear macroscopic constraint equations using weak compactness methods, first for one species then for two species with weak interactions. They prove energy estimates for sequences of renormalized solutions scaled one or two species to Vlasov–

Maxwell–Boltzmann system. The chapter ends with considerations on the difficulty to pass to the limit in Maxwell equations.

In Chapter 7, the authors intend to prove strong compactness results for the fluctuations. They first assume that the collision operator b is smooth and compactly supported and they derive a compactness result with respect to the velocity v. They quote from previous results they obtained locally relatively compact results in $L^p(\mathbb{R}_t \times \mathbb{R}^3_x \times \mathbb{R}^3_v)$, $1 < p < \infty$, for families of functions in this space which satisfy a locally relatively compactness property with respect to v and further properties which allow to use the hypoellipticity property of the free transport equation. The chapter ends with the proof of compactness results for fluctuations in the one or two species cases.

In Chapter 8, the authors consider the case with two species. Using the symmetries of the collision integrands $q^{\pm}$ and $q^{\mp}$, they derive a singular limit for a sequence of renormalized solutions to the scaled Vlasov–Maxwell–Boltzmann system in the case of weak interspecies interactions. They assume that $\delta = o(1)$, δ/ϵ is unbounded and different conditions on the data of the problem. They then characterize the limiting kinetic equations for this case of two species for strong interspecies interactions, assuming that $\delta = 1$ and different conditions on the data. They also characterize the limiting collision integrands and finally the limiting energy inequality in this case.

Chapter 9 investigates the consistency of the electro-magneto-hydrodynamic approximation for the incompressible quasi-static Navier-Stokes–Fourier–Maxwell-Poisson system. The authors consider the admissible nonlinearity

$$\Gamma(z) - 1 = (z-1)\gamma(z) \quad \text{with} \quad \gamma \in C^1([0,\infty);\mathbb{R})$$

satisfying further conditions and they first build approximate conservation laws for the scaled one-species Vlasov–Maxwell–Boltzmann system, considering fluctuations of the kind

$$g_\epsilon \gamma_\epsilon \chi \left(\frac{|v|^2}{K \left|\log \epsilon\right|} \right)$$

where $\chi \in C^\infty_c([0,\infty))$ with $1_{[0,1]} \le \chi \le 1_{[0,2]}$ and $K > 0$ is large enough. They prove that the associated reminders converge to 0 in $L^1_{\mathrm{loc}}(dt; W^{-1,1}_{\mathrm{loc}}(dx))$. They prove that the conservation defects converge to 0 in $L^1_{\mathrm{loc}}(dtdx)$. They finally build approximate conservation of mass, momentum and energy in the case of two species proving estimates and convergence to 0 on the reminders.

In Chapter 10, the authors consider the case of one species and they analyze the time oscillations in the incompressible quasi-static Navier-Stokes–Fourier–Maxwell-Poisson system which allows to derive the weak stability and the convergence of the Vlasov–Maxwell–Boltzmann system as ϵ tends to 0. They introduce the singular linear system

$$\partial_t \begin{pmatrix} \rho_\epsilon \\ u_\epsilon \\ \sqrt{\frac{3}{2}}\theta_\epsilon \\ E_\epsilon \\ B_\epsilon \end{pmatrix} + \frac{1}{\epsilon} W \begin{pmatrix} \rho_\epsilon \\ u_\epsilon \\ \sqrt{\frac{3}{2}}\theta_\epsilon \\ E_\epsilon \\ B_\epsilon \end{pmatrix} = O(1)$$

where $W : L^2(dx) \to H^{-1}(dx)$ is defined through

$$W = \begin{pmatrix} 0 & \mathrm{div} & 0 & 0 & 0 \\ \nabla_x & 0 & \sqrt{\frac{2}{3}}\nabla_x & -Id & 0 \\ 0 & \sqrt{\frac{2}{3}}div & 0 & 0 & 0 \\ 0 & Id & 0 & 0 & -rot \\ 0 & 0 & 0 & rot & 0 \end{pmatrix}.$$

They also introduce the Leray projector $P : L^2(dx) \to L^2(dx)$ onto solenoidal vector fields. The main result of this chapter proves a a weak stability result for acoustic and electromagnetic waves in the sense of distributions for nonlinear terms using the Leray projector, considering a sequence of renormalized solutions to the scaled one species Vlasov–Maxwell–Boltzmann system.

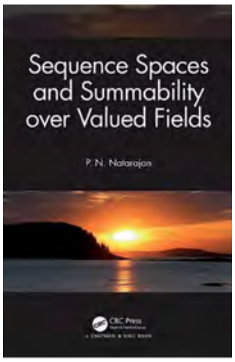
Chapter 11 is devoted to the proof of the result announced in Chapter 4 and concerning the convergence of the renormalized solution to the one species Vlasov–Maxwell–Boltzmann system to a weak solution to the incompressible quasi-static Navier-Stokes–Fourier–Maxwell-Poisson system.

In the final Chapter 12, the authors consider the asymptotics leading to the two-fluid incompressible Navier-Stokes–Fourier–Maxwell system. The main tool is a relative entropy method. They prove the results announced in Chapter 4 first for weak interactions and finally for strong interactions.

Appendix A gives a short analysis of the cross-section for momentum and energy transfer. Appendix B is devoted to the presentation and the properties of Young measures. Appendix C gives short complements to the hypoelliptic transfer of compactness which has been used in Chapter 7.

The book presents deep results concerning the Vlasov–Maxwell–Boltzmann system and of its asymptotics.

Alain Brillard [alain.brillard@uha.fr] is full professor of applied mathematics but since 2000 he is member of the laboratory Gestion des Risques et Environnement (Risk Management and Environment) from the University of Mulhouse. He was President of the University of Mulhouse from 2007 to 2012. His research focused on homogenization and now he mainly works on models of combustion and depollution processes. He published more than 60 articles in international journals, most of them in collaboration with colleagues from Morocco and Russia. He created a research group on applied mathematics with colleagues from the universities of Basel and Freiburg.



P. N. Natarajan
Sequence Spaces and
Summability over Valued Fields

CRC Press , 2020
xxiii, 191 p.
ISBN 978-0-367-23662-5

Reviewer: İbrahim Çanak

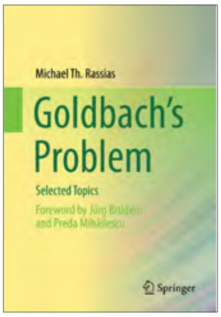
The Newsletter thanks zbMATH and İbrahim Çanak for permission to republish this review, which originally appeared as Zbl 07064156.

Infinite matrix transformations in Archimedean fields have been studied by a number of mathematicians for a long time. However, the study of matrix transformations in non-Archimedean valued fields is of a recent origin. The author of this book has been working in summability theory, especially in matrix transformations and special summability methods in non-Archimedean valued fields, for almost fifty years. It is emphasized in the preface of the book that it is not true that every result in non-Archimedean analysis has a proof analogous to its classical counterpart or even a simpler proof.

This book contains eight important chapters at a research level. Each chapter ends with a detailed bibliography for readers who want to learn the contents in-depth. This book can serve as a reference book for graduate students and research scholars specializing in summability theory, both classical (Archimedean) and ultrametric (non-Archimedean).

The author had two things in mind when writing this book. The first one is to contribute to the literature on sequence spaces and matrix transformations in non-Archimedean analysis. The second one is to illustrate how new proofs are necessary to prove the analogues of classical results. Chapter 1 deals with a brief introduction to non-Archimedean analysis. Chapter 2 considers certain sequence spaces, called Λ_r, containing the space of Cauchy sequences. At the end of the second chapter, a Steinhaus-type theorem has been proved in the classical case. In Chapter 3, it is aimed to characterize the matrix class $(\ell_\alpha, \ell_\alpha)$, $\alpha > 0$, in the non-Archimedean case. Chapter 4 characterizes the regular and Schur matrices. Chapter 5 is devoted to a study of the spaces $c_0(p)$ where $p = (p_n)$ is a positive and bounded sequence. Chapter 6 deals with a study of the spaces $\ell_p, c_0(p), c(p), \ell_\infty(p)$, when K is a complete, non-trivially valued, non-Archimedean field. Chapter 7 gives a characterization of the matrix class (ℓ_∞, c_0), when K is a complete, non-trivially valued, non-Archimedean field. Moreover, the author introduces a suitable definition of summability matrices of type M in such a field K and provides a study of such matrices. Chapter 8 is devoted to several Steinhaus-type theorems in K, where $K = \mathbb{R}$ or $\mathbb{C}$ or a complete, non-trivially valued, non-Archimedean field. The differences in proofs between the classical and non-Archimedean cases are also stated in Chapter 8.

