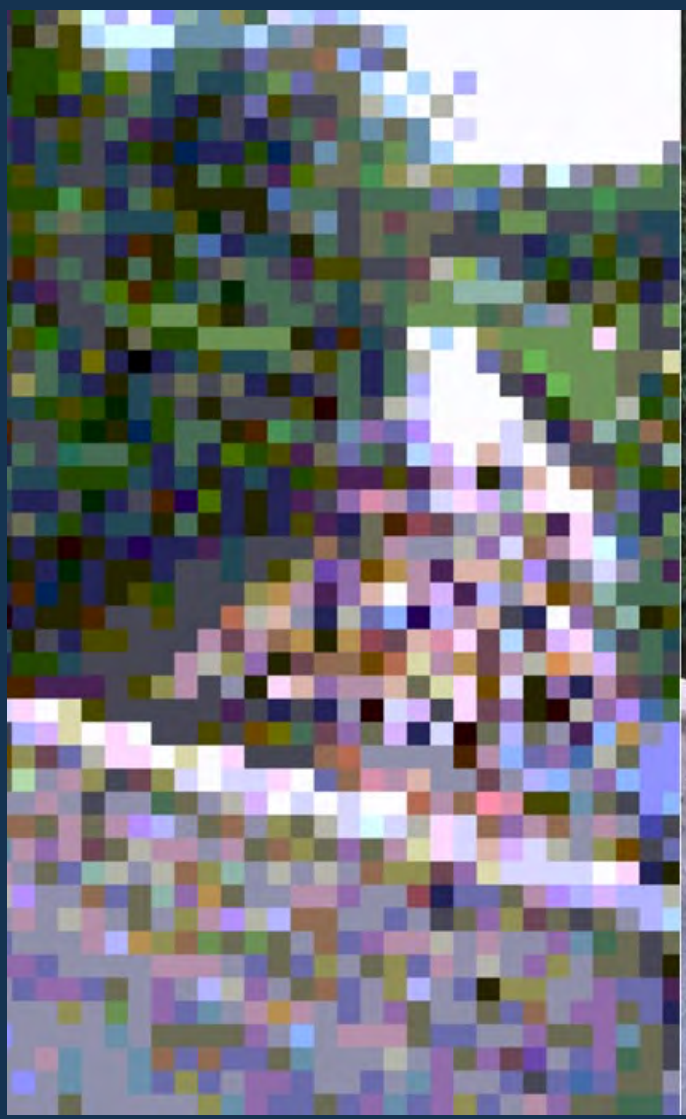
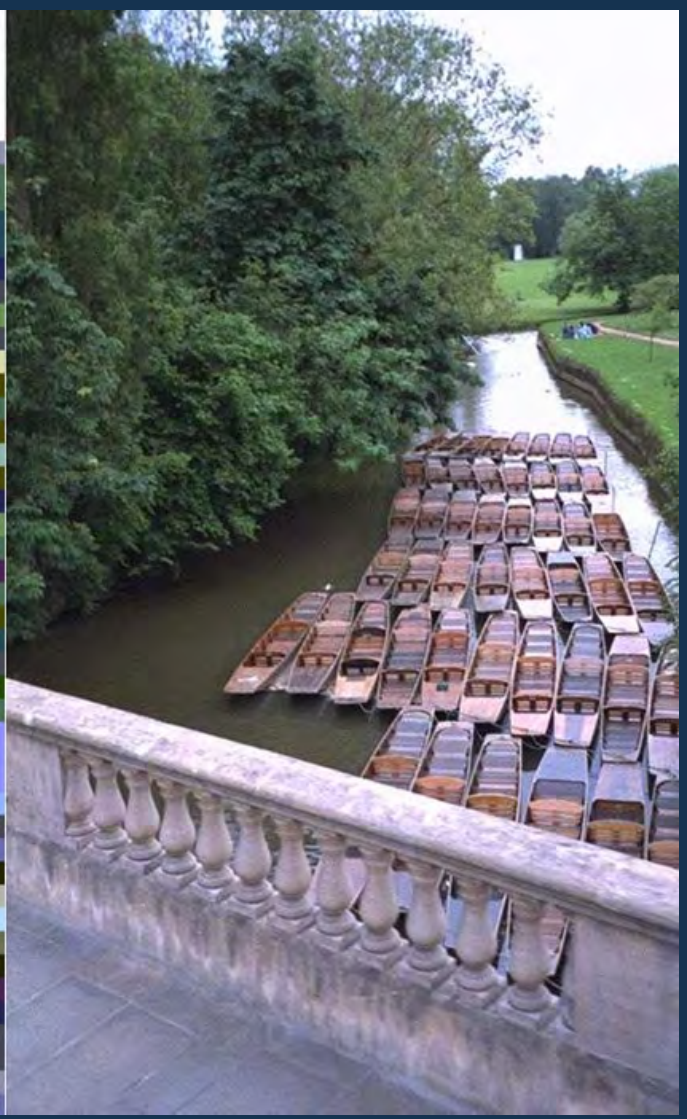
LONDON MATHEMATICAL SOCIETY
EST. 1865

NEWSLETTER

Issue: 510 - February 2024





AUTONOMOUS ROBOTS & ALGEBRAIC GEOMETRY

PREVENTING THE QUANTUM CRYPTO APOCALYPSE

NOTES OF A NUMERICAL ANALYST

EDITORIAL OFFICE

London Mathematical Society
De Morgan House
57–58 Russell Square
London WC1B 4HS
newsletter@lms.ac.uk

Charity registration number: 252660

COVER IMAGE

Cover image: a pair of images of punts under Magdalen Bridge, Oxford, illustrating the theme of discrete and continuous in the *Notes of a Numerical Analyst* column (page 32). On the left, 32x48 pixels, and on the right, 512x768.

Do you have an image of mathematical interest that may be included on the front cover of a future issue? Email images@lms.ac.uk for details.

ISSN: 2516-3841 (Print)
ISSN: 2516-385X (Online)
DOI: 10.1112/NLMS

NEWSLETTER WEBSITE

The Newsletter is freely available electronically at lms.ac.uk/publications/lms-newsletter.

MEMBERSHIP

Joining the LMS is a straightforward process. For membership details see lms.ac.uk/membership.

SUBMISSIONS

The Newsletter welcomes submissions of feature content, including mathematical articles, career related articles, and microtheses from members and non-members. Submission guidelines and LaTeX templates can be found at lms.ac.uk/publications/submit-to-the-lms-newsletter.

Feature content should be submitted to the editor-in-chief at newsletter.editor@lms.ac.uk.

News items should be sent to newsletter@lms.ac.uk.

Notices of events should be prepared using the template at lms.ac.uk/publications/lms-newsletter and sent to calendar@lms.ac.uk.

For advertising rates and guidelines see lms.ac.uk/publications/advertise-in-the-lms-newsletter.

CONTENTS

LMS Strategy 2023–28

Council holds a strategic retreat every two years to review progress of delivering the charitable objectives of the Society and discuss the implications of strategic internal and external changes the Society faces. The current charitable objectives for the Society were agreed in January 2006 and have been used since to define the activities and work the Society undertakes to deliver its mission. The charitable objectives are an interpretation of the objectives in the Society's Royal Charter of 1965.

At a strategic retreat In April 2023, Council reviewed the objectives and agreed on areas of focus for the next five years. Council agreed that the charitable objectives remain a clear articulation of the Society's mission, but that they should be updated to include equity, diversity & inclusion, and sustainability. The retreat collectively concluded that the areas of focus for the next five years should be:

- LMS in the global community: play an active role in the international mathematical community and develop our international partnerships and our membership, building on the global reputation of the Society.
- Pathways in mathematics: promote the importance of mathematics and the provision of opportunities for those who wish to study and develop a career in research mathematics and its applications.
- Engaging our community: mobilise and connect with current and potential LMS members and the wider mathematics community.

These goals are underpinned by the Society's ambitions on environmental and financial sustainability and a commitment to equity, diversity, and inclusion.

Council will now work on defining the ambition and implementation plans for each goal. More details can be found on the LMS website at lms.ac.uk/about/governance. If you are interested in supporting the work, please email president@lms.ac.uk.

Jens Marklof
LMS President

Simon Edwards
LMS Executive Secretary

New International Secretary Officer Role for 2024

The LMS Council has taken the opportunity to review the Programme Secretary role with the decision of Chris Parker, following his successful re-election, to continue in the role for one further year until November 2024. Following discussion, Council concluded that the title of Programme Secretary is now largely historic, with the disbanding of the Programme Committee in 2017, and there being no specific governance requirement that the Programme Secretary chair the Early Career Research Committee (ECRC). The update to the Standing Orders in 2019 also allows for the redefining of an Officer title through the Society's statutes, and the Charter only requires that the Society have a President, at least one Vice-President, a Treasurer and at least one Secretary.

With the development of a new strategy for the Society, Council agreed that the LMS role in the global mathematics community was the area that would benefit from Officer-level support and engagement and decided to replace the Programme Secretary role with an International Secretary. The strategic goal is focused on the LMS playing an active role in the international mathematical community, developing LMS international partnerships and membership, and building on the global status of the Society.

The International Secretary role will be part of the election process for 2024 and the successful candidate will take up the role at the AGM in November 2024.

Robb McDonald
LMS General Secretary

OPPORTUNITIES

LMS Distinguished Visiting Fellowships Programme (@ICMU)

The LMS is delighted to have launched a joint programme with the newly formed International Centre for Mathematics in Ukraine (ICMU). The ICMU was founded in 2022 by a group of mathematicians of Ukrainian origin who believe that science and research would play a crucial role in the reconstruction of Ukraine after the war. The centre aims to support top-level research in mathematics with a special focus on training young scientists and fostering the development of mathematics in Ukraine.

The LMS Distinguished Visiting Fellowship Programme will allow mathematical scientists with recognised achievements in their disciplines to spend a period of time at the ICMU and give a series of lectures or a colloquium for the benefit of the Ukrainian mathematical community and students. It is expected that visitors within this programme spend a period between one week (five working days) to one month at the ICMU.

Further details of the scheme and how to apply can be found at: mathcentre.in.ua/en/programmes/visitors.

Simon Salamon
LMS Treasurer

LMS Research Schools and Research Schools in Knowledge Exchange 2025

LMS Research Schools and Research Schools in Knowledge Exchange 2025 Grants of up to £15,000 are available for LMS Research Schools, one of which will be focused on Knowledge Exchange. The LMS Research Schools provide training for research students in contemporary areas of mathematics. The Knowledge Exchange Research Schools will primarily focus on Knowledge Exchange and can be in any area of mathematics.

The LMS Research Schools take place in the UK and support participation of research students from both the UK and abroad. The lecturers are expected to be international leaders in their field. The LMS Research Schools are often partially funded by the Heilbronn Institute for Mathematical Research (heilbronn.ac.uk) and UK Research and Innovation (ukri.org). Information about the submission of proposals can be found at tinyurl.com/ychr4lwm along with a list of previously supported Research Schools. Applicants are strongly encouraged to discuss their ideas for Research Schools with the Chair of the Early Career Research Committee, Professor Chris Parker (research.schools@lms.ac.uk), before submitting proposals. Proposals should be submitted to Lucy Covington (research.schools@lms.ac.uk) by 22 February 2024.

Clay Mathematics Institute Enhancement and Partnership Program

To extend the international reach of the Research School, prospective organisers may also wish to consider applying to the Clay Mathematics Institute (CMI) for additional funding under the CMI's Enhancement and Partnership Program. Further information about this program can be found at tinyurl.com/cutdkwma. Prospective organisers are advised to discuss applications to this program as early as possible by contacting the CMI President, Martin Bridson (president@claymath.org). There is no need to wait for a decision from the LMS on your Research School application before contacting the CMI about funding through this program.

LMS Undergraduate Summer School 2025: Call for Expressions of Interest

Expressions of interest are invited to host the LMS Undergraduate Summer School in 2025 — deadline 22 February 2024.

A grant of up £25,000 plus income from registration fees (£250 per registered student attending in-person and £25 per registered student attending remotely) is available to support the costs of a Summer School that can accommodate at least 50 undergraduate students attending in-person and up to 200 undergraduates attending remotely.

The LMS Undergraduate Summer Schools, aimed at introducing enthusiastic undergraduate students to modern mathematical research, have run since 2015. They take place for a two-week period in July and have proved very popular.

For more information and to submit an expression of interest, please visit: lms.ac.uk/events/lms-summer-schools.

LMS Grant Schemes

February and May Deadlines

The next closing date for research grant applications (Schemes 1,2,3,4,5,6 and AMMSI) is 15 May 2024. Applications are invited for the following grants to be considered by the Research Grants Committee at its June 2024 meeting. Applicants for LMS Grants should be mathematicians based in the UK, the Isle of Man or the Channel Islands. For grants to support conferences/workshops, the event must be held in the UK, the Isle of Man or the Channel Islands.

Conferences (Scheme 1)

Grants of up to £5,500 are available to provide partial support for conferences. This includes travel, accommodation and subsistence expenses for principal speakers, UK-based research students, participants from Scheme 5 countries and Caring Costs for attendees who have dependents.

Visits to the UK (Scheme 2)

Grants of up to £1,500 are available to provide partial support for a visitor who will give lectures in at least three separate institutions. Awards are made to the host towards the travel, accommodation and subsistence costs of the visitor. Potential applicants should note that it is expected the host institutions will contribute to the costs of the visitor. In addition, the Society allows a further amount (of up to £200) to cover Caring Costs for those who have dependents.

Research in Pairs (Scheme 4)

For those mathematicians inviting a collaborator, grants of up to £1,200 are available to support a visit for collaborative research either by the grant holder to another institution abroad, or by a named mathematician from abroad to the home base of the grant holder. For those mathematicians collaborating with another UK-based mathematician, grants of up to £600 are available to support a visit for collaborative research either by the grant holder to another institution or by a named mathematician to the home base of the grant holder. In addition, the Society allows a further amount (of up to £200) to cover Caring Costs for those who have dependents.

Research Reboot (Scheme 4)

Grants of up to £500 for accommodation, subsistence and travel plus an additional £500 for caring costs are available to assist UK mathematicians who may have found themselves with very little time for research due to illness, caring responsibilities, increased teaching or administrative loads, or other factors. This scheme offers funding so that they can leave their usual environment to focus entirely on research for a period from two days to a week. For applications submitted by the next deadline (22 January 2024), the Reboot Retreats should take place between 15 March and 30 June 2024.

Collaborations with Developing Countries (Scheme 5)

For those mathematicians inviting a collaborator to the UK, grants of up to £3,000 are available to support a visit for collaborative research, by a named mathematician from a country in which mathematics could be considered to be in a disadvantaged position, to the home base of the grant holder. For those mathematicians going to their collaborator's institution, grants of up to £2,000 are available to support a visit for collaborative research by the grant holder to a country in which mathematics could be considered to be in a disadvantaged position. Applicants will be expected to explain in their application why the proposed country fits the circumstances considered eligible for Scheme 5 funding. In addition, the Society allows a further amount (of up to £200) to cover Caring Costs for those who have dependents. Contact the Grants team if you are unsure whether the proposed country is eligible or check the IMU's Commission for Developing Countries definition of developing countries (tinyurl.com/y9dw364o).

Research Workshop Grants (Scheme 6)

Grants of up to £10,000 are available to provide support for Research Workshops. Research Workshops should be an opportunity for a small group of active researchers to work together for a concentrated period on a specialised topic. Applications for Research Workshop Grants can be made at any time but should normally be submitted at least six months before the proposed workshop.

African Mathematics Millennium Science Initiative (AMMSI)

Grants of up to £2,000 are available to support the attendance of postgraduate students at conferences in Africa organised or supported by AMMSI. Please contact grants@lms.ac.uk for more information. The next closing date for early career research grant applications (Schemes 8,9 and ECR Travel Grants) is 22 February 2024.

Applications are invited for the following grants to be considered by the Early Career Research Committee at its March/April 2024 meeting:

Postgraduate Research Conferences (Scheme 8)

Grants of up to £2,500 are available to provide partial support for conferences, which are organised by and are for postgraduate research students. The grant award will be used to cover the costs of participants. In addition, the Society allows the use of the grant to cover to cover Caring Costs for those who have dependents.

Celebrating New Appointments (Scheme 9)

Grants of up to £400-£500 are available to provide partial support for meetings to celebrate the new appointment of a lecturer at a university. Potential applicants should note that it is expected that the grant holder will be one of the speakers at the conference. In addition, the Society allows the use of the grant to cover to cover Caring Costs for those who have dependents.

ECR Travel Grants

Grants of up £500 are available to provide partial travel and/or accommodation support for UK-based Early Career Researchers to attend conferences or undertake research visits either in the UK or overseas.

Forthcoming LMS Events

The following events will take place in forthcoming months:

LMS Northern Regional Meeting and Workshop 2024: 28 March, Durham (tinyurl.com/3dyha4sb)

LMS Midlands Regional Meeting and Workshop 2024: 2 April, Loughborough (tinyurl.com/4v3fmhrk)

LMS Spitalfields History of Mathematics Meeting and Hirst Lecture: 26 April, London (tinyurl.com/mwm7mwkf)

LMS Popular Lecture 2024 (Speaker: Sarah Hart): 9 May, Birmingham (tinyurl.com/2xwvatr3)

LMS General Meeting and Kelvin 200th Anniversary Lecture, London: 28 June, London (details to follow)

LMS Invited Lecture Series 2024: 1-5 July, Imperial College London (tinyurl.com/4vjhaeka)

A full listing of upcoming LMS events can be found on page 45.

VISITS

Visit of Stéphanie Nivoche

Professor Stéphanie Nivoche will be visiting the School of Mathematical Sciences, Queen Mary University of London from 4 - 15 March 2024. Professor Nivoche is based at the Université Côte d'Azur in Nice. She works in several complex variables and pluripotential theory and is perhaps best known for providing the key result for the first proof of a long-standing conjecture of Kolmogorov on the asymptotic behaviour of the epsilon-entropy of sets of holomorphic functions. During her visit Professor Nivoche will give lectures at:

- Queen Mary University of London, 5 March 2024 (contact Bolys Sabitbek: b.sabitbek@qmul.ac.uk);
- University of Reading, 12 March 2024 (contact Jani Virtanen: j.a.virtanen@reading.ac.uk);
- King's College London, 14 March 2024 (contact Jean Lagacé: jean.lagace@kcl.ac.uk)

For further details contact Oscar Bandtlow (o.bandtlow@qmul.ac.uk). The visit is supported by an LMS Scheme 2 grant.

Visit of Joaquín Singer

Dr Joaquín Singer will be visiting the Department of Mathematics, King's College London from 7 February to 22 February 2024. Dr Singer is a member of the Research Group of Functional Analysis of the University of Buenos Aires as well as an assistant professor at the University of San Andrés. His research interests include algebras of holomorphic functions, infinite dimensional holomorphy, asymptotic geometric analysis and high-dimensional probability, that allow to study high-dimensional systems, which are very frequent in mathematics and applied sciences. During his visit Dr Singer will give a lecture about Hadwiger's covering problem at:

- King's College London, 15 February (contact Felipe Marceca: felipe.marceca@kcl.ac.uk)

For further details contact Felipe Marceca (felipe.marceca@kcl.ac.uk). The visit is supported by an LMS Scheme 5 grant.

LMS Council Diary — A Personal View

The day of the AGM is always a special one for the Society. But before the formalities, lectures and festivities, Council met in person for its final meeting of the year.

Council approved the memorandum of understanding with the International Centre for Mathematics in Ukraine (ICMU), establishing the LMS Distinguished Visitor Fellowship scheme, along with the appointment of LMS Treasurer Simon Salamon to its Scientific Board. Council was delighted that Masha Vlasenko, Managing Director of the ICMU, was able to join the subsequent AGM and Annual Dinner to announce the partnership.

Further internationally focussed activities for the Society came with an update of its bid, joint with the Institute of Mathematics and its Applications, to host the 10th European Congress of Mathematics in London in 2028. The update included the proposed 15-person local organising committee. Continuing the 'international' theme, Council approved the role description for a new International Secretary post, which is set to replace the Programme Secretary from the 2024 elections. Council welcomes interest from the mathematical community to this role and looks forward to making an excellent appointment in helping the Society develop and achieve its international strategy.

It was agreed to put the Society's fundraising activities on a more professional footing by engaging the services of experienced fundraisers. The Treasurer reported on the recommendations of the recent Investment Sub-Committee meeting and Council agreed, in accordance with its sustainability ambitions, to move 100% of its quoted investments (managed by Schroder/Cazenove) to the Sustainable Multi-Asset Fund (previously 50% was in the Charities Multi-Asset Fund).

The Newsletter Editor-in-Chief, Alina Vdovina, presented her annual report to Council. From the positive feedback from a recent members' survey, it was evident that the Newsletter is a cherished benefit to members. Council reaffirmed its commitment to the regular publication of a high-quality Newsletter.

The last Council meeting of the year often sees the departure of long-serving Council members. This year was no exception, with Council giving warm thanks to those departing. All have given many years of sustained and exceptional service to the Society and will be much missed.

Robb McDonald
General Secretary

LMS Council and Nominating Committee 2023–24

The results of the 2023 LMS Elections to Council and Nominating Committee were announced at the AGM on 17 November 2023.

The President, Professor Jens Marklof FRS, was elected for a term of two years in November 2022, taking office as President in November 2023.

LMS Council

Officers of Council:

Vice-President: Professor Iain Gordon
Vice-President: Professor Catherine Hobbs
General Secretary: Professor Robb McDonald
Treasurer: Professor Simon Salamon
Publications Secretary: Professor Niall MacKay
Programme Secretary: Professor Chris Parker
Education Secretary: Professor Mary McAlinden

Members-at-Large of Council:

Member-at-Large (Committee for Women and Diversity): Professor Sara Lombardo
Member-at-Large: Dr Andrew Brooke-Taylor
Member-at-Large: Professor Elaine Crooks
Member-at-Large: Dr Jessica Enright
Member-at-Large: Dr Rachel Newton
Member-at-Large: Professor Gregory Sankaran

Continuing Members-at-Large of Council are: Professor Peter Ashwin, Professor Minhyong Kim, Professor Jason Lotay, Professor Anne Taormina, Professor Amanda Turner, and Professor Sarah Whitehouse.

Nominating Committee

Professor Karin Baur
Professor Victoria Gould

Continuing members of the Nominating Committee are: Professor Tara Brendle FRSE (Chair), Professor Nira Chamberlain, Professor Laura Ciobanu, Professor Philip K. Maini FRS FMedSci FRSB, and Professor Helen Wilson. Council will also appoint a representative to the Committee.

Members of Council 2023–2024

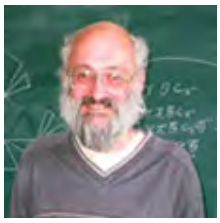
Jens Marklof
President

Cathy Hobbs
Vice-President

Iain Gordon
Vice-President

Simon Salamon
Treasurer

Robb McDonald
General Secretary



Chris Parker
Programme Secretary

Niall MacKay
Publications Secretary

Mary McAlinden
Education Secretary

Sara Lombardo
Member-at-Large (Women and Diversity)

Peter Ashwin
Member-at-Large

Andrew Brooke-Taylor
Member-at-Large

Elaine Crooks
Member-at-Large

Jessica Enright
Member-at-Large

Minhyong Kim
Member-at-Large

Jason Lotay
Member-at-Large

Rachel Newton
Member-at-Large

Gregory Sankaran
Member-at-Large

Anne Taormina
Member-at-Large

Amanda Turner
Member-at-Large

Sarah Whitehouse
Member-at-Large

Retiring Members of Council

The following people retired from the LMS Council at the Annual General Meeting in November 2023: Professor Ulrike Tillmann (LMS President); Professor Kevin Houston (Education Secretary); Professor Andrew Dancer (Member-at-Large); and Professor Frank Neumann (Member-at-Large).

Professor Ulrike Tillmann FRS
LMS President, 2021–2023

Professor Tillmann was a tireless advocate for the Society throughout her presidency, promoting its activities and acting as a spokesperson for the interests of the LMS and the wider mathematical community. Through the Protect Pure Maths Campaign, she worked to influence decision making at the highest level, giving evidence at the select inquiry into Diversity and Inclusion in STEM and writing articles in the national press on topics such as the urgent need to address the closure of mathematics departments in 'lower-tariff' universities — a vital step towards achieving the government's levelling up plans.

Professor Tillmann was instrumental in maintaining and strengthening relationships with LMS donors, members and external stakeholders in a changing landscape, representing the Society on the Council for Mathematical Sciences during the ongoing development of an Academy for Mathematical Sciences. She led the LMS Council Strategic Retreat in April 2023, at which three new strategic goals for the next five years were agreed, in the areas of membership engagement, pathways in mathematics, and the role of the Society in the global community. Under her leadership, Council clarified its ambitions towards environmental and financial sustainability and a full commitment to equity, diversity and inclusion.

Notable among her many acheivements was Professor Tillmann's oversight of the Society's response to the Russian invasion of Ukraine. This response included the launch of two successful solidarity grant schemes to support members of the mathematical community forced to leave their homes and, most recently, the launch of the Distinguished Visiting Fellowship Programme, a joint initiative with the newly formed International Centre for Mathematics in Ukraine.

As she hands over the badge of office to Professor Jens Marklof, we would like to thank Professor Tillmann for her dedication, enthusiasm and leadership, and wish her well for the future.

Professor Kevin Houston
Education Secretary, 2017–2023

As Education Secretary, Professor Houston chaired the Society's Education Committee for six years. During this time, he oversaw the committee's work in supporting mathematical education and encouraging young people to develop an interest in mathematics, and represented the Society publicly on a number of issues relating to maths education policy. Among his achievements as Chair was the launch of the popular Mathematics Communication and Outreach Workshop Series, at which attendees are taught to communicate mathematics effectively and accessibly during interactive training sessions.

Professor Andrew Dancer
Member-at-Large, 2019–2023

Professor Dancer was Chair of the LMS Research Grants Committee during his tenure as Member-at-Large. In this role, he successfully steered the grants programme through the pandemic and oversaw the introduction of the Research Reboot Grant Scheme to support those whose research had been affected during the pandemic.

Professor Frank Neumann
Member-at-Large, 2019–2023

Professor Neumann was and continues to be Chair of the Mentoring African Research in Mathematics (MARM) scheme, and continues to be a member of the Research Grants Committee. He has worked tirelessly to champion the work of MARM and brings valuable insights from mathematics outside the UK.

In addition to those listed above, the following Committee Chairs retired at the November AGM: Professor Chris Parker (Chair, Early Career Research Committee, 2017–2023); Professor Brita Nucinkis (Chair, Society Lectures and Meetings Committee, 2019–2023); and Professor Prudence Wong (Chair, Computer Science Committee, 2017–2023).

The Society recognises and is grateful for the enormous amount of work put in by its volunteers towards the effective running of the LMS. We would like to thank all of those who have stepped down recently for their dedication and service.

Katherine Wright
LMS Communications and Policy Manager

Speeches at the 2021 LMS AGM Reception and Dinner

Jens Marklof, incoming LMS President:

Good evening, members, friends and supporters of the London Mathematical Society. Following the conclusion of our Annual General Meeting with two wonderful lectures by Oscar Randal-Williams and Ulrike Tillmann, I am delighted to welcome you all to this year's annual dinner. I am pleased we are joined by so many who have supported the Society and UK mathematics over the past year.

In particular, I'd like to extend a very warm welcome to:

- The winners of this year's LMS Prizes; we are extremely proud of your achievements!
- Representatives of our sister organisations, the Institute for Mathematics and its Applications, the Operational Research Society, and the Royal Statistical Society.
- Masha Vlasenko from the International Centre for Mathematics in Ukraine. We also have here today three colleagues from Ukraine who are supported by the INI/LMS Solidarity for Mathematicians programme.
- Hans Buehler (representing XTX Markets), Tony Hill (Levelling Up) and Rudi and Florence Bogni (Liber Foundation). The Society is enormously grateful for your generous continued support of the Society's activities.
- Viscount Stansgate, who earlier this week raised mathematics in the House of Lords in the debate on the King's speech.
- Viscount Hanworth, who proposed a special inquiry into mathematics this autumn, working closely with the LMS.
- Thank you to Trustees and Committee Chairs who are central to the work of the Society, especially Kevin Houston, Andrew Dancer and Frank Neumann, who have stood down today. A very warm welcome to our new trustees elected today: Mary McAlinden, Andrew Brooke-Taylor and Gregory Sankaran.
- Three members of LMS staff celebrating significant anniversaries: Ephrem Abate, celebrating 25 years' service, and Katherine Wright and Valeriya Kolesnykova, both celebrating 10 years' service.
- And last but not least: very special thanks to Ulrike Tillmann for her service as President of the Society for the past two years:
  - working with the Protect Pure Maths Campaign;
  - supporting the various initiatives to support colleagues in Ukraine;
  - key role in helping setting up the Academy of Mathematical Sciences;
  - her many other roles outside of the Society, amongst others as Director of the Isaac Newton Institute, Vice-President of the Royal Society and Chair of Royal Society's Education Committee;
  - internationally: Vice-President of the International Mathematical Union, and her work on several high-ranking committees;
  - Ulrike will give us her own reflections — and I hope some good advice for her successor — on her time as President later this evening.

I am sure you will not be short of talking points over dinner, but there are three topics I'd like to propose for your table. These concern challenges and opportunities the Society and general mathematics community will be facing over the next decade. They link closely with the Society's new strategy, and I would welcome your opinion and feedback:

1. The first is: How will advances in modern mathematics — both pure and applied — contribute to the solution of global challenges: from environmental and health sciences, cybersecurity and data science, to disruptive technologies, such as AI and Quantum? Mathematics is widely recognised as an underpinning subject, an invaluable part of education and training in virtually all quantitative subjects, but I believe there is an irrefutable case to be made for advanced research in mathematics in our complex, increasingly digital world. But we have to evidence and tell this story to both policy makers and those A-level students who want to change the world for the better. I firmly believe that the global society will not solve its major challenges without the advanced tools provided by modern mathematics.

2. This last point highlights also the challenge of diversity in our subject. We need to increase the pathways to mathematics, make sure we enable outreach activities to bring those into the subject who might not consider mathematics as a career option, because of their background, because they might not see the exciting career opportunities the subject has to offer outside of academia, or simply because they believe the subject is reserved only to those who are best-in-class. We have witnessed an alarming trend in mathematics programmes closing in lower tariff institutions, something the Society will continue to actively combat in partnership with the Protect Pure Maths Campaign. It seems absurd that the closure of maths programmes is happening at a time when mathematical skills are in increasing demand in business and industry. How can we make mathematics in higher education more relevant and attractive to a wider pool of school leavers?

3. Finally, the creation of the new Academy of Mathematical Sciences in the UK is a tremendous opportunity for the subject and our profession. The LMS has been an active supporter in setting up the proto-Academy, with many of our members represented in key roles in the relevant working groups and committees, including also key support provided by Ulrike Tillmann both as LMS President and Director of the Newton Institute. Many of the issues I mentioned earlier will be central to the Academy's business. But this will not mean that the LMS and other societies representing the mathematical sciences will become obsolete. For the LMS in particular, there is an exciting opportunity to build on our already very strong reputation as a global rather than a purely national society, with a large proportion of overseas members. The Society's strategy includes plans to build on this and increase its global presence, developing activities across the world to support and foster education and collaboration as a truly global society. Central here will be the networks our members have already in place, and I would welcome ideas and suggestions from you on where you see particular opportunities we could support.

Once more, thank you all again for being here today and your continued support of the Society. I very much hope I will have a chance to catch up with you tonight. Enjoy the rest of the evening. Bon Appetit!

Ulrike Tillmann, retiring LMS President:

Two years ago, when I took over the presidency from Jon Keating, we were still seated wide apart, worrying about when and where to wear masks. And indeed soon after, Covid cases increased again and we had another lock-down. It is surprising how quickly professional life seems to have bounced back to what it was with one significant difference, in person meetings for committees are much rarer and we have become much more efficient, talking on Zoom, which allows people to fully partake wherever they are.

But that makes occasions like this all the more important, where we meet in person to catch up on all those small conversations that otherwise don't happen, where we can reflect, celebrate and simply enjoy each other's company.

This has in many ways been my dream job. The LMS is a fantastic organisation. Throughout its long history it has led the way in so many ways in the past:

- colleagues in other countries like France and the US started maths societies inspired by the LMS;
- its journals, some of which go back to its foundation in 1865, have a high international reputation thanks to the hard work of generations of editors;
- and this brings with it international esteem that is reflected in our large international membership;
- the LMS has also led on Women in Maths and on EDI more generally – and its Good Practice Scheme was recognized by a Royal Society award a few years ago.

And more recently, the LMS has been active in communication and outreach (our Levelling Up scheme has been tremendously successful), as well as lobbying for mathematics through the Protect Pure Maths campaign. Many of our activities are now supported very generously by our donors — a big personal thank you to them from me. Without their commitments we would not be able to do so much. Indeed, donations take a more and more important role for the LMS, and this past year they contributed to our budget significantly and the total income from donations was comparable to our investment income and more than half of our net publication income.