İbrahim Çanak is Professor of Mathematics at Ege University, İzmir, Turkey. He received his PhD in Mathematics from Missouri University of Science and Technology, Rolla, MO, USA in 1998. He has been a member of the Faculty of Sciences at Ege University, Turkey since 2010. His research interest focuses mainly on summability theory and its applications. He has been a referee and/or reviewer for several journals, MathSciNet and zbMATH and is also on the editorial board of several mathematics journals.



Michael Th. Rassias
Goldbach's Problem: Selected
Topics

Springer, 2017.
xv, 122 p.
ISBN 978-3-319-57912-2

Reviewer: Vijay Gupta

The investigation of the behaviour of prime numbers is related to some of the most profound and demanding open problems in mathematics, with the study of their distribution remaining a mystery since the time of the ancient Greeks. Among the most famous riddles in the history of the research related to prime numbers are the Goldbach conjectures. In 1742 Christian Goldbach formulated these famous conjectures in two letters sent to L. Euler. The first conjecture stated that "every even integer can be represented as the sum of two prime numbers" and the second, that "every integer greater than 2 can be represented as the sum of three prime numbers".

As is mentioned in the introduction of the wonderful book by Michael Th. Rassias "Goldbach's Problem: Selected Topics", except for Euler's response to Goldbach, little is known about the interest of the mathematical community in the proof of Goldbach's conjectures before 1900. David Hilbert in his celebrated lecture at the 1900 ICM in Paris, where he posed the 23 now famous problems, included Goldbach's conjectures as a part of Problem 8, entitled: "Problems of Prime Numbers".

This book introduces the reader in a very friendly manner to the study of the Goldbach conjectures and mainly to the investigation of the so-called Ternary Goldbach Conjecture (TGC), which states that:

> *"Every odd integer greater than 5 can be represented as the sum of three prime numbers".*

In 1937 Ivan M. Vinogradov proved by using the Circle Method that all sufficiently large odd integers can be represented as the sum of three prime numbers. This profound result has remained of central importance in the study of the TGC ever since, even after the complete proof of the conjecture by H. Helfgott in 2013.

In the monograph under review, the author presents the Circle Method in a very clear and elaborate way, as well as all other tools necessary for the proof of Vinogradov's Theorem. More specifically, he devotes an important part of the book to a complete step-by-step presentation of this result, making all the complex stages of the investigation of the problem easy to grasp. For the sake of completeness, the author also makes sure to recall central theorems of classical and analytic Number Theory, making the book completely self-contained; a feature rarely seen in monographs devoted to such demanding subjects.

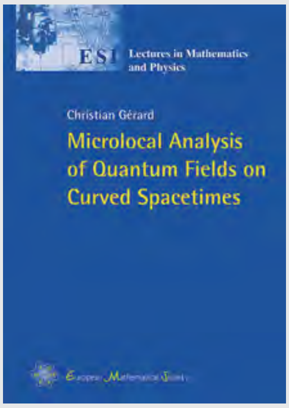
The book gradually progresses to more advanced topics, also including a new research result of the author with Helmut Maier on a version of Vinogradov's theorem under the assumption of the Generalized Riemann Hypothesis. This also makes the book alluring to research mathematicians working on the problem, as well as to advanced graduate students who wish to be introduced to the area.

The final chapter features the basic steps of the proof of Schnirelmann's theorem, which constitutes a combinatorial approach to Goldbach's conjecture. This theorem has the interesting aspect that it provides results which hold true for all natural numbers, not only for large ones.

The book concludes with an Appendix in which the author presents some useful biographical remarks of some of the mathematicians who have greatly contributed to the investigation of the Goldbach conjectures. Finally, another essential addition to the Appendix is Olivier Ramaré's summary of Helfgott's proof of the TGC, thus bringing the reader to the latest frontier of research for the TGC.

Overall, the author masterfully introduces the uninitiated reader to this beautiful but also demanding subject of mathematics in a step-by-step, self-contained manner. Throughout the book, the reader is also lead to explore more advanced aspects of the problems studied. The topics treated, the structure and the presentation of this book are such that it would be excellent for class as well as seminar use.

Vijay Gupta is a professor of Mathematics at Netaji Subhas University of Technology, New Delhi, India. He works in the area of Approximation Theory. He has written over 300 research papers and 5 books.


ESI Lectures in Mathematics and Physics
Christian Gérard
Microlocal Analysis of Quantum Fields on Curved Spacetimes
European Mathematical Society

Solved and Unsolved Problems

Michael Th. Rassias (University of Zürich, Switzerland)

Number theorists are like lotus-eaters
– having tasted this food
they can never give it up.

Leopold Kronecker (1823–1891)

The present column is devoted to Analytic Number Theory. For the previous "Solved and Unsolved Problems" column devoted to Number Theory, the interested reader is referred to the Issue 103, March 2017, of the EMS *Newsletter*.

I Six new problems – solutions solicited

218.
Determine the sum of the series

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{2^n - 1},$$

where φ is the Euler's totient function.

(Dorin Andrica, Babeş-Bolyai University,
Cluj-Napoca, Romania)

219[a]. Let $\omega(n)$ denote the number of distinct prime factors of a non-zero natural number n.

(i) Prove that $\sum_{n\le x} \omega(n) = x \log\log x + \mathcal{O}(x)$.

(ii) Prove that $\sum_{n\le x} \omega(n)^2 = x(\log\log x)^2 + \mathcal{O}(x \log\log x)$.

(iii) Using (i) and (ii), prove that $\sum_{n\le x}(\omega(n) - \log\log x)^2 = \mathcal{O}(x \log\log x)$.

(iv) Using (iii), prove that $\sum_{n\le x}(\omega(n) - \log\log n)^2 = \mathcal{O}(x \log\log x)$.

(v) Using (iv), prove that $\omega(n)$ has normal order $\log\log n$, i.e., for every $\varepsilon > 0$,

$$\#\{n \le x : (1-\varepsilon)\log\log n < \omega(n) < (1+\varepsilon)\log\log n\} \sim x \quad (\text{as } x \to \infty).$$

[a] Parts (i)–(v) of Problem 219 are extracted from a proof by Paul Turán (1910–1976), published in 1934, of a theorem of G. H. Hardy (1877–1947) and S. Ramanujan (1887–1920), published in 1917; see references below:
[1] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number *n*. *Quart. J. Math.* **48** (1917), 76–92.
[2] P. Turán, On a Theorem of Hardy and Ramanujan. *J. London Math. Soc.* **9** (1934), 274–276.

(Alina Carmen Cojocaru, Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, USA, and Institute of Mathematics "Simion Stoilow" of the Romanian Academy, Bucharest, Romania)

220. Using Chebyshev's Theorem, prove that for any integer M there exists an even integer $2k$ such that there are at least M primes p with $p + 2k$ also prime. *Unfortunately $2k$ will depend on M. If it did not, we would have solved the Twin Prime Conjecture, namely, there are infinitely many primes p such that $p + 2$ is also prime.*

(Steven J. Miller, Department of Mathematics & Statistics,
Williams College, Massachusetts, USA)

221. For any three integers a, b, c, with $\gcd(a, b, c) = 1$, prove that there exists an integer m such that

$$0 \le m \le 2^{2^{2002}} c^{\frac{1}{1000}} \text{ and } \gcd(a + mb, c) = 1.$$

(Abhishek Saha, School of Mathematical Sciences,
Queen Mary University of London, UK)

222. Show that

$$\sum_{n=1}^{\infty} \frac{\sin^2(\pi\delta n)}{n^2} = \tfrac{1}{2}\pi^2\delta(1-\delta) \quad \text{for } 0 \le \delta \le 1,$$
$$\sum_{n=1}^{\infty} \frac{\sin^3(\pi\delta n)}{n^3} = \tfrac{1}{2}\pi^3\delta^2(\tfrac{3}{4}-\delta) \quad \text{for } 0 \le \delta \le 1/2,$$
$$\sum_{n=1}^{\infty} \frac{\sin^4(\pi\delta n)}{n^4} = \tfrac{1}{2}\pi^4\delta^3(\tfrac{2}{3}-\delta) \quad \text{for } 0 \le \delta \le 1/2.$$

Setting $\delta = 1/2$, deduce the values of $\zeta(2)$ and $\zeta(4)$.