International politics does not normally have a great impact on the LMS but the invasion of Ukraine in 2022 did. Because of the then imminent ICM in St Petersburg, Council felt we had to take a position. It was a sad moment when our 60 year cooperation with the Russian Academy of Sciences on three translation journals came to an end (because of sanctions we could not operate and we needed to give our Russian colleagues the chance to continue the journals). On a more positive note, the LMS, with the Newton Institute and financial help from XTX Markets, set up immediately a Solidarity programme. By now 18 refugee research mathematicians are supported and based in 14 different UK universities. Some have found already regular academic jobs and PhD studentships. I am particularly pleased that today we were able to announce our partnership with the newly founded International Centre for Mathematics Ukraine (ICMU) to set-up the LMS Distinguished Visiting Fellowships. The money that the LMS has pledged for this programme over the next ten years will be matched by XTX Markets. I am pleased that ICMU's Managing Director, Masha Vlasenko, could join us tonight to mark the occasion.

An important development for the UK mathematical sciences has been the project to set-up a national academy. Serious work started a bit more than a year ago, and things are moving fast. The executive Committee of the proto-academy has worked hard raising funds, setting-up a policy unit and registering as a charity. Together with all the other CMS societies, the LMS has pledged its full support for the Academy, assuming enough funds can be raised. There is more work to do to set up governance and a fellowship. But that is for the Academy to do and for us to support.

What will the Academy mean for the LMS? There will be areas where the Academy should take a lead, such as policy, and others where the LMS hopes to collaborate. Equity, diveristy and inclusion comes to mind and through such a collaboration we hope our work will be strengthened and have even wider reach. But there are also areas where it is expected that the Academy will have little influence or interest. For example, we do not expect the Academy to become a membership organisation like the LMS nor to start academic publications. Council also identified another distinct feature of the LMS, namely that we are not just a national but also an international organisation with a significant proportion of overseas members and a worldwide reputation. This international perspective has now been clearly articulated in our new strategy for 2023–28 which Council agreed to today and which commits the LMS to play an active role in the international mathematical community and develop international partnerships.

I would like to express my sincere thanks to our many volunteers — the editors of our journals, the chairs and members of our plethora of committees — many of whom are here today and our members more generally many of whom I had the privilege to meet at events and meetings during the past two years. They do most of the hard work supported by our excellent and loyal staff. I would like to extend my warmest congratulations on their anniversaries to Valeriya, Katherine, and Ephrem.

I would also like to thank Council for all its support throughout the two years. I cannot recall when I went away from a meeting and felt we made a wrong decision. And I don't mean that I always got my way but decisions on difficult issues were taken collectively after extensive and constructive discussion.

The President works closely with the officers, especially the Vice-Presidents, and even more so with the Executive Secretary. I much appreciated Cathy's and Iain's solid support — Iain first chairing the Ukraine working group then the one for the Academy, and Cathy's firm grip on HR and communications. As to the Executive Secretaries, during my term there were three (Caroline, Fiona, and Simon) — likely a record — but I have to say, all three have been wonderful to work with. Having seen Simon in action for just over a year now, I am confident that the LMS is in excellent hands, and I calmly pass on the presidency to Jens who I am sure will guide the Society to new heights.

Please join me for a toast: "To the continued health of mathematics and the London Mathematical Society."

LEVELLING UP

This column includes the latest updates about the *Levelling Up: Maths* scheme being developed by the LMS, made possible by a generous donation from Dr Tony Hill and Mr Simon Goodwin. The scheme seeks to widen participation of those who are under-represented in mathematics. It is part of a broader *Levelling Up: STEM* project which also covers Physics and Chemistry.

We are now entering our third year of running Levelling Up: Maths in conjunction with the IMA. In the first year three universities participated in Levelling Up: Maths. We are now at 13 with 2 more universities about to join in spring 2024. In September 2023, the LMS and IMA commissioned an evaluation framework to assist universities to evaluate the scheme and measure success. The LMS and IMA bring the Levelling Up: Maths universities together twice a year to share good practice and learning. Julia Goedecke, curator of the Levelling Up: Maths materials joins the meetings and is on hand to answer questions on content.

The scheme founder, Dr Tony Hill, joined us at the LMS Annual Dinner in November 2023 and was very pleased to meet some of the undergraduate and master's students delivering the scheme.

We extend our thanks to all the Levelling Up: Maths tutors who work with A level mathematics students across the country.

Dr Tony Hill and the Levelling Up: Maths tutors from Durham, Kent and Queen Mary London University

Jennifer Gunn
LMS Head of Society Business

Records of Proceedings at LMS meetings
Annual General Meeting and Presidential Address 2023, 17 November 2023

held on 17 November 2023 at the Mary Ward House, London and online via Zoom along with the Presidential address. Over 150 members and guests were present either in person (110 people) or online (40 people) for all or part of the meeting.

The meeting began at 3.00pm with The President, Professor Ulrike Tillmann FRS, in the Chair.

The Minutes of the General Meeting, which was held on 30 June 2023, were circulated to members 21 days in advance of this meeting. Copies of those Minutes were also available at the meeting. The President asked those members present and online if there were any clarifications or corrections to those minutes? There were none and the Minutes were confirmed.

The Vice-President, Professor Cathy Hobbs, presented a report on the Society's activities in 2022-2023 and the President invited questions. The Treasurer, Professor Simon Salamon, presented his report, online, on the Society's finances during the 2022-23 financial year and the President invited questions. Copies of the Trustees' Report for 2022-23 were made available on the day and the President invited members to adopt the Trustees' Report for 2022-23 by a show of hands for those in person and via a poll for those joining online. The Trustees' Report for 2022-23 was adopted.

The President asked the membership to note that the Society would undertake a tendering exercise in 2023-24 to appoint the Society's external organisers and that the membership would be asked to vote on the appointment at the General Meeting on 28 June 2024.

There were 264 members elected to Membership at this Society Meeting.

34 members were elected to Associate membership: Mr Stuart Abercrombie, Mr Bethel Agozie, Ms Shaked Bader, Miss Daniela Cialfi, Mr Nathan Creighton, Miss Riya Danait, Ms Harriett Du Four, Miss Zoe Godard, Dr Erdong Guo, Mr Jad Hamdan, Dr Lucien Hennecart, Ms Emma Hogan, Dr Carmen Jorge-Diaz, Ms Patricia Lamirande, Mr Glen Lim, Mr Adam Mabrouk, Mr Maximilien Mackie, Mr Mutaz Mango, Mr Lewis Matthews, Dr Elle McLean, Dr Marianthi Moschou, Ms Sarah Parry, Mr Peter Paulovics, Ms Katerina Santicola, Mrs Adnan Shamaoon, Mr Fraser Sparks, Mr Md Abu Sufian, Dr Minwei Sun, Mr Daniel Threlfall, Mr Vlad Tuchilus, Mr Julius Nathan Villar, Miss Ashleigh Wilcox, Mr Christopher Wright and Mr Yue Wu.

10 members were elected to Associate (Undergraduate) membership: Miss Zoe Davenhill, Ms Ria Debnath, Mr Yuao (Kevin) Du, Mr William Fayers, Miss Yilin Jin, Miss Taraneh Latifi Seresht, Mr Mark Lyttle, Mr Jacob Smith, Mr Zhiyu Wang and Mr Eu Wen Wong.

183 members were elected to Associate (Teacher Training Scholarship) membership: Miss Mia Adams, Mr Benedict Agagli, Miss Hafsa Akmal, Mrs Zakira Al Mukhtar, Mr Ahmed Alhad, Miss Francesca Allmark, Mr Mhd Reda Alnshiwati, Dr Jessica Andrews, Mr Oskar Apperley, Mr Dominic Attrell, Mr Abdullahi Awale, Mr Ridwan Axmed, Mr Muhammad Baasit, Miss Tamara Bakry, Mr Jake Battersby, Mr Ozan Baybars Sutcu, Mr Jon Beasley, Miss Georgia Beeton, Mr David Benson, Mr Mark Beville, Miss Humairaa Bhana, Ms Tausif Bhatty, Mr Jack Bland, Miss Hanaa Bouf-Tah, Mr Louis Bounds, Mr Mykhailo Bratyk, Miss Catherine Bray, Mrs Alison Brejza, Mr Josiah Brenchley, Mrs Bena Briggs, Mr Angus Brownlie, Miss Philippa Bryant, Miss Sophie Campin, Mr John Joe Chiasson, Mr Ryan Chivers, Dr Edward Clark, Mr Charles Clarke, Ms Eve Clarke, Miss Lowyne Courtney, Mr Thomas Cripps, Miss Sophie Cross, Mr Liam Crossley-Gilbank, Mr Stephen Curran, Mr Jack Davis, Miss Rebecca Dean, Mr Callum Diplock, Mr Thomas Dixon, Miss Telka Donyai, Mr Jacques Dunn, Mr Matthew Durrant, Ms Aaliya Dussroth, Miss Freya Elphick-Webb, Mr Ben Ettridge, Mr Ben Evans, Mr James Everitt, Miss Malindi Felfeli, Mr Andrew Fennell, Miss Kiah Ferrarin, Mr Callum Fielding, Dr Kevin Findlay, Mr Thomas Fines, Mr Charlie Foster, Miss Merle French-Jamieson, Ms Sophie Gebray, Mrs Eider Goicoechea Banuelos, Mr Vincent Golding, Mrs Sophie Grady, Dr Timothy Grange, Mr Benjamin Green, Mrs Laura Gueran, Mr Sean Guthrie, Miss Elizabeth Hall, Miss Eleanor Ham, Miss Annabel Hartley, Mr Max Hersh, Miss Erin Heywood, Miss Jade Hird, Mr Jonathan Hodges, Mr Simon Holt, Miss Kenna Hook, Mr Edward Hopper, Mr Samuel Hor, Mr Muneem Hussain, Miss Sara Hussein, Miss Amy Hutchins, Miss Aiysha Ismail, Mr Matthew Jackson, Ms Kaye Jennings, Miss Elle Jones, Miss Ellie Jones, Mr Harry Jones, Mr Jacob Jones, Mr Samuel Jones, Miss Aamna Kamil, Miss Matilda Kannan, Mr Nasko Karaganev, Mr Karim Karass, Mr James Kearney, Miss Ellie Keeble, Mr James Kewley, Mr Naseer Khan,

Mr David King, Mrs Danielle Kirwan, Mr Dylan Knott, Miss Thekla Lambri, Ms Rebecca Lee, Miss Liberty Lee, Miss Emilia Lewis, Mrs Stephanie Lewis, Mr Felix Lindsay-Smith, Ms Aysha Lohan, Miss Deborah Lowden, Miss Erin MacQuarrie, Mr Harvey Manley, Mr Edmund Mann, Miss Bethany Marshall, Mrs Victoria McKnight, Mr Luke Melville, Miss Eleni Michaela, Mr Harry Mill, Miss Savannah Miller, Mrs Isabelle Mills, Miss Zeinab Miyir, Mx George Moore, Mr William Mottram, Mr Vincent Murphy, Mrs Amanda Murray, Miss Jennifer Musson, Mrs Rohima Nazmin, Mr Robin Newby, Mr Harry Newman, Miss Kasia Nickells, Miss Natasha Noble, Mr Ivan Orlinski Pilfold, Miss Charlotte Orsler, Mr Jared Parker, Ms Sonja Perreten, Mrs Tzvetanka Petrova, Mr Ethan Pill, Mr Jamie Potter, Mrs Joanne Preston, Mr Aaran Rajathevan, Miss Ruqaiya Rani, Mr Douglas Renwick, Miss Anna Roberts, Mr Stuart Robinson, Miss Faizah Ruhi, Mr Claudio Amos Ruiz Richard, Mr Sam Russell, Miss Amal Said, Mr David Sánchez-Bermejo Oliver, Mr Oliver Seabarron, Dr Lonie Sebagh, Miss Georgia Seddon, Mr Prasanna Sekaran, Miss Carla Simons, Miss Nicole Simpson-Burns, Mr Liam Slater, Mrs Jessica Sleight, Dr David Smith, Mr Aidan Stannard, Mr David Stewart, Miss Lauren Stockley, Miss Jodie Stocks, Mr Ben Stones, Miss Tamanna Tanzim, Ms Samantha Taylor-Hayward, Miss Paola Torche, Mr Hemal Trivedy, Miss Kate Turnbull, Miss Sumayyah Uddin, Mr Animesh Upreti, Mr Jack Virgin, Mr Oliver Wadey, Ms Flora Walker, Miss Jordan West, Mrs Victoria Williams, Mr Samuel Woodruff, Mr Daniel Woolridge, Mr Haoyin Wu, Mr Andrew Yip and Mr Nhamburo Ziyenge.

28 members were elected to Ordinary membership: Dr Gabriel Berzunza Ojeda, Miss Atrayee Bhattacharya, Mr Arfan Bhatti, Dr Christian Bönicke, Dr Ferran Brosa Planella, Professor Ivan Cheltsov, Dr Antoine Dahlqvist, Professor Tudor Dan Dimofte, Dr Erzsebet Dombi, Mr Stuart Dootson, Dr Omar El Deeb, Dr Ana Lucia Garcia Pulido, Miss Simona Iliesi, Dr Yury Korolev, Dr Cheuk Yu Mak, Dr Zachiri McKenzie, Dr Hannah Mitchell, Dr Imran Nasim, Dr Panos Parpas, Professor Mark Powell, Dr James Roberts, Professor Damian Rössler, Mr Robin Taylor, Dr Leonardo Tolomeo, Dr Jackie Wong Siaw Tze, Dr Dapeng Wang, Professor Wendelin Werner and Dr Michele Zordan.

9 members were elected to Reciprocity membership: Dr Badr Alharbi, Mr Amitava Bhattacharya, Dr William Harrod, Professor Arthur Jaffe, Dr Per Nilsson, Mr Winfred Ooh-Azlin, Mr Madan Srivastava, Dr Guhan Venkat and Mr James Wilson.

12 members signed the Members' Book and were admitted to the Society.

The LMS Scrutineer, Professor Charles Goldie announced the results of the ballot. The following Officers and Members of the Council were elected.

President: Jens Marklof, FRS
Vice-Presidents: Catherine Hobbs, Iain Gordon
Treasurer: Simon Salamon
General Secretary: Robb McDonald
Publications Secretary: Niall MacKay
Programme Secretary: Chris Parker
Education Secretary: Mary McAlinden
Members-at-Large of Council for two-year terms: Andrew Brooke-Taylor, Elaine Crooks, Jessica Enright, Rachel Newton and Gregory Sankaran
Member-at-Large (Women and Diversity): Sara Lombardo

Six Members-at-Large, who were elected for two years in 2022, have a year left to serve: Peter Ashwin, Minhyong Kim, Jason Lotay, Anne Taormina, Amanda Turner and Sarah Whitehouse.

The following were elected to the Nominating Committee for three-year terms: Karin Baur and Victoria Gould. The continuing members of the Nominating Committee are: Tara Brendle (Chair), Nira Chamberlain, Laura Ciobanu, Philip K. Maini and Helen Wilson. In addition, Council would appoint a representative to the Committee.

The President presented the LMS Prizes for 2024, as follows:

Senior Anne Bennett Prize: Dr Eugénie Hunsicker (The Access Group)
Naylor Prize and Lectureship: Professor Jens Eggers (University of Bristol)

Whitehead Prizes:
Dr David Bate (University of Warwick)
Professor András Juhász (University of Oxford)
Dr Yankı Lekili (Imperial College London)
Professor Marie-Therese Wolfram (University of Warwick)

The Pólya Prize was awarded to Professor Dame Frances Kirwan FRS (University of Oxford). The Senior Whitehead Prize was awarded to Professor Agata Smoktunowicz FRSE (Edinburgh). The Berwick Prize was awarded to Professor Jian Ding (Peking University) and Professor Ewain Gwynne (University of Chicago), and two further Whitehead Prizes were awarded to Professor Soheyla Feyzbakhsh (Imperial College London) and Professor Mahesh Kakde (Indian Institute of Science). However, they were unable to collect their certificates and so their certificates have been sent to them.

The President introduced the first lecture given by Professor Oscar Randal-Williams (University of Cambridge) on *Symmetries of Manifolds*.

After tea, the retiring President handed over the badge of office to the new President, Professor Jens Marklof FRS, who then introduced the Presidential Address, which was given by Professor Tillmann FRS (Isaac Newton Institute, Cambridge, and University of Oxford) on *Utilising Shape in Data*.