(Olof Sisask, Department of Mathematics,
Stockholm University, Sweden)

223. Fix a prime number p, and an integer $\beta \ge 2$. Consider the function defined on $x \in \mathbf{R}$ by $e(x) = \exp(2\pi i x)$. Given a coprime residue class r mod p^β, consider the additive character defined on integers $m \in \mathbf{Z}$ by $m \mapsto e\left(\frac{mr}{p^\beta}\right)$. Given a complex parameter $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, consider the Dirichlet series defined by

$$D(s, r, p^\beta) = \sum_{m\ge1} e\left(\frac{rm}{p^\beta}\right) m^{-s}.$$

Show that this series has an analytic continuation to all $s \in \mathbf{C}$, and moreover that it satisfies a functional equation relating values at s to $1 - s$.

(Jeanine Van Order, Fakultät für Mathematik,
Universität Bielefeld, Germany.)

II (A) An Open Problem, by Joseph Najnudel (School of Mathematics, University of Bristol, UK)

Central limit theorems for random multiplicative functions

The distribution of the patterns obtained by taking consecutive values of arithmetic multiplicative functions have been intensively studied. For example, a conjecture by Chowla [2] states that for all $k \geq 1$, each possible sign pattern of

$$(\lambda(n+1), \ldots, \lambda(n+k))$$

appears with asymptotic density 2^{-k}, λ being the Liouville function, i.e.,

$$\lambda(m) = (-1)^{\Omega(m)}$$

where $\Omega(m)$ is the number of prime factors of m, counted with multiplicity. It has been proven by Hildebrand [7] that for $k = 3$, the eight possible values of

$$(\lambda(n+1), \lambda(n+2), \lambda(n+3))$$

appear infinitely often. This result has been improved by Matomäki, Radziwill and Tao [8], who prove that these eight values appear with a positive lower density. Similar results and conjectures are stated for the Möbius function, or for the number of prime factors modulo 3 (see [10]).

In [9], we consider similar questions for consecutive values of random completely multiplicative functions $(X_m)_{m\geq 1}$, such that $(X_p)_{p \text{ prime}}$ are i.i.d. random variables on the unit circle $\mathbb{U}$, and

$$X_m = \prod_{p \text{ prime}} X_p^{\nu_p(m)}$$

where $\nu_p(m)$ is the p-adic valuation of m. In this setting, the law of $(X_m)_{m\geq 1}$ is completely determined by the law of X_2, and we have studied the two following cases in detail: X_2 uniform on the unit circle $\mathbb{U}$, and X_2 uniform on the set $\mathbb{U}_q$ of q-th roots of unity for some integer $q \geq 2$. The randomness we have introduced allows us to prove more precise results than what is known for Liouville or Möbius function, with much more elementary proofs. However, a part of the arguments used in [9] are related to deep results on the number and the size of the solutions of some diophantine equations. The main result of [9] is the proof that the empirical distribution

$$\frac{1}{N}\sum_{n=1}^{N} \delta_{(X_{n+1},\ldots,X_{n+k})} \tag{1}$$

tends almost surely to the uniform distribution on $\mathbb{U}^k$ if X_2 is uniform on $\mathbb{U}$, and to the uniform distribution on $\mathbb{U}_q^k$ if X_2 is uniform on $\mathbb{U}_q$. We also have an estimate on the speed of convergence of the empirical measure: in the case of the uniform distribution on $\mathbb{U}_q$, each of the q^k possible patterns for $(X_{n+1}, \ldots, X_{n+k})$ almost surely occurs with a proportion $q^{-k} + O(N^{-t})$ for n running between 1 and N, for all $t < 1/2$. We have a similar result in the uniform case, if the test functions we consider are sufficiently smooth. These results are deduced, via the Fourier transform of the empirical measure, from the following bound, available for all $(m_1, \ldots, m_k) \neq (0, \ldots, 0)$ if X_2 is uniform on $\mathbb{U}$, and for $m_1, \ldots, m_k$ not all divisible by q if X_2 is uniform on $\mathbb{U}_q$:

$$\mathbb{E}\left[\left|\sum_{n=N'+1}^{N}\prod_{j=1}^{k} X_{n+j}^{m_j}\right|^2\right] \leq O((N-N')N^{\varepsilon}),$$

for $1 \leq N' < N$ and $\varepsilon > 0$, the implied constant depending only on k, ε, and on q if X_2 is uniform on $\mathbb{U}_q$. The bound is obtained from an upper bound of the number of solutions of

$$\frac{\prod_{j=1}^{k}(n_1+j)^{m_j}}{\prod_{j=1}^{k}(n_2+j)^{m_j}} \in \mathcal{A}$$

where $\mathcal{A} = \{1\}$ if X_2 is uniform on $\mathbb{U}$, $\mathcal{A} = (\mathbb{Q}_+^*)^q$ if X_2 is uniform on $\mathbb{U}_q$.

The convergence (1) corresponds to a law of large numbers satisfied by the sums of the form

$$\sum_{n=1}^{N}\prod_{j=1}^{k} X_{n+j}^{m_j}. \tag{2}$$

An open question concerns the existence of a central limit theorem for such sums. To simplify the discussion, let us focus on the case where X_2 is uniform on the unit circle. It is not possible to have a central limit theorem for the sum $\sum_{n=1}^{N} X_n$, because its L^2 norm is equal to n, whereas its L^1 norm is $o(\sqrt{n})$, as recently proven by Harper [3]. This last result is called Helson's conjecture (see [6]), and has been previously discussed in several papers including [4] and [5]. However, central limit theorem may be true for other sums. In [1], Chatterjee and Soundararajan have proven a central limit theorem of sums of the form $\sum_{n=N'+1}^{N} X_n$ when $1 \leq N' < N$ and N' sufficiently close to N. Moreover, in [9], we have quite easily proven the following result: if for all integers $r \geq 1$, the number of non-trivial solutions

$$(n_1, \ldots, n_{2r}) \in \{1, \ldots, N\}^{2r}$$

of the diophantine equation

$$\prod_{j=1}^{r} n_j(n_j+1) = \prod_{j=1}^{r} n_{r+j}(n_{r+j}+1)$$

is negligible with respect to the number of trivial solutions, i.e., $o(N^r)$ when $N \to \infty$, then we have the central limit theorem:

$$\frac{1}{\sqrt{N}}\sum_{n=1}^{N} X_n X_{n+1} \underset{N\to\infty}{\longrightarrow} \frac{\mathcal{N}_1 + i\mathcal{N}_2}{\sqrt{2}}$$

where $\mathcal{N}_1$ and $\mathcal{N}_2$ are two i.i.d. standard Gaussian variables. This fact is obvious for $r = 1$ and we have proven that it is true for $r = 2$. More precisely, we have checked that the number of non-trivial solutions of

$$a(a+1)d(d+1) = b(b+1)c(c+1)$$

where $1 \leq a < b \leq c < d \leq N$ is between $\delta N - 1$ and $N^{3/2+o(1)}$, for an explicit constant $\delta > 0$. We have also proven that the infimum of the ratio d/a for all the solutions is $3 + 2\sqrt{2}$ (this very last result, with elementary but quite difficult solution, may have been suitable for an olympiad problem). We don't know how to generalize our method to $r \geq 3$, or to other sums of the form (2), like

$$\sum_{n=1}^{N} X_n X_{n+1}^{-1}$$

or

$$\sum_{n=1}^{N} X_n X_{n+1} X_{n+2} = \sum_{n=1}^{N} X_{n(n+1)(n+2)}.$$

A natural generalisation of the sums of the form 2, using the multiplicativity of $(X_m)_{m\geq 1}$, gives the following problem.

224*. Open Problem. Let $(X_m)_{m\geq 1}$ be a random completely multiplicative function, such that $(X_p)_{p \text{ prime}}$ are i.i.d., uniform on the unit circle. For which integer-valued polynomials P and Q do we have the central limit theorem:

$$\frac{1}{\sqrt{N}}\sum_{n=1}^{N} X_{P(n)} X_{Q(n)}^{-1} \underset{N\to\infty}{\longrightarrow} \frac{\mathcal{N}_1 + i\mathcal{N}_2}{\sqrt{2}},$$

where $\mathcal{N}_1, \mathcal{N}_2$ are independent standard Gaussian variables? In particular, does this central limt theorem occur for $P(n) = n(n+1)$ and $Q(n) = 1$?

References

[1] S. Chatterjee, K. Soundararajan, Random multiplicative functions in short intervals. *Int. Math. Res. Notices* **2012** (3) (2012), 479–492.

[2] S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*. Gordon and Breach, New York, 1965.

[3] A. Harper, Moments of random multiplicative functions, I: low moments, better than squareroot cancellation, and critical multiplicative chaos. Preprint (2017), arXiv:1703.06654

[4] A. Harper, A. Nikeghbali, M. Radziwill, A note on Helson's conjecture on moments of random multiplicative functions. Preprint. To appear in *Analytic Number Theory* in honor of Helmut Maier's 60th birthday.

[5] W. Heap, S. Lindqvist, Moments of random multiplicative functions and truncated characteristic polynomials. Preprint (2015), arXiv:1505.03378

[6] H. Helson, Hankel Forms. *Studia Math.* **198** (2010), 79–84.

[7] A. Hildebrand, On consecutive values of the Liouville function. *Enseign. Math. (2)* **32** (1986), 219–226.

[8] K. Matomäki, M. Radziwill, T. Tao, Sign patterns of the Liouville and Möbius functions. *Forum of Math., Sigma* **4** (e14) (2016).

[9] J. Najnudel, On consecutive values of random completely multiplicative functions. Preprint (2017), arXiv:1702.01470

[10] T. Tao, J. Teräväinen, Value patterns of multiplicative functions and related sequences. *Forum of Math., Sigma* **7** (e33) (2019).

II (B) An Open Problem, by Joseph H. Silverman (Mathematics Department, Brown University, Providence, RI, USA)

225* A problem in (ostensibly elementary) number theory

Our problem is not new, dating back to a 2004 paper of Ailon and Rudnick [2], but at the same time it is surprisingly new in the sense that one can imagine it appearing in millenia-old mathematical works from Greece, India, or China, since it involves nothing more than powers and greatest common divisors.

The initial version of the problem is simply stated: *Are there infinitely many integers $n \geq 1$ such that*

$$\gcd(2^n - 1, 3^n - 1) = 1\,?$$

It is natural to replace 2 and 3 with arbitrary integers a and b, although a small amount of care is needed to avoid degenerate situations such as $a = b$, and there is the issue that $\gcd(a^n - 1, b^n - 1)$ is always divsiible by $\gcd(a - 1, b - 1)$. With these caveats, a first generalisation asks: *Let $a, b \in \mathbb{Z}$ be non-zero multiplicatively independent integers, i.e., integers such that $a^m b^n \neq 1$ for all $(m, n) \neq (0, 0)$. Are there infinitely many integers $n \geq 1$ such that*

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1)\,?$$

More generally, one may allow a and b to be rational numbers by defining the gcd of two rational numbers to be the gcd of their numerators; and one may take a and b from a number field K by defining

$$\gcd_K(\alpha, \beta) := \gcd(N_{K/\mathbb{Q}}\alpha, N_{K/\mathbb{Q}}\beta) \quad \text{for } \alpha, \beta \in K^*.$$

The best evidence says that there is an affirmative answer in a strong sense for characteristic 0 function fields. To avoid excessive notation, we state the result for polynomials: *Let $a(T), b(T) \in \mathbb{C}[T]$ be polynomials that are multiplicatively independent modulo $\mathbb{C}^*$. Then not only are there infinitely many $n \geq 1$ such that*

$$\gcd\left(a(T)^n - 1, b(T)^n - 1\right) = \gcd\left(a(T) - 1, b(T) - 1\right),$$

but there is also a non-zero polynomial $c(T)$ such that

$$\gcd(a(T)^n - 1, b(T)^n - 1) \text{ divides } c(T) \text{ for all } n \geq 1.$$

The proof by Ailon and Rudnick [2] uses a theorem due variously to Lang, Ihara, Serre and Tate [4], which says that an irreducible algebraic curve in $\mathbb{P}^2$ has only finitely many points with root-of-unity coordinates unless the curve is itself a translate of a torus.

Assuming that the Ailon–Rudnick question has an affirmative answer, it is natural to ask how often the gcd is minimal. The fact that

$$m \mid n \quad \Longrightarrow \quad \gcd(a^m - 1, b^m - 1) \mid \gcd(a^n - 1, b^n - 1)$$

means that the minimal-gcd property for a composite n is contingent on it being true for exponents that are factors of n. This suggests restricting it to prime exponents, which leads to the next question: *What is the densisty (if it exists) of the set*

$$\{p \text{ prime} : \gcd(a^p - 1, b^p - 1) = \gcd(a - 1, b - 1)\}\,?$$

Experiments suggest that the density is large, but they are inconclusive as to whether one should expect density 1, or density $1 - \delta$ for some small $\delta = \delta(a, b) > 0$.

The strong result over function field raises the question of how large $\gcd(2^n - 1, 3^n - 1)$ can be as $n \to \infty$. The function field bound is uniform in n, but there is no such bound for $\mathbb{Q}$, since taking $n = p - 1$ with $p \geq 5$ prime, Fermat's little theorem tells us that $\gcd(2^{p-1} - 1, 3^{p-1} - 1)$ is divisible by p. Thus, any lower bound for $\gcd(2^n - 1, 3^n - 1)$ must grow at least linearly as a function of n, but this is far from the truth, since in fact any lower bound must grow almost exponentially: *There is a constant $C = C(a, b) > 0$ such that*

$$\log \gcd(a^n - 1, b^n - 1) \geq n^{C/\log\log n} \quad \text{for infinitely many } n \geq 1.$$

Bugeaud, Corvaja, and Zannier [3] noted that this follows from an analytic estimate of Adelman–Pomerance–Rumely [1, Proposition 10] that was used to prove the validity of an almost-linear-time primality test.

Thus there exists a subsequence of $\gcd(a^n - 1, b^n - 1)$ that grows almost exponentially in n. This raises the question of whether the growth can be fully exponential. The answer is no, as proven by Bugeaud, Corvaja, and Zannier [3]: *Let $a, b \in \mathbb{Z}$ be non-zero and multiplicatively independent. Then*

$$\lim_{n \to \infty} \frac{\log \gcd(a^n - 1, b^n - 1)}{n} = 0.$$

The proof is an intricate application of Schmidt's subspace theorem, which in turn is a higher-dimensional version of Roth's theorem on Diophantine approximation. As such, it is ineffective, in the sense that one cannot write down an explicit $n_0(\varepsilon)$ such that the fraction in the limit is smaller than ε for all $n \geq n_0(\varepsilon)$. (We mention in passing for function fields over finite fields, e.g., for $a(T), b(T) \in \mathbb{F}_p[T]$, the Bugeaud–Corvaja–Zannier limit is false, even if one restricts n to lie in a fixed congruence class modulo p; see [5].)

In fancier terms, the n-power map is an endomorphism of the multiplicative group, the pair (a, b) is a point in $\mathbb{G}_m^2(\mathbb{Q})$ whose powers are Zariski dense, and $\gcd(a^n - 1, b^n - 1)$ is a measure of the arithmetic distance from $(a, b)^n$ to the identity $(1, 1)$. This viewpoint allows us to reformulate the Ailon–Rudnick question for other (commutative) algebraic groups. Roughly speaking, for any algebraic variety $V/\mathbb{Q}$, we fix a model over $\mathbb{Z}$ and define the arithmetic distance between points $P, Q \in V(\mathbb{Q})$ to be

$$\mathrm{gcd}_V(P,Q) := \prod_{p \text{ prime}} (p\text{-adic distance from } P \text{ to } Q)^{-1}.$$

Then we ask: *Let $G/\mathbb{Q}$ be a semi-abelian variety of dimension at least* 2*, i.e., G is the extension of an abelian variety by a torus, and let $P \in G(\mathbb{Q})$ be a point generating a subgroup $\mathbb{Z}P$ that is Zariski dense in G. Are there infinitely many $n \geq 1$ such that*

$$\mathrm{gcd}_V(nP, O) = \mathrm{gcd}_V(P, O)\,?$$

Specialising to $G = E_1 \times E_2$ a product of elliptic curves, we get questions about $\gcd(A_n, B_n)$, where A_n and B_n are independent elliptic divisibiilty sequences. In this setting, neither the Ailon–Rudnick question nor the analogue of the Bugeaud–Corvaja–Zannier limit is known, although the latter is a consequence of Vojta's conjecture applied to the blow-up of $E_1 \times E_2$ at the identity.

References

[1] Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely, On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)* **117** (1983), 173–206.

[2] Nir Ailon and Zéev Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. *Acta Arith.* **113** (2004), 31–38.

[3] Yann Bugeaud, Pietro Corvaja, and Umberto Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.* **243** (2003), 79–84.

[4] Serge Lang, Division points on curves. *Ann. Mat. Pura Appl. (4)* **70** (1965), 229–234.