The President thanked the speakers for their excellent lectures and then expressed the thanks of the Society to the organisers for a wonderful meeting.

Afterwards, a wine reception was held at Mary Ward House, London. The Society's Annual Dinner was also held at the Mary Ward House, London.

Autonomous Robots and Algebraic Topology

MICHAEL FARBER

In this articles we show how methods of algebraic topology help in designing algorithms forming "the brain" of autonomous robots.

Robots and their configuration spaces

According to Wikipedia, *"a robot is a machine - especially one programmable by a computer - capable of carrying out a complex series of actions automatically"*. In this article instead of the term "robot" we shall often use the term "mechanical system" or simply "a system". The latter concept is slightly broader and also includes multiple machines simultaneously moving in space (say, swarms of drones, fleets of ships or submarines, multiple vehicles etc) if such systems require coordinated centralised control.

Any mechanical system S determines a topological space which reflects its many important properties. This is *the configuration space* $\mathscr{C}(S)$ of S, which is defined as the variety of all states of S. By a state of the system S we mean not only the position and orientation of the system in space but also the positions and orientations of all its internal parts. Typically, a state of the system is fully determined by positions of a finite set of anchor points $a_1, \dots, a_N$ of S. Assigning vectors $x_1, \dots, x_N \in \mathbb{R}^d$ to the anchor points $a_1, \dots, a_N$ gives an injective map

$$\mathscr{C}(S) \to (\mathbb{R}^d)^N, \tag{1}$$

where $d = 2$ or $d = 3$. The topology of $(\mathbb{R}^d)^N$ induces a topology on the configuration space $\mathscr{C}(S)$ via the embedding (1). We shall see in examples below that the image of $\mathscr{C}(S)$ in $\mathbb{R}^d$ is a real semialgebraic set, i.e. it is the set of solutions of a system of real polynomial equations and inequalities.

Example 1. Consider a rigid body S moving in $\mathbb{R}^2$. Its configuration can be fully characterised by the positions of three anchor points a_1, a_2, a_3.

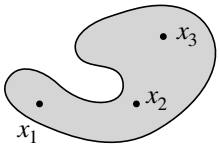


Figure 1. Rigid body with anchor points

The positions of the anchor points in $\mathbb{R}^2$ determine the embedding

$$\mathscr{C}(S) \subset \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2.$$

The image is the set

$$\{(x_1, x_2, x_3) \in \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2;\ |x_1 - x_2| = c_{12},\ |x_1 - x_3| = c_{13},\ |x_2 - x_3| = c_{23}\},$$

where c_{12}, c_{13}, c_{23} are distances between the corresponding anchor points.

Example 2. Similarly to the previous example, the configuration space of a rigid body in $\mathbb{R}^3$ can be embedded into $(\mathbb{R}^3)^4$ by specifying positions of 4 anchor points.

Example 3. An interesting class of mechanical systems form linkages built out of rigid bars and revolving joints with some of the joints of the linkage being pinned in space while the others are capable of moving freely. Figure 2 depicts the famous Peaucellier–Lipkin inversor. The point O is pinned and when the point D moves along the straight line the point B moves along the circle passing through O, see [11], §40.

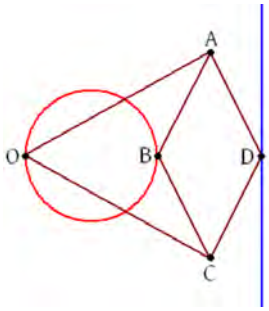


Figure 2. Peaucellier–Lipkin linkage

This linkage played an important role in the history of the industrial revolution. A steam engine contains a piston moving along a straight line up and down the cylinder and the mechanical part of the engine converts the straight line motion of the piston into circular motion of the wheels, i.e. it functions similarly to the linkage of Figure 2.

Example 4. Consider the system consisting of k disjoint round balls of radius $r > 0$ moving in space $\mathbb{R}^3$.

Figure 3. A configuration of the system of Example 4 with $k = 5$

A configuration of this system is determined by the locations $c_i \in \mathbb{R}^3$ of the centres of the balls, where $i = 1,2,\ldots,k$. The centres must satisfy the inequalities $|c_i - c_j| \geq 2r \quad$ for $\quad i \neq j$. Thus in this case

$$\mathcal{C}(S) = \{(c_1,\ldots,c_k) \in (\mathbb{R}^3)^k;\ |c_i - c_j| \geq 2r \ \text{ for } i \neq j\}.$$

It is natural to ask how large is the class of configuration spaces of mechanical systems. There exist many mathematical theorems which answer this question asserting roughly that this class is extremely large. We state below the universality theorem of D. Jordan and M. Steiner [12].

Theorem 1 (See [12]). *Any compact real algebraic variety is homeomorphic to the union of some components of the configuration space of a planar mechanical linkage.*

Autonomous robots and motion planning algorithms

Imagine the following situation. A robot receives an order to move from its current state to a prescribed state. This command is given in one of the natural languages (say, in English) and the robot must decide by itself how to implement it. To solve this problem the robot needs *a motion planning algorithm* which generates a specific robot motion once the initial and the final states are given.

If X is the configuration space of the robot (equipped with its natural topology, see above) then a motion planning algorithm is a function which associates to every pair $(x,x') \in X \times X$ of states a continuous curve $\gamma(t) \in X$, where $t \in [0,1]$, starting at $x = \gamma(0)$ and ending at $x' = \gamma(1)$.

Clearly, if the topological space X is path-connected, then for every pair of states $(x,x') \in X \times X$ such a continuous path γ exists. However, our task is not to specify a solution γ for a specific pair (x,x') but rather to design a globally defined algorithm (i.e. a function) which produces such a path γ as an output once the pair (x,x') is given, as an input.

We shall denote by $I = [0,1]$ the unit interval whose points parametrise the time moments, $t \in [0,1]$. The symbol X^I will stand for the space of all continuous maps $\gamma : I \to X$. The function space X^I carries the compact-open topology. Recall that a prebase of the compact-open topology is formed by the sets $\langle K,U\rangle$, where $K \subset I$ is compact and $U \subset X$ is open, and $\langle K,U\rangle$ is defined as $\{\gamma \in X^I; \gamma(K) \subset U\}$.

The evaluation map

$$p : X^I \to X \times X, \quad p(\gamma) = (\gamma(0),\gamma(1)), \qquad (2)$$

is obviously continuous: the pre-image of the open set $V_1 \times V_2 \subset X \times X$ is the inetrsection $\langle\{0\},V_1\rangle \cap \langle\{1\},V_2\rangle$ of two open sets of the prebase. The map p is known as *the path-fibration*. The discussion above can now be expressed as follows: a motion planning algorithm is a map $A : X \times X \to X^I$ satisfying

$$p \circ A = 1_{X\times X},$$

i.e. it is *a section* of the path-fibration (2).

Lemma 1 (See [2]). *A continuous motion planning algorithm $A : X \times X \to X^I$ exists if and only if the space X is contractible.*

Proof. A path-connected topological space X is contractible if there exists a continuous map $a : X \to X^I$ (called a contraction) such that for every $x \in X$ one has $a(x)(0) = x$ and $a(x)(1) = x_0$ where $x_0 \in X$ is a fixed point. A continuous motion planning algorithm $A : X \times X \to X^I$ defines a contraction

$$a(x)(t) = A(x,x_0)(t)$$

where $x \in X$ and $t \in I$. Conversely, suppose that X is contractible, and let $a : X \to X^I$ be a contraction. Then a continuous motion planning algorithm can be defined by

$$A(x,x')(t) = \begin{cases} a(x)(2t), & \text{for} \quad 0 \leq t \leq 1/2, \\ a(x')(2-2t), & \text{for} \quad 1/2 \leq t \leq 1, \end{cases}$$

i.e. the motion from x to x' first follows the contraction which brings x to x_0 and then it follows the reversed path of x'.

Corollary 1. *For a system with non-contractible configuration space any motion planning algorithm is discontinuous.*

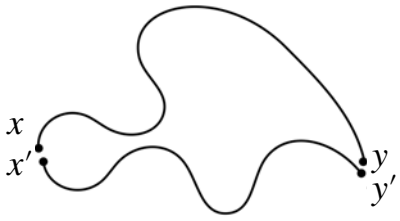


Figure 4. Discontinuity of a motion planning algorithm

Having in mind the Universality Theorem 1, we understand that typically motion planning algorithms will have discontinuities which appear as pairs $(x,y) \in X \times X$ such that arbitrarily close to (x,y) there exist pairs (x',y') with the property that the motion $A(x',y')(t)$ is essentially distinct from the motion $A(x,y)(t)$, see Figure 4.

Example 5. Suppose that the configuration space $X = S^1$ is the unit circle on the complex plane.

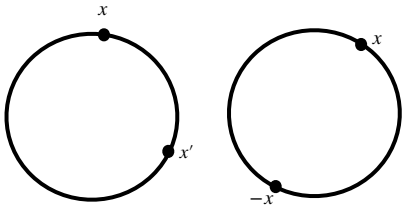


Figure 5. Motion planning algorithm on the circle

The circle is the configuration space of a wheel or of a planar pendulum. One can partition the space $X \times X$ into two sets $X \times X = F_0 \sqcup F_1$ where $F_0 \subset X \times X$ consists of all non-antipodal pairs (x,x'), $x \neq -x'$ and the remaining set $F_1 \subset X \times X$, where $F_1 = \{(x,-x); x \in X\}$ consists of the antipodal pairs. A continuous section $A_0 : F_0 \to X^I$ over F_0 can be defined by setting $A_0(x,x')(t)$ to be the shortest geodesic arc connecting x to x', see Figure 5. If the points x and x' are antipodal, i.e. $x' = -x$, then there are two shortest geodesic arcs connecting x to x'. We shall fix an orientation of the circle and use it to define a continuous section $A_1 : F_1 \to X^I$ over F_1. We define $A_1 : F_1 \to X^I$ by setting $A_1(x,x')(t)$ to be the motion from x to $x' = -x$ in the direction of the orientation with constant velocity.

Thus we obtain a motion planning algorithm for the circle having two continuity domains F_0 and F_1. By Corollary 1, no globally defined continuous motion planning algorithm $X \times X \to X^I$ exists since the circle is not contractible.

Example 6. Consider a robot arm with k bars schematically depicted in Figure 6. We assume that each bar can rotate 360 degrees independently of the other bars.

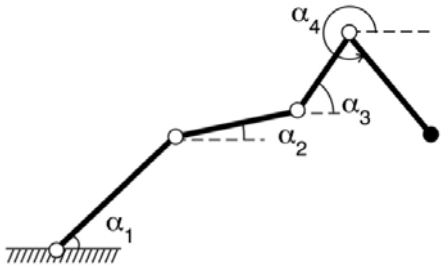


Figure 6. Robot arm with 4 bars

Hence a state of the arm is determined by k angles, i.e. k points on the unit circle $(z_1,\dots,z_k) \in (S^1)^k = T^k$, i.e. the configuration space of the arm is the k-dimensional torus T^k. We may describe a motion planning algorithm for the robot arm as follows. For a subset $J \subset \{1,2,\dots,k\}$ we denote by $F_J \subset T^k \times T^k$ the set of all pairs of configirations $(z_1,z_2,\dots,z_k) \in T^k$ and $(z_1',z_2',\dots,z_k') \in T^k$ such that $z_i = -z_i'$ if and only if $i \in J$. We may define a continuous section $A_J : F_J \to (T^k)^I$ using the construction of Example 5: for $i \notin J$ we let z_i move towards z_i' along the shortest geodesic arc and for $i \in J$ we order z_i to move towards z_i' along the geodesic arc in the direction of the orientation of the circle. Since J may be arbitrary, we obtain 2^k domains F_J on which our algorithm is defined and is continuous. Note that $F_J \cap F_{J'} = \emptyset$ for $J \neq J'$ and the union $\cup_J F_J$ equals $T^k \times T^k$.

The domains F_J can be "repackaged" into $k+1$ "aggregated" domains as follows. For $s = 0,1,\dots,k$ let F_s denote the union of all domains F_J with $|J| = s$. We note that the closure $\overline{F}_J$ equals the union of the domains F_K with $K \supseteq J$. Thus, if $|J| = |J'|$ one has $\overline{F}_J \cap F_{J'} = \emptyset = \overline{F}_{J'} \cap F_J$. This implies that the continuous sections over the sets F_J define collectively a continuous section $A_s : F_s \to (T^k)^I$ where $s = |J|$. Thus we have the partition

$$T^k \times T^k = F_0 \sqcup F_1 \sqcup \dots \sqcup F_k$$

and on each of the sets $F_0,\dots,F_k$ we have a continuous section A_s.

The concept of topological complexity

The topological complexity $\mathrm{TC}(X)$ is an integer depending on the topology of the system's configuration space X which gives a useful measure of navigational complexity of the system. For every path-connected topological space X one defines $\mathrm{TC}(X)$ as the minimal integer $k \geq 0$ such that the Cartesian square $X \times X$ has an open cover

$$X \times X = U_0 \cup U_1 \cup \cdots \cup U_k \tag{3}$$

with the property that each set U_i admits a continuous section $A_i : U_i \to X^I$ of the fibration (2) where $i = 0,1,\ldots,k$. The latter means that the composition $p \circ A_i : U_i \to X \times X$ coincides with the inclusion $U_i \to X \times X$. Each such section A_i can be understood as *a local motion planning algorithm*: it is defined only for pairs (x,x') lying in U_i and the image $A_i(x,x')(t)$ is a continuous path in X starting at the point x and ending at the point x'.

We can rephrase Lemma 1 as follows:

Lemma 2. *A path-connected space X is contractible if and only if* $\mathrm{TC}(X) = 0$.

The concept $\mathrm{TC}(X)$ was originally defined and studied in [2]. Note that in [2] we used "the unreduced convention" according to which contractible spaces have complexity 1.

In a recent paper [8] it was shown that, for ANR spaces X, instead of open covers (3) one may use arbitrary partitions

$$X \times X = F_0 \sqcup F_1 \sqcup \cdots \sqcup F_k. \tag{4}$$

Any partition (4) with continuous sections $A_i : F_i \to X^I$ for $i = 0,1,\ldots,k$ define a motion planning algorithm $A : X \times X \to X^I$ which acts as follows: given an input pair $(x,x') \in X \times X$, find the index $i \in \{0,1,\ldots,k\}$ such that (x,x') lies in F_i, then apply $A_i(x,x')$.

The symbol ANR is the abbreviation of "absolute neighbourhood retract". The class of ANR's is very large; it includes all spaces which may appear as configuration spaces of mechanisms in practical robotics.

The construction of Example 6 gives $\mathrm{TC}(T^k) \leq k$, i.e. the topological complexity of the robot arm with k bars is at most k. We shall see below that in fact $\mathrm{TC}(T^k) = k$. To establish this fact we shall employ cohomology theory.

The role of the cohomology algebras

One may use cohomology algebras to give lower bounds for the topological complexity $\mathrm{TC}(X)$. A lower bound for $\mathrm{TC}(X)$ is essentially a lower bound on the number k of sets in any partition (4) for all possible motion planning algorithms for an arbitrary system having the space X as its configuration space. We shall see that this technique will help us to find the exact value of the topological complexity of the robot arm. However there exist examples when the cohomological lower bound is only a bound and is smaller than the topological complexity $\mathrm{TC}(X)$.

Let $H^*(X)$ denote the cohomology algebra of X with coefficients in a field $\mathbb{F}$ which can be arbitrary; the field $\mathbb{F}$ will not be mentioned in the notation. The product structure in $H^*(X)$ is called the cup-product. Here, for simplicity, we shall denote the product of cohomology classes $\alpha,\beta \in H^*(X)$ as $\alpha\beta$.

The cohomology is a graded algebra, $H^*(X) = \bigoplus_{s=0}^{\infty} H^s(X)$. For $\alpha \in H^s(X)$ we shall say that the class α has degree s and write $|\alpha| = s$. If X is path-connected then the vector space $H^0(X)$ is one-dimensional generated by the class $1 \in H^0(X)$.

The tensor product $H^*(X) \otimes_{\mathbb{F}} H^*(X)$ is an algebra with the product

$$(a \otimes b) \cdot (c \otimes d) = (-1)^{|b|\cdot|c|} \cdot ac \otimes bd. \tag{5}$$

Mapping a tensor $a \otimes b \in H^*(X) \otimes_{\mathbb{F}} H^*(X)$ to the product $ab \in H^*(X)$ defines an algebra homomorphism $\psi : H^*(X) \otimes_{\mathbb{F}} H^*(X) \to H^*(X)$.