[5] Joseph H. Silverman, Common divisors of a^n-1 and b^n-1 over function fields. *New York J. Math.* **10** (2004), 37–43.

III (A) Solutions

211. Recall that a smooth function $u : \mathbf{R}^2 \to \mathbf{R}$ is called harmonic if

$$\Delta u(x,y) := \frac{\partial^2 u}{\partial x^2}(x,y) + \frac{\partial^2 u}{\partial y^2}(x,y) = 0\,, \quad \text{for any } (x,y) \in \mathbf{R}^2.$$

Determine all harmonic polynomials in two real variables.

(Giovanni Bellettini, Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche, Siena, Italia, and ICTP International Centre for Theoretical Physics, Mathematics Section, Trieste, Italy)

Solution by the proposer. Let $P(x,y)$ be a harmonic polynomial of degree $n \geq 0$ in the real variables x and y; since the cases $n = 0$ and $n = 1$ are trivial, we shall assume $n \geq 2$. The first step is to show that we can reduce to the case when the polynomial is homogeneous. Indeed, we can always write P as the sum of its homogeneous components:

$$P = P_0 + \cdots + P_n$$

where, for any $i \in \{0,\ldots,n\}$, the polynomial P_i is homogeneous of degree i, that is

$$P_i(\lambda x, \lambda y) = \lambda^i P_i(x,y)$$

for any $\lambda \in \mathbf{R}$ and any $(x,y) \in \mathbf{R}^2$. Since Δ acts linearly, we have

$$0 = \Delta P = \Delta P_0 + \cdots + \Delta P_n.$$

We observe now that $\Delta P_i = 0$ for any $i = 0,\ldots,n$. Indeed, let $j,k \in \{0,\ldots,n\}$, $2 \leq j < k$, and suppose that $0 = \Delta P_j + \Delta P_k$. Set $\psi_j := \Delta P_j$, $\psi_k := \Delta P_k$. By a direct computation, ψ_j is a $(j-2)$-homogenous polynomial and ψ_k is a $(k-2)$-homogenous polynomial. For any $\lambda \in \mathbf{R}$ and any $(x,y) \in \mathbf{R}^2$ we then have

$$\begin{aligned} 0 &= \psi_j(\lambda x, \lambda y) + \psi_k(\lambda x, \lambda y) = \lambda^{j-2}\psi_j(x,y) + \lambda^{k-2}\psi_k(x,y) \\ &= \lambda^{j-2}(\lambda^{k-j} + 1)\psi_j(x,y). \end{aligned}$$

Since this equality must be valid for any $\lambda \in \mathbf{R}$, we deduce that ψ_j must be identically zero. This observation shows therefore that

$$\Delta P_i = 0 \qquad \forall i \in \{2,\ldots,n\},$$

and hence we can always reduce to the case when our polynomial is n-homogeneous, $n \geq 2$,

$$P_n(x,y) = a_{n,0}x^n + a_{n-1,1}x^{n-1}y + \cdots + a_{1,n-1}xy^{n-1} + a_{0,n}y^n.$$

We have to determine the $n+1$ coefficients $a_{n,0}, a_{n-1,1}, \ldots, a_{1,n-1}, a_{0,n}$ in such a way that $\Delta P_n = 0$. A direct computation shows that the coefficient of the generic monomial $x^j y^k$ of ΔP_n, with $j + k = n - 2$, is given by

$$(j+2)(j+1)a_{j+2,k} + (k+2)(k+1)a_{j,k+2}. \tag{3}$$

Using the expressions in (3), we obtain a homogeneous linear system of $(n-1)$ equations in $(n+1)$ unknowns; it is not difficult to check that the system has (maximal) rank $n-1$. Therefore, the subspace of solutions has dimension two. A possible choice of a basis generating the n-homogeneous harmonic polynomials is given by

$$\mathrm{Re}(z^n) = \sum_{\substack{k=0,\ldots,n \\ k \text{ even}}} \binom{n}{k} (-1)^{\frac{k}{2}} x^{n-k} y^k, \quad \mathrm{Im}(z^n) = \sum_{\substack{k=0,\ldots,n \\ k \text{ odd}}} \binom{n}{k} (-1)^{\frac{k-1}{2}} x^{n-k} y^k,$$

where $z = x + iy \in \mathbb{C}$. Indeed, it is sufficient to check that $\mathrm{Re}(z^n)$ and $\mathrm{Im}(z^n)$ do not have proportional coefficients, and to recall that $z \in \mathbb{C} \to z^n \in \mathbb{C}$ is entire holomorphic, so that $\mathrm{Re}(z^n)$ and $\mathrm{Im}(z^n)$ are harmonic in $\mathbb{R}^2$. □

Also solved by Sotirios E. Louridas (Athens, Greece), George Milikakos (Sparta, Greece) and Socratis Varelogiannis (France)

212 Reaction-diffusion systems of the form

$$u_t = Du_{xx} + g(u) + \mu Mu, \qquad (x,t) \in \mathbb{R} \times (0,\infty),$$

where

$$u(x,t) \in \mathbb{R}^n,\ g_i(u) = r_i u_i \left(1 - \sum_{j=1}^{n} \alpha_j u_j\right),\ r_i, \alpha_i > 0,$$
$$i = 1,\ldots,n,\ \mu > 0,$$

and D and M are constant $n \times n$ matrices such that D is positive-definite diagonal and M has strictly positive off-diagonal elements and zero column sums, arise in the modelling of the population densities of n phenotypes of a species that diffuse, compete both within a phenotype and with other phenotypes, and may mutate from one phenotype to another. Denoting the Perron-Frobenius eigenvalue of a matrix Q by $\eta_{PF}[Q]$ and assuming that the n phenotypes spread together into an unoccupied spatial region at the

μ-dependent speed

$$c(\mu) := \inf_{\beta>0} \eta_{PF}\Big[\beta D + \beta^{-1}(\mathrm{diag}(r_1, \dots, r_n) + \mu M)\Big],$$

which is determined by the linearisation of the reaction-diffusion system about the extinction steady state $u = (0, \dots, 0) \in \mathbb{R}^n$, prove that spreading speed $c(\mu)$ is a non-increasing function of μ.

(Elaine Crooks, Department of Mathematics,
College of Science, Swansea University,
Swansea, UK)

Solution by the proposer. Let $\mu > \mu_0 > 0$, denote the zero $n{\times}n$ matrix by Z, and define

$$P := \bar\beta^2 D + \mathrm{diag}(r_1, \dots, r_n) - c(\mu_0)I,$$

where $\bar\beta$ is such that the infimum in the definition of $c(\mu_0)$ is attained at $\beta = \bar\beta$. Then

$$\begin{aligned}\eta_{PF}[P + \mu_0 M] &= \bar\beta\, \eta_{PF}\Big[\bar\beta D + \bar\beta^{-1}(\mathrm{diag}(r_1, \dots, r_n) + \mu_0 M) - c(\mu_0)I\Big]\\ &= 0,\end{aligned}$$

and by the convexity of the Perron-Frobenius eigenvalue of a matrix on its diagonal,

$$\begin{aligned}\eta_{PF}\left[\frac{1}{\mu}P + M\right] &\le \frac{\mu_0}{\mu}\eta_{PF}\left[\frac{1}{\mu_0}P + M\right] + \left(1 - \frac{\mu_0}{\mu}\right)\eta_{PF}[Z + M]\\ &= \frac{\mu_0}{\mu}\eta_{PF}\left[\frac{1}{\mu_0}P + M\right] + \left(1 - \frac{\mu_0}{\mu}\right)\eta_{PF}[M]\\ &= 0,\end{aligned}$$

since

$$\eta_{PF}[M] = 0 \quad \text{and} \quad \eta_{PF}\left[\frac{1}{\mu_0}P + M\right] = \frac{1}{\mu_0}\eta_{PF}[P + \mu_0 M] = 0.$$

Hence

$$\eta_{PF}[P + \mu M] \;\le\; 0,$$

which says that,

$$\eta_{PF}\Big[\bar\beta D + \bar\beta^{-1}(\mathrm{diag}(r_1, \dots, r_n) + \mu M)\Big] \le c(\mu_0),$$

and so

$$c(\mu) := \min_{\beta>0} \eta_{PF}\Big[\beta D + \beta^{-1}(\mathrm{diag}(r_1, \dots, r_n) + \mu M)\Big] \;\le\; c(\mu_0).$$

□

Also solved by Mihály Bencze (Brasov, Romania), Jim Kelesis (Athens, Greece), Sotirios E. Louridas (Athens, Greece), George Miliakos (Sparta, Greece)

213. Consider the second-order PDE with non-constant coefficients,

$$u_{xx} - x^2 u_{yy} = 0.$$

Find at least one family of solutions.

(Jonathan Fraser, School of Mathematics and Statistics,
The University of St Andrews, Scotland)

Solution by the proposer. In the general form of a second-order PDE,

$$a(x, y)u_{xx} + 2b(x, y)u_{xy} + c(x, y)u_{yy} = 0,$$

we have $a = 1$, $b = 0$ and $c = -x^2$. Hence, the discriminant $b^2 - ac = x^2$ implying that the equation is *hyperbolic* for $x \neq 0$. The characteristic curves are given by

$$\frac{dy}{dx} = \frac{b}{a} \pm \frac{1}{a}\sqrt{b^2 - ac} = \pm x, \qquad \Longrightarrow \qquad y = \pm\frac{1}{2}x^2 + \text{ constant.}$$

So the characteristic coordinates are

$$\xi = y + \frac{1}{2}x^2, \qquad \eta = y - \frac{1}{2}x^2$$

noting

$$\xi_x = x, \quad \xi_y = 1, \quad \eta_x = -x, \quad \eta_y = 1.$$

Hence,

$$\begin{aligned}u_x &= xu_\xi - xu_\eta,\\ u_{xx} &= \Big[x(u_\xi - u_\eta)\Big]_x\\ &= (u_\xi - u_\eta) + x(u_\xi - u_\eta)_x\\ &= (u_\xi - u_\eta) + x^2(u_{\xi\xi} - 2u_{\xi\eta} + u_{\eta\eta})\\ u_y &= u_\xi + u_\eta,\\ u_{yy} &= u_{\xi\xi} + 2u_{\xi\eta} + u_{\eta\eta}.\end{aligned}$$

Substituting into $u_{xx} - x^2 u_{yy} = 0$, we obtain

$$-4x^2 u_{\xi\eta} + (u_\xi - u_\eta) = 0 \qquad \Longrightarrow \qquad u_{\xi\eta} = \frac{(u_\xi - u_\eta)}{4x^2}.$$

Finally, we must replace the x in the equation by ξ and η. From their definitions, we have

$$\xi - \eta = x^2,$$

and so the canonical form of the equation is

$$u_{\xi\eta} = \frac{(u_\xi - u_\eta)}{4(\xi - \eta)}.$$

It turns out that this equation can be solved by assuming a solution of the form

$$u(\xi, \eta) = f(\xi\eta) = f(t),$$

with $t = \xi\eta$. Differentiating gives

$$u_\xi = \eta f', \qquad u_\eta = \xi f', \qquad u_{\xi\eta} = f' + \xi\eta f''.$$

When these are substituted into the canonical form of the equation, it reduces (greatly) to a single first-order ODE for $g = f'$,

$$4tg' + 5g = 0,$$

which can be solved and integrated to give

$$f = A(\xi\eta)^{-1/4} + B.$$

Therefore the solution in terms of the original x, y variables is

$$u = A\Big[\Big(y + \tfrac{1}{2}x^2\Big)\Big(y - \tfrac{1}{2}x^2\Big)\Big]^{-1/4} + B = A\Big(y^2 - \tfrac{1}{4}x^4\Big)^{-1/4} + B.$$

This can be verified by direct differentiation. A solution exists only in the regions above $y = \frac{1}{2}x^2$ or below $y = -\frac{1}{2}x^2$, i.e., above and below the characteristics $\xi = 0$ and $\eta = 0$ emanating from $(0, 0)$, as shown in Figure 1.

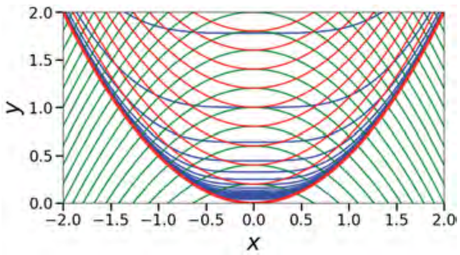


Figure 1. Illustration of the solution to the (almost) hyperbolic PDE $u_{xx} - x^2 u_{yy} = 0$. The blue curves show lines of constant u (equally spaced in value). Note $u \to \infty$ approaching the critical characteristic $y = \frac{1}{2}x^2$ (the thick red curve). The characteristics $y = \xi - \frac{1}{2}x^2$ are shown in green, and the characteristics $y = \eta + \frac{1}{2}x^2$ are shown in red (for $\eta \geq 0$). Note that the characteristics and solution curves are tangent along $x = 0$ where the PDE is parabolic.

Note, there are in fact many other solutions. One for example is

$$u = a(\xi + \eta) = 2ay.$$

Another is

$$u = a(\xi^2 + \eta^2) + b\xi\eta$$

so long as $b = 2a/5$. In the coordinates x and y, this solution is

$$u(x, y) = \frac{2a}{5}(6y^2 + x^4)\,.$$

Infinitely many other analogous solutions can be constructed assuming

$$u(\xi, \eta) = \sum_{j=0}^{n} a_j \xi^{n-j}\eta^j\,,$$

for all $n > 0$, and with $a_{n-j} = a_j$ for all j. It is just a matter of plugging this form into the PDE and determining relations among the coefficients a_j. □

Also solved by Mihály Bencze (Brasov, Romania), Sotirios E. Louridas (Athens, Greece), George Miliakos (Sparta, Greece) and Socratis Varelogiannis (France)

214. Let u solve

$$(\Delta + 200^2 xy^2)u = 1$$

on the triangle $T = \{(x, y) : 0 < x < 1, 0 < y < 1 - x\}$ with zero Dirichlet conditions:

$$u(x, 0) = u(0, y) = u(x, 1 - x) = 0.$$

What are the first 10 significant digits of $u(0.1, 0.2)$?

(Sheehan Olver, Department of Mathematics,
Imperial College, London, UK)

Solution by the proposer.

$$-0.00321203523532$$

should be accurate to 12 digits of relative accuracy.

This problem is motivated by a similar question recently posed by A. Gopal and L. N. Trefethen on NADigest, 3 Dec 2018:

> Let the domain be the L-shaped region in the (x, y)-plane consisting of $[0, 2]\times[0, 2]$ minus its upper-right quarter. If u is harmonic in this region with $u = x^2$ on the boundaries, what is $u(.99, .99)$ to 8 digits?

The difficulty is that the solution has weak singularities at the corners, which limits accuracy of most numerical methods. They proposed a solution based on using fundamental solutions with cleverly chosen spacing near the corners [6], but this technique is not immediately adaptable to Problem 1, where the fundamental solutions are not known in closed form. Furthermore, the large factor introduces oscillations into the solution and ill-conditioning into standard discretisations that make the problem challenging.

To solve Problem 1 we use a recently introduced method [3], where we represent the solution in orthogonal polynomials on the triangle and construct a sparse representation of the partial differential operator. This is close to prior work on p-finite element methods [1, 5], but with the added benefit of sparsity for variable coefficients. This sparsity allows us to use very high order approximations and thereby resolve the solution to high accuracy, despite the corner singularities and oscillations.

In detail, define

$$P_{n,k}^{(a,b,c)}(x, y) := P_{n-k}^{(2k+b+c+1,a)}(2x - 1)(1 - x)^k P_k^{(b,c)}(2y/(1 - x) - 1)$$

which are orthogonal with respect to the weight $x^a y^b (1 - x - y)^c$ on T (cf. for example [2]) and write

$$u(x, y) \approx u_N(x, y) = xyz \sum_{n=0}^{N}\sum_{k=0}^{n} u_{n,k}^N P_{n,k}^{(1,1,1)}(x, y)$$

where $z := 1 - x - y$ and the coefficients $u_{n,k}^N$ are to be determined. The action of the Laplacian on this basis can be deduced in closed form by employing recurrence relationships for the orthogonal polynomials [4]. That is, the following recurrences (which follow from manipulation of 1D Jacobi polynomial relationships) can be combined to express $\frac{\mathrm{d}^2}{\mathrm{d}x^2}\Big(xyzP_{n,k}^{(1,1,1)}\Big)$ in terms of $P_{n,k}^{(1,1,1)}$:

$$\begin{aligned}
-(2k+3)\frac{\mathrm{d}}{\mathrm{d}x}\Big(xyzP_{n,k}^{(1,1,1)}\Big) &= y\Big((k+1)(n-k+1)P_{n+1,k}^{(0,1,0)} \\
&\qquad + (k+1)(n-k+1)P_{n+1,k+1}^{(0,1,0)}\Big),\\
(2k+2)(2n+3)yP_{n,k}^{(0,1,0)} &= (k+1)(n+k+2)P_{n,k}^{(0,0,0)}\\
&\quad - (k+1)(n-k)P_{n,k+1}^{(0,0,0)}\\
&\quad - (k+1)(n-k+1)P_{n+1,k}^{(0,0,0)}\\
&\quad + (k+1)(n+k+3)P_{n+1,k+1}^{(0,0,0)},\\
(2k+1)\frac{\mathrm{d}}{\mathrm{d}x}P_{n,k}^{(0,0,0)} &= (n+k+2)(k+1)P_{n-1,k}^{(1,0,1)},\\
(2n+4)(2k+2)P_{n,k}^{(1,0,1)} &= (n+k+4)(k+2)P_{n,k}^{(1,1,1)}\\
&\quad - (n-k+1)(k+2)P_{n-1,k}^{(1,1,1)}\\
&\quad + (k+1)(n+k+2)P_{n-1,k-1}^{(1,1,1)}\\
&\quad - (k+1)(n-k+1)P_{n,k-1}^{(1,1,1)}.
\end{aligned}$$