Definition 1. We say that an element $\mathfrak{a} \in H^*(X) \otimes_{\mathbb{F}} H^*(X)$ is *a zero-divisor* if $\psi(\mathfrak{a}) = 0$.

As an example consider the tensor $\mathfrak{a} = v \otimes 1 - 1 \otimes v$ where $v \in H^*(X)$, $|v| > 0$. This element $\mathfrak{a} \in H^*(X) \otimes_{\mathbb{F}} H^*(X)$ is a zero-divisor since $\psi(\mathfrak{a}) = v1 - 1v = v - v = 0$.

Theorem 2 (See [2]). *Let X be a path-connected topological space. If for some $k \geq 1$ there exist k zero-divisors $\mathfrak{a}_1,\ldots,\mathfrak{a}_k \in H^*(X) \otimes_{\mathbb{F}} H^*(X)$, such that their product $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_k \in H^*(X) \otimes_{\mathbb{F}} H^*(X)$ is nonzero, then* $\mathrm{TC}(X) \geq k$.

This means that under the assumptions of Theorem 2 any motion planning algorithm for a system having X as its configuration space has at least $k+1$ local domains (4).

Example 7. Let us consider again the case of the planar robot arm with k bars, see Example 6. The configuration space is k-dimensional torus $X = T^k$ and the cohomology algebra $H^*(T^k)$ is the exterior algebra with generators $\alpha_1, \dots, \alpha_k \in H^1(T^k)$, $\alpha_i^2 = 0$ for $i = 1, \dots, k$. Each class α_i is induced from the standard generator $u \in H^1(S^1)$ via the projection $q_i : T^k \to S^1$ in the i-th factor, i.e. $\alpha_i = q_i^*(u)$.

We have the zero-divisors $\mathfrak{a}_i = \alpha_i \otimes 1 - 1 \otimes \alpha_i$, where $i = 1, \dots, k$. The product $\prod_{i=1}^k \mathfrak{a}_i$ can be represented as the sum

$$\sum_J \epsilon_J \left(\prod_{i \in J} \alpha_i \right) \otimes \left(\prod_{j \notin J} \alpha_j \right), \quad \epsilon_J = \pm 1, \qquad (6)$$

where $J \subset \{1, 2, \dots, k\}$ runs over all subsets including $J = \emptyset$. The terms of the sum (6) are linearly independent and hence the product $\prod_{i=1}^k \mathfrak{a}_i \neq 0$ is nonzero. Applying Theorem 2 and taking into account Example 6 we obtain:

Corollary 2. *The topological complexity of the planar robot arm with k bars equals k. In other words,* $\mathrm{TC}(T^k) = k$.

Topological complexity of spheres

First we apply Theorem 2 to the sphere $X = S^n$. The cohomology algebra of the sphere has the fundamental class $u \in H^n(S^n)$ satisfying $u^2 = 0$. There are two zero-divisors, $a = u \otimes 1 - 1 \otimes u$ and $b = u \otimes u$. Using formula (5) we find $a^2 = -[1 + (-1)^n] \cdot b$. We see that, for n even, $a^2 = -2b$ is nonzero, assuming that the characteristic of the field $\mathbb{F}$ is not 2. Hence, by Theorem 2, for n even one has $\mathrm{TC}(S^n) \geq 2$ and for n odd $\mathrm{TC}(S^n) \geq 1$.

Next we describe specific motion planning algorithms for spheres. As in the case of the circle (i.e. Example 5), we set $F_0 \subset S^n \times S^n$ to be the set of non-antipodal pairs and let $F_1 \subset S^n \times S^n$ be the set of antipodal pairs. We can define a continuous section $A_0 : F_0 \to (S^n)^I$ by associating with a pair (x, x') the shortest geodesic arc from x to x'. If the dimension n of the sphere is odd then S^n admits a continuous nowhere zero tangent vector field w, and we may use it to define a continuous section over F_1: with a pair $(x, -x)$ we associate the geodesic arc $A_1(x, -x)$ which starts at x in the direction of the tangent vector $w(x)$ and arrives at the point $-x$ after making the angle π. We conclude that $\mathrm{TC}(S^n) = 1$ for $n \geq 1$ odd.

For n even the sphere S^n admits no continuous non-vanishing tangent vector fields. However we may find a continuous tangent vector field w on S^n vanishing at a single point $x_0 \in S^n$. Let's consider the partition $S^n \times S^n = F_0 \sqcup F_1' \sqcup F_2'$ where F_0 is the set of non-antipodal pairs, F_1' is the set of all pairs $(x, -x)$ with $x \neq x_0$ and the set F_2' consists of a single pair $(x_0, -x_0)$. As above we may define continuous motion planning algorithms over F_0 and F_1'. Any path connecting x_0 to $-x_0$ on S^n defines a section over F_2'. Thus, we see that $\mathrm{TC}(S^n) \leq 2$ for n even. Combining this with the lower bound $\mathrm{TC}(S^n) \geq 2$ obtained above, we conclude $\mathrm{TC}(S^n) = 2$ for $n \geq 2$ even.

Some further developments

I want to finish this article by mentioning several further results and giving a few literature references.

In [7] the topological complexity of multiple collision-free moving objects in $\mathbb{R}^d$ was established and some explicit motion planning algorithms of minimal complexity were designed.

As a surprise we discovered in [3] that the topological complexity of real projective spaces coincides with their immersion dimension (except in dimensions 1, 3, 7). A few years later it was understood that the symmetric topological complexity of the real projective spaces (properly normalised and with a few exceptions) coincides with their embedding dimension, see paper by J. González and P. Landweber [9].

In paper [1] new types of motion planning algorithms were proposed and analysed. These are *the parametrized motion planning algorithms* which can work under variable external conditions, are universal and flexible. In [6], explicit motion planning algorithms were developed for autonomous collision-free motion of many robots in the presence of many moving obstacles. This approach has great potential; it accounts not only for the configuration space of the controlled robot but includes into the picture the configuration space of the external conditions (such as obstacles and other moving objects etc).

The monograph [4] summaries the developments of the subject which happened by 2006.

The volume [10] is a collection of articles, it reflects many more recent developments.

Michael Farber

Michael Farber is a professor in the School of Mathematical Sciences of the Queen Mary University of London. His main research interests are in algebraic and differential topology and their applications in engineering, statistics and computer science. Michael studies knot theory, topology of closed 1-forms, convex billiards, topology of configuration spaces of linkages and some other problems of topological robotics.

FURTHER READING

[1] D.C. Cohen, M. Farber and S. Weinberger, *Parametrised topological complexity of collision-free motion planning in the plane.* "Annals of Mathematics and Artificial Intelligence", **90**(2022), pp. 999-1015.

[2] M. Farber, *Topological complexity of motion planning*, Discrete & Computational Geometry, **29**(2003), no. 2. pp. 211–221.

[3] M. Farber, S. Tabachnikov and S. Yuzvinsky, *Int. Math. Res. Not.* (2003), no. 34, 1853–1870.

[4] M. Farber, *Invitation to topological robotics*. Zurich Lectures in Advanced Mathematics, EMS, 2008.

[5] M. Farber, *Collision free motion planning on graphs.* in: "Algorithmic Foundations of Robotics IV", M. Erdmann, D. Hsu, M. Overmars, A. Frank van der Stappen editors, Springer, 2005, pp. 123 - 138.

[6] M. Farber, S. Weinberger, *Parametrized motion planning and topological complexity,* "Algorithmic Foundations of Robotics, XV", S. LaValle et. al. editors, Springer 2023, pp 1 - 17.

[7] M. Farber, M. Grant, *Topological complexity of configuration spaces*, Proc. Amer. Math. Soc. **137** (2009), no. 5, 1841–1847.

[8] J. M. García-Calcines, *A note on covers defining relative and sectional categories*, Topology Appl. **265** (2019), 106810, 14 pp.

[9] J. González, P. Landweber, *Symmetric topological complexity of projective and lens spaces.* Algebr. Geom. Topol. **9**(2009), no.1, 473–494.

[10] M. Grant, G. Lupton and L. Vandembroucq editors, *Topological Complexity and Related Topics*, Contemporary Math, AMS, volume 702, 2018.

[11] D. Hilbert and S. Cohn-Vossen, *Geometry and the imagination*, Chelsea Publishing Co., New York, 1952, ix+357 pp.

[12] D. Jordan, M. Steiner, *Configuration spaces of mechanical linkages*, Discrete Comput. Geom., **22** (1999), pp. 297-315

Preventing the Quantum Crypto-Apocalypse with Linear Algebra with Errors

NIGEL P. SMART

Quantum computers threaten to render our modern digital world insecure, as they enable the breaking of all the deployed public key cryptographic algorithms which secure the internet. Recently, the American National Institute for Standards and Technology have published their proposals to mitigate this threat. The majority of the solutions utilise easy to explain problems in linear algebra.

Introduction

Our modern digital infrastructure is secured using the mathematics of cryptography. Whether this be securely accessing a web-site, communicating via secure messaging services such as WhatsApp or Signal, authenticating oneself to corporate networks or banks; all these applications require cryptography. Indeed usually it is a form of public key cryptography.

In public key cryptography there are two keys; one public (which anyone can have, indeed one usually publishes it on a website or whatever), and one secret (which really must remain secret for the system to be secure). When used for encryption, the public key is used to encrypt a message, and the private key is used for decryption. This enables anyone to send the holder of the private key a message securely. When used for digital signatures, the public key is used to verify that the message did indeed originate from the person who held the secret key.

The algorithms used to secure the internet today are based on two basic problems from first year undergraduate mathematics; the factoring problem and the discrete logarithm problem. Sufficiently large instances of these problems are currently so difficult to solve, even for the world's most powerful computers, that we can reliably base security on them for a wide range of important applications.

The problem is that these two problems may not remain hard for very much longer. The so-called quantum crypto-apocalypse is coming, in which the existence (or even threat of existence) of a large enough quantum computer will render the above two problems easy. This would mean the instant collapse in trust of the digital infrastructure on which our modern society depends. Luckily, just as in some Hollywood movie, a small band of cryptographic heroes have the tools at hand to protect us from the crypto-apocalypse. In 2023 we saw the culmination of these heroic efforts with the publication by NIST (the American National Institute for Standards and Technology) of its first post-quantum cryptographic standards [2]. Luckily, for the world of undergraduate cryptography, the underlying hard problems also come from the world of first year undergraduate mathematics; namely linear algebra.

Classical Public Key Cryptography

There are two basic mathematical problems underlying the public key cryptography which we currently use on the internet: the factoring and discrete logarithm problems. A third problem, of finding solutions to knapsack problems, is also of historical importance, and becoming more so as we shall see. These three problems were introduced in the mid 1970s in a flurry of papers by six American-based researchers: Diffie, Hellman, Merkle, Rivest, Shamir and Adleman.

The first problem is that of factoring large integers: It is believed that if I give you an integer N and tell you that $N = p \cdot q$, for some secret large prime numbers p and q, then it is hard for you to find p and q. What this problem is actually setting up is a finite abelian group of secret order. We are creating a public group

$$(\mathbb{Z}/N\mathbb{Z})^* = \{x \ : \ 1 \leq x < N, \gcd(x, N) = 1\}$$

for which the group order is secret. Basic undergraduate group theory/elementary number theory tells us that the group order, if $N = p \cdot q$ for primes p and q, is given by Euler's phi function

$$\phi(N) = (p-1) \cdot (q-1).$$

So if you do not know the primes p and q then you do not know $\phi(N)$ and hence you do not know the order of the above finite abelian group.

The second problem is also related to finite abelian groups, but groups of known large prime order. Suppose I have a multiplicative group G whose order is a large prime q. If I draw a random element $g \in G$ and pick a random integer $x \in \mathbb{Z}/q\mathbb{Z} = \{0, \ldots, q-1\}$, then I can easily compute the value

$$h = g^x$$

in the group. The problem is that given (g, h) it is, for suitably chosen groups G, hard to find x. The finding of x given (g, h) is said to be finding the discrete logarithm of h with respect to g.

In the real world one selects G to be a subgroup of an elliptic curve group, but for expository purposes (and often in undergraduate introductory courses) one thinks of a G as being a large prime subgroup of the multiplicative group of a finite field $\mathbb{F}_p^*$.

Historical Aside

The idea of public key encryption and digital signatures was announced publicly in a beautiful paper [1] by Diffie and Hellman in 1976. In this paper they explained the ideas, but could not come up with a practical instantiation. Although they did introduce the discrete logarithm problem whilst describing the famous Diffie–Hellman key exchange protocol (which is now used when you connect to a website with your browser).

In 1977, Ron Rivest, Adi Shamir and Len Adleman, came up with an algorithm (called the RSA algorithm) which practically gave public key encryption and digital signatures and was based on the factoring problem. With Merkle and Hellman coming up with public key cryptosystem based on the knapsack problem in 1978.

It was revealed many years later, that in GCHQ in Cheltenham the idea of public key encryption was conceived by James Ellis in 1970, that a scheme very similar to the RSA encryption scheme was conceived by Clifford Cocks in 1973, and in 1974 Malcolm Williamson had conceived of the idea of Diffie–Hellman key exchange.

Another easy to explain, but hard to solve problem, introduced by Merkle and Hellman, was the knapsack problem. This problem can be stated, in one of its forms, as follows: Given a modulus q, an integer n and a set of weights $w_i \in \mathbb{Z}/q\mathbb{Z}$, for $i = 1, \ldots, n$, and a value $s \in \mathbb{Z}/q\mathbb{Z}$, to find a solution (if it exists) to the equation

$$x_1 \cdot w_1 + \ldots + x_n \cdot w_n = s \pmod{q},$$

where we restrict the solutions to be single bits, i.e. we require a solution with $x_i \in \{0, 1\}$. However, this problem, whilst as old in cryptography as the factoring and discrete logarithm problem, has had less traction in real world systems. It is however closely related to the problems of noisy linear algebra which we will return to below.

Figure 1. Merkle, Hellman and Diffie (Chuck Painter/Stanford News Service)

These three problems of factoring, discrete logarithms and knapsack algorithms are amazingly useful. They can they be explained using basic first year undergraduate mathematics, yet are hard to solve. In addition, the factoring and discrete logarithm problems can be easily turned into efficient cryptographic algorithms for both encryption and digital signatures. They were originally introduced in the 1970s, when public key cryptography was invented, and have stood the test of time. Despite over 50 years of research there is no known classical algorithm which can solve these three problems efficiently.

Figure 1. Shamir, Rivest and Adleman
(Printed with permission of Ron Rivest)

Two parts of the last sentence are important. Firstly, it talks about a classical algorithm. This is an algorithm which can be executed on a normal computer, such as the one on your desktop, or one which resides in a big data centre of Amazon, Apple, Google, Meta, or Microsoft. The second important word is that we are interested only in efficient algorithms, i.e. something which will solve the underlying mathematical problem in the lifetime of the data being secured. There are obviously naive algorithms which can solve all three of these problems, but these naive algorithms are all inefficient.

Quantum Cryptanalysis

A classical computer operates on binary digits, all data is broken down into an on or off signal, i.e. a value from the set $\{0,1\}$. There is however a form of computation which uses the properties of quantum mechanics. At its heart a so-called quantum computer acts on quantum bits. A quantum bit is like a normal bit, but it can be both simultaneously zero and one; just as the famous Schrödinger's cat can be simultaneously both alive and dead.

Quantum algorithms are very different from normal algorithms, and only certain problems seem to be able to be accelerated via the use of a quantum computer. The most famous quantum algorithm is Shor's algorithm, which was invented in 1994 [4]. At its heart, Schor's algorithm enables one to find a hidden subgroup in finite abelian groups very fast. In other words given two groups G_1 and G_2 and a group homomorphism $f : G_1 \longrightarrow G_2$, then Schor's algorithm finds the kernel of f.

Given an algorithm to find hidden subgroups we can find the order of an element $a \in G$ where G is a finite abelian group. We just take $G_1 = \mathbb{Z}$ to be the group of integers under addition, $G_2 = G$, with the map f being $f(x) = a^x$ for the fixed value $a \in G$. Determining the kernel of this map gives us the order of a in the group G, i.e. we find $r \neq 0$ such that

$$a^r = 1.$$

To see how this can be used to factor an integer N, we take G to be the group $(\mathbb{Z}/N\mathbb{Z})^*$ above. We pick a random value $a \in G$ and apply Schor's algorithm to find r, if r is odd we repeat, otherwise we can assume r is even. Since r is even we can write

$$(a^{r/2} - 1) \cdot (a^{r/2} + 1) = 0 \pmod{N}.$$

This means the factors p and q of N divide one or both of the two factors on the left. The different possibilities happen with roughly equal probability, so we can find a factor N with high probability by computing

$$\gcd(a^{r/2} - 1, N).$$

If this does not result in a nontrivial factor of N, we repeat with a different value of a.

To solve discrete logarithms we look at the group homomorphism

$$f : \begin{cases} \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} & \longrightarrow & G \\ (a,b) & \longmapsto & g^a \cdot h^{-b} \end{cases},$$

where $h = g^x$ is the discrete logarithm we are trying to solve. The kernel of this map is all elements in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ which are multiples of $(x,1)$, i.e. by finding the hidden kernel we find the discrete logarithm.

It appears that quantum computers provide relatively little improvement when tasked with solving knapsack problems. Thus it appears that the old idea of Merkle and Hellman in using knapsack algorithms to create cryptographic systems may have some mileage in it. It turns out that a closely related problem to the knapsack problem does indeed provide the solution, as we shall see below.

The world's governments and large organisations are trying to build quantum computers, as they can be used for all sorts of things (and not just breaking cryptosystems). However, if such a quantum

computer would come along then we would need to upgrade all of our digital security protocols. This impending crisis has been called the quantum crypto-apocalypse.

Preventing the Quantum Crypto-Apocalypse

The world's cryptographers have known about the impending quantum crypto-apocalypse since Schor came up with his algorithm in 1994. For the next twenty years they have created a whole subfield called Post-Quantum Cryptography (or PQC). The area of PQC aims to come up with algorithms, which can run on classical computers, but which are resistant to the advent of a quantum computer. PQC algorithms are designed to be essentially drop-in replacements for our existing algorithms, which would not require many changes in infrastructure or computing capabilities.

There is another topic called Quantum Cryptography, which uses the properties of quantum mechanics to create cryptographic systems. However, such systems usually require special hardware and/or networks, and they have properties which mean they cannot be dropped into existing protocols on the internet. Whilst some companies are looking at quantum cryptography, the main focus of companies and governments is on PQC; thus this is where we shall place our focus for the rest of the article.

PQC uses a variety of supposedly hard mathematical problems on which to base its security. Some scheme utilise problems based on breaking cryptographic schemes such as block-ciphers or hash functions. Such primitives are able to be 'attacked' by another quantum algorithm (called Grover's search algorithm); but the effect of this algorithm on the overall security is negligible. Other schemes utilise the problem of finding solutions to large systems of quadratic equations modulo two, others make use of hard problems arising from coding theory, others make use of a problem called Learning-with-Errors (which we will return to below).

In 2017 the American organisation NIST issued a call for PQC algorithms. In this call it requested teams to submit proposals for new cryptographic algorithms to prevent the quantum crypto-apocalypse. Unlike the AES and SHA-3 'competitions', which had a definitive winner, the PQC 'process' would not be a competition as the expectation was that it would have multiple algorithms output at the end. Despite the fact it was not a competition, this did lead most cryptographers to treat it as one.

The first round of submissions to NIST consisted of 69 different algorithms. After two years of public analysis these were whittled down, in 2019, to a set of 26 second round candidates. Then in 2020, there were announced seven 'finalists', along with eight alternate algorithms (which were to be considered as back-up algorithms). Finally, in 2022 NIST announced the first set of four 'winners', [2]. These four algorithms, Kyber, Dilithium, Falcon and SPHINCS, contained three which were based on Learning-with-Errors (namely Kyber, Dilithium and Falcon). The first draft standards were published in August 2023, with the final standards being expected to be published sometime in 2024.

NIST and Crypto-Competitions

There is a long tradition of NIST organising public competitions for creating new cryptographic standards which are adopted worldwide and not just internally within the USA.

In the mid 1990s it was clear that the workhorse block cipher, called the Data Encryption Standard (DES), was in need of replacement. It had first been deployed in the mid 1970s, but by the early 1990s was considered too weak. Between 1997 and 2000, NIST organized the Advanced Encryption Standard (AES) competition. This resulted in the selection of a Belgian algorithm (Rijndael) to be the new AES algorithm. Whilst DES is still in use (in 2023) in some banking applications, almost all usages of DES in the real world have now been replaced by AES.

A similar situation occurred with hash functions. These are functions which compress data in a cryptographically secure way. Previous algorithms, such as MD5, SHA-1 etc had been shown to be very weak indeed by the early 2000s. Thus between 2008 and 2012, NIST organized a hash function competition to design a new algorithm, to be called SHA-3. In 2012 they selected another Belgian algorithm (Keccak) to be SHA-3.

Learning-with-Errors

The most promising post-quantum algorithms are those based on so-called lattice problems, in particular one technically called Learning-with-Errors (or LWE), see [3] for a complete mathematical treatment of the underlying problem. One interesting aspect of LWE is that, just like factoring, discrete logarithms and knapsack problems, can be explained to a first year undergraduate, so can LWE. This is because LWE arises from a standard problem in Linear Algebra. One could even call it a form of Linear Algebra with Errors.

The basic idea is as follows. Suppose we have a large linear system of equations modulo an integer q. To set this system up we fix a dimensions n, and then generate a random matrix A, with n rows and n columns, with entries lying in $\mathbb{Z}/q\mathbb{Z}$. Here think of q as a prime such as 65537, with n being around 256 (other sizes are possible, we just use these to fix the reader's ideas as to what order of magnitude of numbers we are talking about). If q is prime, then, with probability $1/q$, the matrix A will be invertible.

Consider the map

$$f_A : \left\{ \begin{array}{ccc} (\mathbb{Z}/q\mathbb{Z})^n & \longrightarrow & (\mathbb{Z}/q\mathbb{Z})^n \\ \mathbf{s} & \longrightarrow & A \cdot \mathbf{s} \end{array} \right.$$

With probability $1/q$ this map is injective, i.e. for each image there is at most one preimage. If we evaluate many values of this map, with different matrices, then the probability that there is more than one preimage becomes vanishingly small. i.e. if I give you $\mathbf{b}_1 = f_{A_1}(\mathbf{s})$ and $\mathbf{b}_2 = f_{A_2}(\mathbf{s})$ for random matrices A_1 and A_2 then the probability there is more than one $\mathbf{s}$ in the preimage is bounded by $1/q^2$, when q is prime.

Now we can pick an n-dimensional vector $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$, which we think of as our secret, and we use as our public values $\mathbf{b}_i = f_{A_i}(\mathbf{s}) = A_i \cdot \mathbf{s}$, for various random matrices A_i. Computing f_{A_i} in the forward direction requires n^2 multiplications modulo q. Computing $f_{A_i}^{-1}$, i.e. given $\mathbf{b}$ determine $\mathbf{s}$, requires slightly more operations. To invert we essentially need to form an inverse of A_i, which naively would require n^3 operations.

This gap in difficulty between the forward and reverse directions of computing f_{A_i} is not enough for cryptographic purposes. But interestingly it was mentioned in the original Diffie–Hellman paper [1] as a feasibility result on the existence functions which are easy to compute in one direction, but hard in another.

To try to fix this problem let us generalise the map f_A slightly. Now let us consider the map

$$f_A : \left\{ \begin{array}{ccc} (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^n & \longrightarrow & (\mathbb{Z}/q\mathbb{Z})^n \\ (\mathbf{s}, \mathbf{e}) & \longrightarrow & A \cdot \mathbf{s} + \mathbf{e} \end{array} \right.$$

where we select A again as a public random $n \times n$ matrix with coefficients in $\mathbb{Z}/q\mathbb{Z}$. Now we have a different problem: If we fix $\mathbf{s}$ and apply the map a number of times to obtain values $\mathbf{b}_i = f_{A_i}(\mathbf{s}, \mathbf{e}_i) = A_i \cdot \mathbf{s} + \mathbf{e}_i$, then the pairs $(A_i, \mathbf{b}_i)$ do not fix $\mathbf{s}$ to a single value at all. Since for all possible $\mathbf{s}$, and all matrices A_i, there is a vector $\mathbf{e}_i$ which satisfies the required equation.

So we somehow want to restrict this error term $\mathbf{e}$ we add on in two ways:

- We need repeated applications of the map f_A for different matrices A, and different error vectors $\mathbf{e}$, to fix (or commit in the cryptographic jargon) the secret vector $\mathbf{s}$.
- We need the map f to be hard to invert, i.e. given values $(A_i, \mathbf{b}_i)$ it should be hard to find $\mathbf{s}$.

The idea is to make $\mathbf{e}$ small? But what does being small mean? After all the entries of $\mathbf{e}$ are chosen modulo q, and there is no notion of 'distance' modulo q.

The solution is to think of the entries of $\mathbf{e}$ as being reduced modulo q into a centered range, i.e. instead of thinking of $\mathbb{Z}/q\mathbb{Z}$ as the set $\{0, \ldots, q-1\}$, to instead think of it as $\{-\lfloor q/2 \rfloor, \ldots, \lfloor q/2 \rfloor\}$. Then we can think of an entry modulo q of being small, if it is close to zero when considered in this range.

Having decided what small means, we now have to decide 'how small'. The usual answer to this question is to pick the entries of $\mathbf{e}$ from a distribution which looks a bit a like a Gaussian distribution, i.e. there should be a higher weight associated to smaller values than larger ones. For example, one could select the i-th entry e_i of $\mathbf{e}$ to be chosen such that

$$e_i = \sum_{j=1}^{B} (b_j - b'_j)$$

where b_j and b'_j are chosen from $\{0, 1\}$ with probability one half. So for example if we selected

$B = 1$ in the above we would have the probability distribution

$$\begin{aligned}\Pr[e_i = -1] &= 1/4,\\ \Pr[e_i = 0] &= 1/2,\\ \Pr[e_i = 1] &= 1/4.\end{aligned}$$

Let us call this distribution $\mathcal{D}_B$, and again we abuse notation by letting this denote both the distribution and the underlying set.

We then define our map as

$$f_A : \begin{cases} (\mathbb{Z}/q\mathbb{Z})^n \times \mathcal{D}_B^n & \longrightarrow \quad (\mathbb{Z}/q\mathbb{Z})^n \\ (\mathbf{s}, \mathbf{e}) & \longrightarrow \quad A \cdot \mathbf{s} + \mathbf{e} \end{cases}$$

It turns out that this map, for suitably chosen values of n, q and B, has exactly the properties we want: It is hard to invert and it allows us to commit to the secret when repeated for various values of A and $\mathbf{e}$.

It also has an interesting other property, again for suitably chosen values. In the real method suppose we sample $\mathbf{s}$ and then sample pairs A_i and $\mathbf{e}_i$ and then compute $\mathbf{b}_i = f_{A_i}(\mathbf{s}, \mathbf{e}_i)$, we get a pairs $(A_i, \mathbf{b}_i)$. We could instead sample A_i and just pick $\mathbf{b}_i$ at random, and ignore $\mathbf{s}$ entirely. It appears hard, even for a quantum computer, to determine whether we picked the $\mathbf{b}_i$ using the correct method (using a vector $\mathbf{s}$), or we just picked $\mathbf{b}_i$ at random. This so-called indistinguishability property is why this hard problem (called Learning-with-Errors) is so fruitful in being able to construct cryptosystems which are resistent to quantum attacks.

Naively Encrypting using LWE

All that remains is to provide a mechanism to encrypt using this the map f_A above. The following is just a simple example, it is neither as efficient as the ones selected by NIST, nor is it as secure as the ones selected by NIST. However, it provides the basic idea as to how one can use LWE to encrypt a message to someone.

The receiver of the message (who is usually denoted Bob) first picks the secret $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ as above. They then construct a set of t evaluations of the map f_{A_i} for random values of A_i and $\mathbf{e}_i$, i.e. they compute

$$\mathbf{b}_i = f_{A_i}(\mathbf{s}, \mathbf{e}_i) = A_i \cdot \mathbf{s} + \mathbf{e}_i$$

for t different 'small' vectors $\mathbf{e}_i \in \mathcal{D}^n$ and t different random $n \times n$ matrices A_i with coefficients in $\mathbb{Z}/q\mathbb{Z}$.

By the indistinguishability property this set of t values $(A_i, \mathbf{b}_i)$ is indistinguishable from a random set of values. The set $\{(A_i, \mathbf{b}_i)\}_{i=1}^t$ is called Bob's public key, with the value $\mathbf{s}$ being Bob's private key.

Now the sender of a message (who is usually denoted Alice) gets Bob's public key, and encodes their message as an element $\mathbf{m} \in \{0,1\}^n$. Alice then picks a random vector $\mathbf{u} \in \{-1, 0, 1\}^t$ and computes

$$\begin{aligned} A &= \sum_{i=1}^{t} u_i \cdot A_i \pmod q, \\ \mathbf{b} &= \sum_{i=1}^{t} u_i \cdot \mathbf{b}_i \pmod q. \end{aligned}$$

Notice how this looks very similar to the knapsack problems we considered earlier. Indeed this part of the construction of our public key algorithm relies on knapsack problems being hard to solve.

The pair $(A, \mathbf{b})$ looks like an evaluation of the map $f_A(\mathbf{s}, \mathbf{e})$ for some vector

$$\mathbf{e} = \sum_{i=1}^{t} u_i \cdot \mathbf{e}_i$$

which has small coefficients, but the distribution of the coefficients of $\mathbf{e}$ is not the same as the distribution as used by Bob to choose the $\mathbf{e}_i$. This difference is not important in practice, and we can still treat $(A, \mathbf{b})$ as being indistinguishable from a random choice of A and $\mathbf{b}$.

Alice then adds her message $\mathbf{m}$ onto $\mathbf{b}$ by computing

$$\mathbf{c} = \mathbf{b} + \Delta \cdot \mathbf{m} \pmod q,$$

where $\Delta = \lfloor q/2 \rfloor$. To an outsider, since $(A, \mathbf{b})$ looks totally random (by the indistinguishability) the value $\mathbf{c}$ looks like a one-time-pad encryption of $\Delta \cdot \mathbf{m}$ under the random key $\mathbf{b}$. However, to the receiver Bob it looks very different since he can compute, given $(A, \mathbf{c})$, the value

$$\begin{aligned} \mathbf{c} - A \cdot \mathbf{s} &= (\mathbf{b} + \Delta \cdot \mathbf{m}) - A \cdot \mathbf{s} \pmod q, \\ &= \sum_{i=1}^{t} u_i \cdot (\mathbf{b}_i - A_i \cdot \mathbf{s}) + \Delta \cdot \mathbf{m} \pmod q \\ &= \mathbf{e} + \Delta \cdot \mathbf{m} \pmod q \end{aligned}$$

Now since $\mathbf{e}$ has entries which are small, we can take $\mathbf{c} - A \cdot \mathbf{s}$ and just divide by Δ and round the result, to return the message $\mathbf{m}$.

FURTHER READING

[1] W. Diffie, M.E. Hellman, New Directions in Cryptography, IEEE Trans. Info. Theory, Vol 22, 644–654, 1976.
[2] NIST. Post-Quantum Cryptography: PQC. csrc.nist.gov/projects/post-quantum-cryptography, 2023.
[3] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, Journal of the ACM 56 (2009) 1–40.
[4] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings FOCS (1994) 124–134.

Nigel Smart

Nigel is a part-time Professor of Cryptography in the COSIC research group at KU Leuven in Belgium. He was twice awarded an ERC Advanced Grant, and was previously vice-president of the International Association of Cryptologic Research. He co-founded Unbound Security in 2014, which was bought by Coinbase in 2022. He now spends his spare time advising other cryptographic start-ups across the globe, and going on holidays.

Notes of a Numerical Analyst

Discrete and Continuous

NICK TREFETHEN FRS

There are many parallels between phenomena of linear algebra (discrete) and differential equations (continuous). Here are two of my favourites.

Sturm–Liouville. Consider Wilkinson's $(2n+1)\times(2n+1)$ tridiagonal matrix of the form

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \qquad (1)$$

with the diagonal entries running from n down to 0 and up to n again. Theory tells us that the eigenvalues of A are distinct, though there's no such theorem for a pentadiagonal matrix. Yet the eigenvalues fall in nearly degenerate pairs, like these largest two for $n = 4$ and 8:

$$n = 4: \ 4.745, \ 4.747,$$

$$n = 8: \ 8.7461941826, \ 8.7461941832.$$

A continuous analogue is the Sturm–Liouville problem

$$y'' + |x|y = \lambda y, \quad -L < x < L$$

with $L > 0$ and $y(\pm L) = 0$. Again, theory tells us that the eigenvalues are distinct, though there's no such theorem for a fourth-order equation. Here are the largest eigenvalues for $L = 4$ and 8:

$$L = 4: \ 1.645, \ 1.682,$$

$$L = 8: \ 5.661892585, \ 5.661892595$$

These near-degeneracies are related to line- splitting effects in quantum mechanics.