The following can be combined to express $\frac{\mathrm{d}^2}{\mathrm{d}y^2}\Big(xyzP_{n,k}^{(1,1,1)}\Big)$ also in terms of $P_{n,k}^{(1,1,1)}$:

$$\begin{align}
\frac{\mathrm{d}}{\mathrm{d}y}\Big(xyzP_{n,k}^{(1,1,1)}\Big) &= -(k+1)xP_{n+1,k+1}^{(1,0,0)}, \notag\\
(2n+3)xP_{n,k}^{(1,0,0)} &= (n-k+1)\Big[P_{n,k}^{(0,0,0)} + P_{n+1,k}^{(0,0,0)}\Big], \tag{4}\\
\frac{\mathrm{d}}{\mathrm{d}y}P_{n,k}^{(0,0,0)} &= (k+1)P_{n-1,k-1}^{(0,1,1)}, \notag\\
(2n+4)P_{n,k}^{(0,1,1)} &= (n+k+4)P_{n,k}^{(1,1,1)} + (n+k+3)P_{n-1,k}^{(1,1,1)}. \tag{5}
\end{align}$$

Thus $\Delta\Big(xyzP_{n,k}^{(1,1,1)}\Big)$ has a sparse expansion in $P_{n,k}^{(1,1,1)}$, which can be found in closed form.

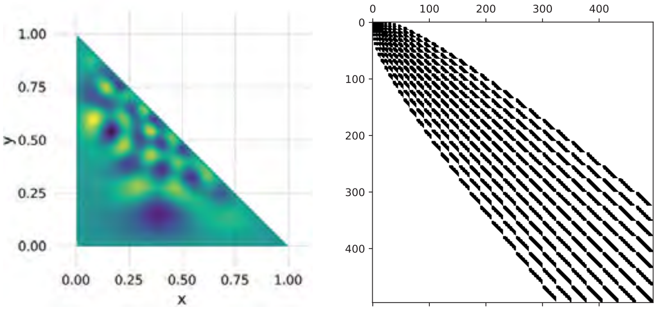


Figure 2. The solution (left). The sparsity of the discretisation L^N for $N = 30$ (right).

We similarly can construct a sparse expression for multiplication by xy^2, using the following:

$$\begin{aligned}
(2n+5)xP^{(1,1,1)}_{n,k} &= (n-k+1)P^{(0,1,1)}_{n,k} + (n-k+1)P^{(0,1,1)}_{n+1,k},\\
(2n+4)P^{(0,1,1)}_{n,k} &= (n+k+4)P^{(1,1,1)}_{n,k} + (n+k+3)P^{(1,1,1)}_{n-1,k},\\
(2k+3)(2n+5)yP^{(1,1,1)}_{n,k} &= (k+1)(n+k+3)P^{(1,0,1)}_{n,k}\\
&\quad - (k+1)(n-k+1)P^{(1,0,1)}_{n,k+1}\\
&\quad - (k+1)(n-k+1)P^{(1,0,1)}_{n+1,k}\\
&\quad + (k+1)(n+k+5)P^{(1,0,1)}_{n+1,k+1},\\
(2n+4)(2k+2)P^{(1,0,1)}_{n} &= (n+k+4)(k+2)P^{(1,1,1)}_{n,k}\\
&\quad - (n-k+1)(k+2)P^{(1,1,1)}_{n-1,k}\\
&\quad + (k+1)(n+k+2)P^{(1,1,1)}_{n-1,k-1}\\
&\quad - (k+1)(n-k+1)P^{(1,1,1)}_{n,k-1},\\
(2k+3)(2n+5)zP^{(1,1,1)}_{n,k} &= (k+1)(n+k+3)P^{(1,1,0)}_{n,k}\\
&\quad + (k+1)(n-k+1)P^{(1,1,0)}_{n,k+1}\\
&\quad - (k+1)(n-k+1)P^{(1,1,0)}_{n+1,k}\\
&\quad - (k+1)(n+k+5)P^{(1,1,0)}_{n+1,k+1},\\
(2n+4)(2k+2)P^{(1,1,0)}_{n} &= (n+k+4)(k+2)P^{(1,1,1)}_{n,k}\\
&\quad - (n-k+1)(k+2)P^{(1,1,1)}_{n-1,k}\\
&\quad - (k+1)(n+k+2)P^{(1,1,1)}_{n-1,k-1}\\
&\quad + (k+1)(n-k+1)P^{(1,1,1)}_{n,k-1}.
\end{aligned}$$

Recurrence relationships induce an operator on matrix coefficients, that is, there exists a block $(N+6)\times N$ matrix L^N so that

$$\begin{aligned}
\Delta u_N(x,y) &= \Delta\left[xyz\left(P^{(1,1,1)}_{0,0}, P^{(1,1,1)}_{1,0}, \ldots, P^{(1,1,1)}_{N,N}\right)\begin{pmatrix} u^N_{0,0}\\ \vdots \\ u^N_{N,N}\end{pmatrix}\right]\\
&= \left(P^{(1,1,1)}_{0,0}, P^{(1,1,1)}_{1,0}, \ldots, P^{(1,1,1)}_{N+1,N+1}\right)L^N\begin{pmatrix} u^N_{0,0}\\ \vdots \\ u^N_{N,N}\end{pmatrix}
\end{aligned}$$

Using this we arrive at a linear system:

$$L^N \boldsymbol{u}^N = \boldsymbol{e}_0$$

where $\boldsymbol{u}^N$ is best interpreted as a block-vector with blocks $\boldsymbol{u}^N_n = \left(u^N_{n,0}, \ldots, u^N_{n,n}\right)^\top$, and L^N is a block-matrix whose entries are determined by $\Delta\left(xyzP^{(1,1,1)}_{n,k}\right)$ using the recurrences. This is a sparse linear system, see the right-hand side of Figure 1, and can be solved efficiently, either in $O(N^4)$ operations using a block-QR decomposition or in $O(N^3)$ operations using sparse direct methods, as implemented in UMFPack. The result was determined using $N = 1000$, which matched the calculation with $N = 999$ to an absolute accuracy of 5.5×10^{-17}. □

References

[1] Beuchler, S., Schoeberl, J., New shape functions for triangular p-FEM using integrated Jacobi polynomials. *Numer. Math.* **103** (2006), 339–366.

[2] Dunkl, C. F., Xu, Y., *Orthogonal Polynomials of Several Variables*. Cambridge University Press, 2014.

[3] Olver, S., Townsend, A., Vasil, G., A sparse spectral method on triangles. Preprint arXiv:1902.04863, 2019.

[4] Olver, S., Townsend, A., Vasil, G., Recurrence relations for orthogonal polynomials on a triangle. ICOSAHOM 2018, to appear.

[5] Li, H., Shen, J., Optimal error estimates in Jacobi-weighted Sobolev spaces for polynomial approximations on the triangle. *Maths Comp.* **79** (2010), 1621–1646.

[6] Gopal, A., Trefethen, L. N., New Laplace and Helmholtz solvers. *Proc. Nat. Acad. Sci.*, **116** (2019), 10223–10225.

Also solved by Mihály Bencze (Brasov, Romania) and Socratis Varelogiannis (France)

215. Let u be an entire harmonic function in $\mathbf{R}^n$, satisfying $u(x) \geq -c(1+|x|^m)$ for some constants $c > 0$ and $m \in \mathbb{N}$. Show that u is a polynomial of degree less or equal to m.