Frozen coefficients. Suppose you have a family of matrices that are individually power-bounded, with all eigenvalues in the unit disk, like this pair:

$$A_1 = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}.$$

Must products like $A_1A_2A_1A_2\cdots$ converge to zero? Certainly not, since A_1A_2 has eigenvalues 0 and 4.

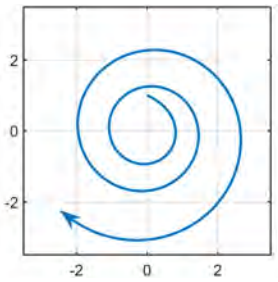


Figure 1. Solutions to a variable-coefficient linear ODE may diverge even though all the frozen-coefficient problems are stable.

A continuous analogue is the ODE

$$u' = Bu, \quad B = \begin{pmatrix} -1 & m \\ 0 & -1 \end{pmatrix},$$

which is stable since the eigenvalues are in the left half-plane. For $m > 2$ and $u(0) = [0,1]^T$, however, the solution $u(t)$ will grow before decaying. If we now define $A(t)$ to be B "rotated by t",

$$A(t) = S(t)BS(-t), \quad S(t) = \begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix},$$

solutions to $u' = A(t)u$ grow exponentially, as shown in the figure (with $m = 2.2$). Such effects were investigated by Lyapunov, Poincaré, Perron, and Vinograd, and this example comes from a celebrated paper by Kreiss about discrete-continuous analogues [1]. This effect is related to why flow in a pipe becomes turbulent even though the linearized problem is stable.

FURTHER READING

[1] H.-O. Kreiss, Über die Stabilitätsdefinition für Differenzengleichungen die partielle Differenzialgleichungen approximieren, *BIT*, 2 (1962), 153–181.

Nick Trefethen
Trefethen is Professor of Applied Mathematics in Residence at Harvard University.

Mathematics News Flash

Jonathan Fraser reports on some recent breakthroughs in mathematics.

After six enjoyable years on the Editorial Board of this Newsletter, my term has come to an end. That said, the plan is for me to continue to write these News Flash pieces, so please 'stay tuned'.

Small sumsets and a conjecture of Marton

AUTHORS: Tim Gowers, Ben Green, Freddie Manners and Terence Tao
ACCESS: https://arxiv.org/abs/2311.05762

Consider a finite set of positive integers A with $|A|$ denoting the number of elements in A. The associated *sumset* is the set $A+A$ consisting of all possible sums of pairs of elements from A. For example, if $A=\{1,2\}$, then $|A|=2$ and $A+A=\{1+1,1+2,2+1,2+2\}=\{2,3,4\}$. If A is unstructured or 'random' then it is likely that most pairs will give rise to a distinct sum and therefore the sumset is likely to be rather larger than the original set. Indeed, we might expect $|A+A|\approx|A|^2$. However, if A has lots of additive structure, then many pairs may produce the same sum and so the sumset might not be much larger than A. There are many deep questions—and some answers—concerning sumsets, often involving a careful quantification of heuristic ideas such as 'unstructured' or 'additive structure'.

Marton's conjecture (or the polynomial Freiman–Ruzsa conjecture) is of this type. In this case the integers are replaced with a finite field and the conjecture states (roughly speaking) that if the sumset is small, that is, if $|A+A|\leq K|A|$ for some constant $K>1$, then A must have 'a lot of additive structure', quantified by admitting a cover by 'not that many' copies of a single group of size at most $|A|$. Here, 'not that many' means at most polynomially in K. This paper, which appeared on the arXiv in November 2023, sensationally proved this conjecture in characteristic 2 (but the general case is forthcoming by the same approach).

The story does not end here. The above result (or rather, the proof) has become significant in another direction, namely, in the rapidly developing area of formal verification of mathematical proofs by computer. In early December 2023, Tao announced that lean had been able to formally verify their argument—and it took just a few weeks via a carefully coordinated collaborative process. Lean is a programming language capable of formally checking a mathematical proof step by step, provided the proof is written in a way the computer can understand. Imagine that the next 80-page paper you are asked to referee is written in this way, and you can simply verify the proof with the click of a button!

Unbounded fast escaping wandering domains

AUTHORS: Vasiliki Evdoridou, Adi Glücksam and Leticia Pardo-Simón
ACCESS: https://arxiv.org/abs/2210.13350

Given a transcendental entire function acting on the complex plane, the *Julia set* is the chaotic set for the action. It is a closed invariant set often with a subtle fractal structure. The complement of the Julia set is the *Fatou set* and consists of a collection of open connected components, known as *Fatou components*. A Fatou component is *wandering* if its forward orbit never becomes periodic and *escaping* if it 'wanders' to infinity. The fact that wandering domains can exist for transcendental entire functions is already in stark contrast to the case of rational maps—see Sullivan's celebrated *no-wandering-domain theorem* from 1985.

This paper, published in *Advances in Mathematics* in 2023, introduces a new technique for building examples of transcendental entire functions with unbounded wandering domains. This approach allows the authors to resolve significant problems, for example by exhibiting entire functions with an orbit of unbounded fast escaping wandering domains (answering a question of Rippon and Stallard) and by providing new 'lower order' examples connected to a conjecture of Baker.

Jonathan Fraser is a pure mathematician working at the University of St Andrews in Scotland. His research is mostly in analysis and often concerns fractals.

Microtheses and Nanotheses provide space in the Newsletter for current and recent research students to communicate their research findings with the community. We welcome submissions for this section from current and recent research students. See newsletter.lms.ac.uk for preparation and submission guidance.

Complexity of Random Substitution Subshifts

ANDREW MITCHELL

Subshifts of random substitutions provide theoretical models for quasicrystals: crystalline structures which exhibit a high degree of long-range order but lack translational symmetry. In this microthesis, I describe how entropy provides an invariant in the study of random substitution subshifts.

Quasicrystals and aperiodic order

The discovery of quasicrystals — naturally occurring substances that exhibit long-range order but lack translation symmetry — came as a surprise to physicists and materials scientists, and was honoured with the 2011 Nobel Prize in Chemistry. This discovery has stimulated a wealth of research in the field of *aperiodic order*, the mathematical study of quasicrystals, as non-periodic point sets provide models for the atomic positions in quasicrystals.

The prototypical examples of mathematical quasicrystals are sequences associated with *substitutions*, symbolic rules that replace each symbol (letter) in a finite set (alphabet) with a concatenation of symbols from the same set. For example, the *period doubling substitution* ρ is the rule $\rho\colon a \mapsto ab,\ b \mapsto aa$ that replaces every a in a given word or sequence with the word ab, and every b with the word aa. A dynamical system (subshift) can be associated with a given substitution in a canonical manner and, under mild assumptions on the substitution, the sequences in the associated subshift are non-periodic under the shift map. Notably, substitution subshifts have zero topological entropy, an indication of low complexity.

Random substitutions

Random substitutions are a generalisation of deterministic substitutions where the substituted image of a letter is chosen from a fixed finite set according to a probability distribution. Given $p \in (0,1)$, a random analogue of the period doubling substitution can be defined by

$$\vartheta\colon \begin{cases} a \mapsto \begin{cases} ab & \text{with probability } p, \\ ba & \text{with probability } 1-p, \end{cases} \\ b \mapsto aa \quad \text{with probability 1.} \end{cases} \tag{1}$$

The action of a random substitution is extended to finite words by applying it *independently* to each letter. Similarly to deterministic substitutions, a subshift can be associated with a random substitution in a natural way. Random substitutions share many features with their deterministic counterparts. For instance, their corresponding diffraction measure often has a non-trivial pure-point component, indicating long-range order. However, their subshifts often have positive topological entropy.

Topological entropy

The level of disorder in a dynamical system can be quantified via its *topological entropy*. For a subshift X, the *complexity function* $p_X\colon \mathbb{N} \to \mathbb{N}$ is the function which, for each $n \in \mathbb{N}$, returns the number of distinct words of length n that appear as a subword of a bi-infinite sequence in X. The topological entropy $h_{\text{top}}(X)$ of the subshift X quantifies the exponential growth rate of p_X. Specifically,

$$h_{\text{top}}(X) = \lim_{n\to\infty} \frac{1}{n} \log p_X(n), \tag{2}$$

where the above limit always exists since the sequence $\log p_X(n)$ is sub-additive. We highlight that if $h_{\text{top}}(X) = 0$, it is possible for p_X to grow polynomially, or faster than every polynomial but sub-exponentially. In this latter case, we say that the complexity function p_X has *intermediate growth*.

Determining the functions that can be obtained as the complexity function of a subshift is a central question in symbolic dynamics. A classical result in this direction is due to Morse and Hedlund (1938), which states that a subshift's complexity function either grows at least linearly, or is bounded above by a constant. Thus, there do not exist subshifts with $\Theta(\sqrt{n})$ complexity function, for example.[1]

For deterministic substitution subshifts, a complete classification of the possible asymptotic growth rates

[1]Given functions $f, g\colon \mathbb{N} \to [0,\infty)$, we write f is $\Theta(g)$ if there exist constants $C_1, C_2 > 0$ such that $C_1 < f(n)/g(n) < C_2$ for all $n \in \mathbb{N}$.

of complexity functions was provided by Pansiot (1984), who showed that the complexity function of a deterministic substitution subshift is either $\Theta(1)$, $\Theta(n), \Theta(n \log\log n), \Theta(n \log n)$ or $\Theta(n^2)$. Further, under a mild assumption on the substitution (namely, *primitivity*), only $\Theta(1)$ and $\Theta(n)$ are possible.

Random substitution subshifts often have non-zero topological entropy. As such, topological entropy provides a new invariant in their study not available for their deterministic counterparts. While subshifts of random substitutions typically have positive topological entropy, it is not true that *every* random substitution gives rise to a positive entropy subshift, since every deterministic substitution subshift can be obtained as the subshift of a random substitution. However, for *primitive*[2] random substitutions, the following dichotomy holds.

Theorem 3. *Let X be the subshift of a primitive random substitution. Then, $h_{\mathrm{top}}(X) = 0$ if and only if X can be obtained as the subshift of a (primitive) deterministic substitution.*

Combining the above with Pansiot's classification of complexity functions for deterministic substitutions yields that if X is the subshift of a primitive random substitution, then the only possible sub-exponential growth rates of its complexity function are $\Theta(1)$ or $\Theta(n)$. However, without primitivity, the picture is very different. In this more general setting, a much broader variety of complexity behaviour is possible. Specifically, non-primitive random substitutions can give rise to subshifts with intermediate growth complexity function, as well as polynomial growth not possible for subshifts of deterministic or primitive random substitutions – see [3] for more details.

Calculating topological entropy

In general, it can be difficult to obtain an exact value for the topological entropy, or even an accurate estimate, directly from the definition (2). However, for subshifts of primitive random substitutions, the topological entropy often coincides with the notion of *inflation word entropy*, which is characterised in terms of the underlying random substitution, as opposed to the subshift. Let ϑ be a random substitution such that for all $m \in \mathbb{N}$ and every letter a, every realisation of $\vartheta^m(a)$ has the same length, which we denote by $|\vartheta^m(a)|$. For each $m \in \mathbb{N}$ and each letter a, let $q_{m,a}$ denote the number of distinct realisations of $\vartheta^m(a)$. The inflation word entropy of type a is defined by

$$h_a = \lim_{m\to\infty} \frac{1}{|\vartheta^m(a)|} \log q_{m,a},$$

whenever this limit exists. In many cases, the limit h_a exists and coincides with $h_{\mathrm{top}}(X_\vartheta)$ – see [1, 3] for more details. For the random period doubling substitution defined in (1), this approach provides an exact value for the topological entropy. Namely, $h_{\mathrm{top}}(X_\vartheta) = h_a = \log(4)/3$.

Measure theoretic entropy

One limitation of topological entropy as a measure of complexity is that it is blind to the choice of probabilities associated with the random substitution. This is not the case for aspects such as word frequencies and diffraction spectra. Instead, these can be viewed as almost-sure properties with respect to an ergodic measure, which arises from the random substitution in a natural way. It is possible to treat entropy as a generic quantity with respect to this measure, capturing the underlying probability distribution. In a similar vein to topological entropy, this measure theoretic version of entropy often coincides with a related notion defined in terms of inflation words, which is typically easier to calculate or empirically estimate – see [2] for more details.

FURTHER READING

[1] P. Gohlke, Inflation word entropy for semi-compatible random substitutions, *Monatsh. Math.*, **192** (2020), 93–110.
[2] P. Gohlke, A. Mitchell, D. Rust and T. Samuel, Measure theoretic entropy of random substitution subshifts, *Ann. Henri Poincaré*, **24** (2023), 277–323.
[3] A. Mitchell, On word complexity and topological entropy of random substitution subshifts, *preprint*, available at arXiv:2305.04817.

Andrew Mitchell

Andrew completed his PhD at the University of Birmingham in 2023 and is now a postdoctoral researcher at the same institution. His main research interests lie in aperiodic order, ergodic theory and fractal geometry.

[2] A random substitution ϑ is primitive if there exists a $K \in \mathbb{N}$ such that for every pair of letters a and b, there is a realisation of $\vartheta^K(a)$ in which b appears as a subword.

How to Expect the Unexpected: The Science of Making Predictions and the Art of Knowing When Not To

by Kit Yates, Quercus, July 2023, £25, ISBN-13: 978-1529408683

Review by Neil Saunders

In *Finite and Infinite Games: A Vision for Life as Play and Possibility*, James P. Carse gave us the maxim: 'To be prepared against surprise is to be trained. To be prepared for surprise is to be educated' [1]. Like many maxims, they are easier said than done and Carse's maxim has a whiff of the paradoxical about it - surely if you are sufficiently educated, not much will surprise you; but then again, one learns a great deal from the various surprises life throws at us (how could it be otherwise?).

This is where Kit Yates' latest book, *How to Expect the Unexpected: The Science of Making Predictions and the Art of Knowing When Not To*, comes in. It is very much a continuation of his first book, *The Maths of Life and Death*, which this author also reviewed. Like in his first book, Yates' main strength as a writer of mathematics for general audiences is on display: drawing on a rich reservoir of stories and anecdotes from history, literature, psychology, science and mathematics, and skilfully weaving the relevant mathematical or statistical ideas into the lively recounting of such tales. It is true that reader will need a little more mathematical proficiency in this book as opposed to the last one, as Yates takes more time in explaining things like the birthday paradox or Bayes' Theorem with numbers and formulae - but this is not a bad thing, as Yates' friendly and accessible style is a joy to read.

*H*ow to Expect the Unexpected is a great primer for Steven Pinker's *Rationality* [3], Daniel Kanheman's *Thinking Fast and Slow* [2] and Daniel Dennett's *Intuition Pumps and Other Tools for Thinking* [4]. Each in their own way elucidate the idea that we humans, because of our evolutionary history, are bad at thinking probabilistically and are susceptible to all sorts of cognitive biases. But, over the course of thousands of years, we have developed (by trial and error, by learning from experience, by pure thought) some wonderful thinking tools that help us navigate the pitfalls and traps that have caught previous generations. In this book, Dennett states that 'some of the best thinking tools are mathematical', and here Yates shows the power of these tools in '...provid[ing] a framework for reasoning in the face of uncertainty'. In similar to Chomsky and Dennett, where they have argued that language's primary function is for thinking rather than communicating, Yates' book demonstrates that mathematics is another language that extends our cognitive reach, laying the ground for better, more prudent and reflective thinking.

Readers should have a notebook close to hand as they make their way through Yates' 400+ pages, particularly as he defines and gives examples of the various biases and fallacies that we often fall victim to: the Baader-Meinhof phenomenon (the frequency illusion where we learn something new and then seem to see it everywhere), the linearity bias (where we are fooled into believing that the relationship between two different phenomena is linear, when in fact it might be exponential, eg. the spread of viruses) and others like the normalcy bias, the Streisand effect, and 'curveballs', 'snowballs' & 'boomerangs'. Readers working in university departments will wince in the sections devoted to Goodhart's Law: 'when the metric becomes the target, it ceases to be a good metric' - think NSS, REF, TEF & KEF (and others yet to come!).

His examples of people falling victim to various biases can be amusing; in Chapter 2, Yates is explaining how genuine randomness tends to cluster, which the Bulgarian sports minister did not appreciate when in

2009, he launched an investigation into his country's lottery system after it produced the same numbers twice in a row. But they can also make you feel a little uncomfortable: the deliberately misleading interview Yates did with a spiritualist in Chapter 1, exposing all the tricks of trade such as the Barnum (or Forer) effect, did feel a little disingenuous. While reading that chapter, it further underlined how people who benefit from exploiting cognitive biases are often just as oblivious to them as 'their victims'.