(Gantumur Tsogtgerel, McGill University,
Department of Mathematics and Statistics,
Montreal, Canada)

Solution by the proposer. Let us first derive an upper bound on u. To this end, let $r > 0$ and let

$$v(x) = u(x) + c(1 + r^m).$$

Then v is harmonic, and $v \geq 0$ in $B(0,r)$, where $B(0,r) \subset \mathbf{R}^n$ is the closed ball of radius $r > 0$, centred at the origin. Now, pick $x \in \mathbf{R}^n$ with $|x| = r/2$, and invoke the mean value property to get

$$v(0) = \frac{1}{|B(0,r)|}\int_{B(0,r)} v \geq \frac{1}{|B(0,r)|}\int_{B(x,r/2)} v = \frac{|B(x,r/2)|}{|B(0,r)|}v(x),$$

where $B(x,r/2)$ is the closed ball of radius $r/2$, centred at x. This yields

$$u(x) \leq v(x) \leq 2^n v(0) = 2^n(u(0) + c + cr^m),$$

and since r was arbitrary, we conclude

$$u(x) \leq 2^n(u(0) + c + c2^m|x|^m), \qquad c \in \mathbf{R}^n.$$

Combining it with the lower bound $u(x) \geq -c(1+|x|^m)$, we infer

$$|u(x)| \leq A + B|x|^m,$$

for some constants A and B. Finally, the standard derivative estimate

$$|\partial^\alpha u(x)| \leq \frac{M(n,|\alpha|)}{r^{|\alpha|}}\sup_{B(x,r)}|u|,$$

for harmonic functions finishes the job. □

Also solved by Mihály Bencze (Brasov, Romania), John N. Daras (Athens, Greece), and Jim Kelesis (Athens, Greece)

216. Let $f : [0, \infty) \to (0, \infty)$ be a continuous function satisfying $f(x) \to 0$ as $x \to \infty$, and let

$$\Omega = \{(x, y) \in \mathbf{R}^2 : x > 0,\ 0 < y < f(x)\}.$$

Exhibit an unbounded function u in Ω, such that $u \in H^k(\Omega)$ for all $k \geq 0$. Here $H^k(\Omega)$ is the standard Sobolev space of functions whose partial derivatives of all orders up to k are square integrable.

(Gantumur Tsogtgerel, McGill University,
Department of Mathematics and Statistics,
Montreal, Canada)

Solution by the proposer. Fix a nontrivial smooth "bump" function $\varphi : \mathbf{R} \to [0, \infty)$, supported in the interval $(0, 1)$, and let

$$u(x, y) = \sum_{n=1}^{\infty} n\varphi(x - a_n), \qquad (x, y) \in \Omega,$$

where $\{a_n\}$ is an increasing sequence of numbers, to be determined below. It is clear that u is well-defined and unbounded as long as $\{a_n\}$ grows sufficiently fast.

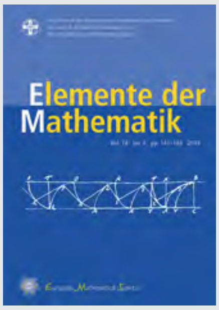
Let us compute the L^2-norm of u. Assuming that $\{a_n\}$ grows sufficiently fast, we have

$$\int_\Omega |u|^2 = \sum_{n=1}^{\infty} n \int_{a_n}^{a_n+1} f(x)|\varphi(x-a_n)|^2 dx = \sum_{n=1}^{\infty} n \int_0^1 f(t+a_n)|\varphi(t)|^2 dt,$$

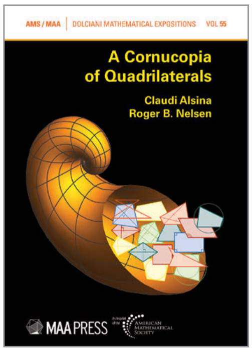
which will be finite if we choose, e.g., a_n so large that $f(x) < n^{-3}$ for all $x > a_n$. It is not difficult to see that the same condition works for the derivatives as well. □

Also solved by Mihály Bencze (Brasov, Romania), John N. Daras (Athens, Greece) and Socratis Varelogiannis (France)

We would like for you to submit solutions to the proposed problems and ideas on the open problems. Send your solutions by email to Michael Th. Rassias, Institute of Mathematics, University of Zürich, Switzerland, michail.rassias@math.uzh.ch.
We also solicit your new problems with their solutions for the next "Solved and Unsolved Problems" column, which will be devoted to *Algebra*.



AMERICAN
MATHEMATICAL
SOCIETY


AMS / MAA | DOLCIANI MATHEMATICAL EXPOSITIONS VOL 55
A Cornucopia of Quadrilaterals
Claudi Alsina
Roger B. Nelsen
MAA PRESS

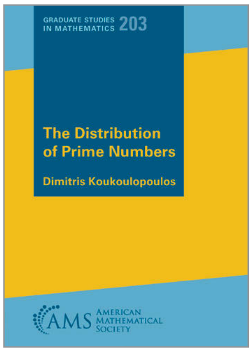
A CORNUCOPIA OF QUADRILATERALS

Claudi Alsina, Universitat Politècnica de Catalunya & Roger B. Nelsen, Lewis & Clark College

Collects and organises hundreds of beautiful and surprising results about four-sided figures. The book contains hundreds of challenging four-sided problems. Instructors of number theory, combinatorics, analysis, and geometry will find examples and problems to enrich their courses.

Dolciani Mathematical Expositions, Vol. 55
MAA Press

Mar 2020 304pp 9781470453121 Hardback €66.00


GRADUATE STUDIES IN MATHEMATICS 203
The Distribution of Prime Numbers
Dimitris Koukoulopoulos
AMS AMERICAN MATHEMATICAL SOCIETY

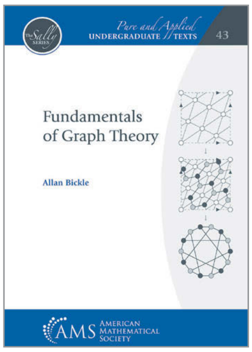
THE DISTRIBUTION OF PRIME NUMBERS

Dimitris Koukoulopoulos, Université de Montréal

Prime numbers have fascinated mathematicians since the time of Euclid. This book presents some of our best tools to capture the properties of these fundamental objects, beginning with the most basic notions of asymptotic estimates and arriving at the forefront of mathematical research.

Graduate Studies in Mathematics, Vol. 203

Jan 2020 356pp 9781470447540 Hardback €95.00


Pure and Applied UNDERGRADUATE TEXTS 43
Fundamentals of Graph Theory
Allan Bickle
AMS AMERICAN MATHEMATICAL SOCIETY

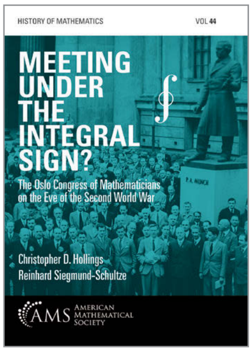
FUNDAMENTALS OF GRAPH THEORY

Allan Bickle, Pennsylvania State University Altoona

Graph theory is a fascinating and inviting branch of mathematics. The goal of this textbook is to present the fundamentals of graph theory to a wide range of readers. The author has included the shortest, most elegant, most intuitive proofs for modern and classic results while frequently presenting them in new ways.

Pure and Applied Undergraduate Texts, Vol. 43

Apr 2020 336pp 9781470453428 Hardback €95.00


HISTORY OF MATHEMATICS VOL 44
MEETING UNDER THE INTEGRAL SIGN?
The Oslo Congress of Mathematicians on the Eve of the Second World War
Christopher D. Hollings
Reinhard Siegmund-Schultze
AMS AMERICAN MATHEMATICAL SOCIETY

MEETING UNDER THE INTEGRAL SIGN?

The Oslo Congress of Mathematicians on the Eve of the Second World War

Christopher D. Hollings, Mathematical Institute and Queen's College, University of Oxford & Reinhard Siegmund-Schultze, University of Agder

Examines the historically unique conditions under which the International Congress of Mathematicians took place in Oslo in 1936. Relying heavily on unpublished archival sources, the authors consider the different goals of the various participants in the Congress, most notably those of the Norwegian organizers, and the Nazi-led German delegation.

History of Mathematics, Vol. 44

Apr 2020 362pp 9781470443535 Hardback €134.00

Free delivery at **eurospanbookstore.com/ams**

AMS is distributed by EUROSPAN

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@eurospan.co.uk