However, Yates once again has done a great service to the mathematical community with his latest book (not to mention the advisory roles he has taken during and since the covid pandemic). A population that is mathematically literate and armed with a strong set of thinking tools can only be beneficial for the health of democracies, particularly with the rise of generative AI trained on our existing biases and exacerbating them further, creating new ones in the process. Human thinking - the process of using logic, reason, metaphor and mathematics - has never been more important, and Yates has made another excellent contribution to how we can harness its power, understand its limitations and better prepare ourselves for future surprises.

FURTHER READING

[1] J. P. Carse, *Finite and Infinite Games: A Vision for Life as Play and Probability*, Free Press, 2013.
[2] D. Kahneman, *Thinking Fast and Slow*, Penguin, 2012.
[3] S. Pinker, *Rationality: What It Is, Why It Seems Scarce, Why It Matters*, Viking, 2021.
[4] D. Dennett, *Intuition Pumps and Other Tools for Thinking*, W. W. Norton & Company, 2013.

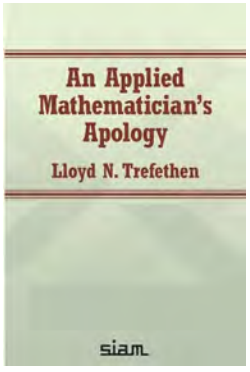
Neil Saunders

Dr Neil Saunders is a Senior Lecturer in mathematics at City, University of London. His research is in algebra and geometric representation theory. He was born in Australia and completed both his undergraduate and postgraduate studies at The University of Sydney. He's a keen cricketer and musician.

An Applied Mathematician's Apology

by Lloyd N. Trefethen, SIAM, 2022, RRP: £39.95, ISBN: 978-1611977189.

Review by Mark McCartney



The title of this short book by Nick Trefethen is a nod to GH Hardy's *A Mathematician's Apology*. The deliberate borrowing from the title of such a well-known book is of course potentially risky, as it invites comparison from stern lovers of Hardy's original (of which I am one), and that comparison may not be favourable. In my view, however, Trefethen manages to borrow the title with good grace. While Hardy gave an apologia for the art of the pure mathematician, Trefethen's apologia is for a very different branch of the mathematical tree: numerical analysis. And the two volumes are sufficiently different in style and content to prevent the aforementioned stern lovers of Hardy from feeling that the title of one of their favourite books has been unfairly nicked.

Numerical analysis is a Cinderella of applied mathematics. It is seen by many as useful, but dull. Applied mathematicians, physicists, chemists, climate modellers and a host of others are very happy that there are techniques to reliably solve their ODEs, PDEs and matrix problems by a simple function call, but ultimately, they take these things for granted. Trefethen, an eminent numerical analyst, takes up the sword to defend the importance of his discipline, and he does it with swash-buckling gallantry. Numerical analysis, he says, is "the heart of applied mathematics, the heart of mathematics, the heart of science… forty years of working in this area have given me a special vision of mathematics.

We numerical people are the ones who see the show live. It happens on our screens and at our fingertips. We *make it happen*. The energy of this experience has kept me going, decade after decade, and it's always something of a mystery to me why more mathematicians don't recognise numerical computation as an indispensable way to explore mathematics" (p.13, emphasis in the original).

Trefethen also emphasises the importance of what he calls 'laboratory mathematics': "Whatever the topic, I use the computer to guide me. This applies when I am working on algorithms and also when I am working on theoretical problems. ... I have long marvelled at how most mathematicians proved their theorems without taking advantage of this kind of help" (p23). I couldn't agree more. I have often pointed out to PhD students that I simply don't trust my own mathematics! Hopefully, it helps to put them at ease, but it also happens to be the truth. I am always looking for a check, a balance, a guide to what I do, and those checks and guides often come from numerical experiments.

I expect Hardy would have been appalled by both quotes above! As a mathematician, he was uncompromisingly pure and disdainful of anything he considered mathematically inelegant. I have little doubt that he would have looked with askance at numerical analysis.

Well, so much the worse for Hardy. There is, of course, nothing wrong with revelling in mathematical abstraction, arcana and the absence of application, but they are not in themselves virtues (even though the first two on the list are often necessities of any technical subject). Mathematics, pure, applied and 'laboratory', is all important, and it is refreshing to read a numerical analyst defend his cause with gusto.

Apart from acting as an apologia for numerical analysis, *An Applied Mathematician's Apology* also gives the reader a mixture of biography, anecdote, and observations on the differences and occasionally self-imposed barriers between the communities of applied and pure mathematics. The tone is conversational and along the way the author provides occasional golden nuggets as asides. For example, on the long-term behaviour of the random Fibonacci series (which grows as $(1.13178824\ldots)^n$). Or the fact that when he was at MIT, Trefethen was the first person on the planet to order a copy of MATLAB and he has a plaque from the company to prove it. Or that at Harvard he once had a bet with Bill Gates to see who could type fastest (to find out who won see p.12). It all adds up to produce a very enjoyable book.

At 79 pages, *An Applied Mathematician's Apology* can be read comfortably in an afternoon, and like Hardy's original *Apology* it deserves to be read widely by aspiring researchers and seasoned scholars alike.

Mark McCartney

Dr Mark McCartney is senior lecturer in mathematics at Ulster University. He is of the view that most situations can be improved by drinking tea and reading a good book. He is pained to note that this strategy does not work at all well during job interviews.

Obituaries

Ian G. Macdonald: 1928–2023

Professor Ian G. Macdonald, who was elected a member of the London Mathematical Society on 17 April 1958, died on 8 August 2023, aged 94. Professor Macdonald was awarded the LMS Pólya Prize in 1991.

Arun Ram writes: Ian Macdonald was born on 11 October 1928. His father worked in insurance; they lived in London. Ian attended Winchester College and earned a scholarship to Trinity College Cambridge. He turned 18 on 11 October 1946 and was thus lucky to avoid conscription but had to complete military service. In addition to Ian Macdonald, among the wranglers at Cambridge in 1952 were Frank Adams, John Polkinghorne, Ronald Shaw, James Mackay and Michael Atiyah. It was tough competition.

Ian Macdonald's father believed strongly in the security of a civil service job. Entrance to the service was by examination and, as usual, Macdonald did well. He said it was the most boring five years of his life but that he 'stuck it' for five years. Then he took a one-year contract at Manchester teaching mathematics (1957). In his words, "I had nothing to recommend me except a first class from Trinity from five years before". But "then one thing led to another" (a position at Exeter, 1960) and eventually he moved to a fellowship position at Oxford (1963, Magdalen college).

Macdonald returned to Manchester in 1972, and then held a chair at Queen Mary College, University of London from 1976 until his retirement.

In the six months between his military service and starting studies at Trinity, Macdonald worked on the writing of his first book, on Euclidean Geometry. The book was never published and the manuscript has been lost but a supplementary chapter on the Clifford sequence remains. By the time of Macdonald's first published paper (1958) he had developed this significantly further. In 1962 he published his — now very famous — paper on symmetric products of an algebraic curve, which established the Weyl conjectures for this case.

It is evident from the 1962 paper that Macdonald was well into understanding the very new, at the time, theory of the Weyl conjectures and the Grothendieck revolution in algebraic geometry. Macdonald's second book *Algebraic Geometry: An Introduction to Schemes*, published in 1968, provides an altogether elegant and enlightening exposition of the modern algebraic geometry, including K-theory, the Chow ring, the Hirzebruch–Riemann–Roch theorem and the Grothendieck–Riemann–Roch theorem. The book by Atiyah and Macdonald, *Introduction to Commutative Algebra*, appeared in 1969 and has shaped the education of generations of mathematicians.

Another important contribution of Ian Macdonald's was to provide the English translations of many volumes of Bourbaki and most of the volumes of Dieudonne's *Treatise on Analysis*.

The announcement of Macdonald's monograph *Spherical Functions on a Group of p-adic Type* (Madras 1972) appeared in 1968 and Macdonald gave an invited address on this work at the International Congress of Mathematicians in Nice in 1970. In this work he identified the spherical function for p-adic GL_n as what is now called a Hall–Littlewood polynomial and explained that the formula, as a sum over the elements of the Weyl group, generalises to all Lie types.

In July 1973 Macdonald gave a series of talks on Hall polynomials at the University of Warwick. His next book, *Symmetric Functions and Hall Polynomials*, appeared in 1979. It was "the belated fulfilment of an undertaking made some years ago to publish a self-contained account of Hall polynomials and related topics". It stimulated a huge interest and activity in research in algebraic combinatorics and, in particular, symmetric functions. In this book there is a full chapter devoted entirely to the Hall-Littlewood polynomials.

The second edition includes a chapter on what are now called Macdonald polynomials, a simultaneous generalisation of Schur functions and Hall–Littlewood polynomials and Jack polynomials. Macdonald's last book, *Affine Hecke Algebras and Orthogonal Polynomials*, was published in 2003, providing an exposition of the general theory of the Macdonald polynomials for affine root systems.

The story of how Macdonald's norm conjectures are related to Selberg's integrals and mathematical physics is an amazing chapter in mathematical history. Aspects of the miracle of these events are told wonderfully in Freeman Dyson's Gibb's lecture and Dyson's article *The Macdonald Equation*, which begins with the words

"The Macdonald Equation is the most beautiful thing that I ever discovered".

In 1989–90 Macdonald spent several months at University of California, San Diego, and gave courses on root systems and on Schubert polynomials. The book *Notes on Schubert Polynomials* was published in 1991, stimulating a huge amount of subsequent research in Schubert calculus: the intersection of algebraic combinatorics and the algebraic geometry of flag varieties. Other examples of Macdonald's expository writing are the notes *Linear Algebraic Groups* (1995) and *Algebraic Structure of Lie Groups* (1980), which appear in LMS volumes.

Tony Gardiner: 1947–2024

Dr Tony Gardiner, who was elected a Member of the London Mathematical Society on 18 November 1983, died on 22 January 2024, aged 76.

Alexandre Borovik writes: Tony Gardiner died suddenly on 22 January 2024. He will be remembered as a national treasure, a man who made a unique contribution to the development of mathematics education in this country and internationally.

Tony set up, and made significant contributions to the work of, the UK Mathematics Trust, which runs problem-solving challenges taken by over half a million students every year. Tony was the Team Leader of the British IMO team in 1990–95 — and a mentor of many bright young mathematicians who are now the crème de la crème of British academia. For many years, he edited the Problem Solving Journal for Secondary Students, with a circulation over 5,000. He wrote and published more than 15 books on mathematical thinking and mathematical problem solving — as well as on teaching mathematics. He was consulted by several UK Ministers of State for Education, and acted as an advisor on mathematics education to the government of Singapore. More can be said about Tony's contribution to this world, but there is no need to compete with Wikipedia where the article devoted to him, en.wikipedia.org/wiki/Tony_Gardiner, is being feverishly updated.

Tony started his work in mathematics in the 1970s. He was a PhD student of the legendary Bernd Fischer, who had just discovered his three sporadic finite simple groups. It was a very fruitful time, when group theoretic ideas were becoming widely applied in combinatorics. Tony's further research was very successful and mostly straddled the two areas of combinatorics and permutation groups.

At the same time Tony started to forge an unusual path in combining research in mathematics with a commitment to high school and undergraduate mathematics. His instinct as a researcher led him to investigate the actual working of mathematics education as a system and look at the entire cycle of reproduction of mathematics: from preschool and primary school through all stages of school education to university to teacher training and then back to school as a teacher. This is also augmented by a smaller cycle: BSc – PhD studies and postdoctoral research, then back to university as a lecturer. This breadth of vision was supplemented by his attention to the socio-economic and political background of education and placed him in a very special position among British mathematics educationalists.

Tony had exceptional academic and intellectual integrity. He was very modest. And, above all, he was a very kind man always helping a talented student or a bright school child who needed help, and did so right up to the last days of his life.

Death Notices

We regret to announce the following deaths:

- Professor Nicholas J. Higham, formerly of the University of Manchester, who was elected an LMS member on 18 June 1993, died on 20 January 2024, aged 62.
- Professor Nelson M. Stephens, formerly of the Heilbronn Institute, Bristol, who was elected an LMS member on 19 May 1966, died on 8 January 2024 aged 83.
- Professor J. Trevor Stuart, FRS, formerly of Imperial College London, who was elected an LMS member on 15 June 1979 and was LMS President 2002–02, died on 17 December 2023, aged 94.
- Dr David L. Johnson, formerly of the University of Nottingham, who was elected an LMS memebr on 16 January 1969, died on 14 December 2023, aged 80.
- Professor Dominic J.A. Welsh, who was elected an LMS member on 20 March 1969, died on 30 November 2023, aged 84.

Microlocal Analysis & PDEs: Advances and Perspectives

Location: Bayes Centre, Edinburgh
Date: 23 February 2024
Website: tinyurl.com/4umwnt6c

This one-day workshop is focused on recent advances in the analysis of PDEs through the prism of microlocal analysis. The event will feature invited talks by Claudio Dappiaggi (Pavia), Claudia Garetto (Queen Mary) and Linhan Li (Edinburgh). All are very welcome to attend. The partial support by an LMS Celebrating New Appointments (Scheme 9) grant is gratefully acknowledged.

16+ Where Can Mathematics Take You?

Location: Online
Date: 15 March 2024
Website: tinyurl.com/3jsnf3xj

This IMA conference aims to give you an insight into where mathematics can take you, introducing you to career options you may never have considered before. Talks will be given by some truly inspiring mathematicians across many different fields, who will share their experiences of work, as well as how they got to where they are today. After the talks there will be a short Q&A panel session, where there is a chance to ask experts any questions.

Mathematical Epidemiology: BAMC 2024

Location: Newcastle University
Date: 9-11 April, 2024
Website: conferences.ncl.ac.uk/bamc2024

Location: Newcastle University Date: 9 -11 April 2024
Website: https://conferences.ncl.ac.uk/bamc2024

A section on Mathematical Epidemiology/Public Health will be held at the BAMC 2024. It is an important interdisciplinary field that uses approaches from mathematics, statistics, and computer science such as machine learning, AI and mathematical models, with the aim of developing and applying new methodologies and interventions to access risk factors associated with disease, including prevention, progression and interventions related to the efficacy of vaccines and treatments. This session is supported by an LMS Conference Grant. Deadline for registration: 15 March 2024.

Tomorrow's Mathematicians Today 2024

Location: Online
Date: 9-10 March 2024
Website: tinyurl.com/3j4n67nj

This will be a fascinating event which will give participants the opportunity to learn about a wide range of mathematics which has excited their peers. The aim of the conference is to enable final year (and other) undergraduates to give presentations on mathematical topics of their choice. Mathematics students will benefit enormously in a number of ways by attending. Those going into research will gain experience of the process of conference submission, while those going into the workplace will gain valuable experience of professional practice and networking to enhance their CVs and career prospects.

Evolution in Structured Populations: Recent Progress and New Challenges

Location: University of Oxford
Date: 18-20 March 2024
Website: bit.ly/48WiRTI

The conference is in honour of Alison Etheridge's contributions to population genetics. This event will focus on various aspects of mathematical models in population genetics, and on the interplay between population structure, natural selection, recombination, dormancy, and other evolutionary forces. Register by 16 February. This conference is supported by an LMS Conference Grant.

Gauge Fields in Arithmetic, Topology and Physics

Location: ICMS Edinburgh
Date: 15-19 April 2024
Website: tinyurl.com/yupvu38j

This workshop is centred around the analogy between number fields and 3-manifolds first observed by Mazur and Mumford which suggests to transfer ideas between number theory, low-dimensional topology, and physics. The workshop will gather practitioners from all three areas to discuss the many interesting ideas that have emerged in recent years. This event is partially funded by an LMS Conference Grant.

LMS Meeting

Northern Regional Meeting & Workshop

25-28 March 2024, Durham

Website: lms.ac.uk/events/society-meetings

The Regional Meeting, to be held on 25 March, forms part of the Northern Regional Workshop on Continued Fractions and SL2-tilings on 26-28 March 2024. The Regional Meeting speakers will be Sophie Morier-Genoud (Université Reims), Matthew Pressland (University of Glasgow) and Ian Short (The Open University). See the website for details of the workshop speakers. Funds are available for partial support to attend. Requests for support, including an estimate of expenses, as well as all queries about the two events may be addressed to one of the organisers, Anna Felikson: anna.felikson@durham.ac.uk.

LMS Meeting

Midlands Regional Meeting & Workshop

2-5 April 2024, Loughborough

Website: lms.ac.uk/events/lms-midlands-regional-meeting-2024

The Regional Meeting, to be held on 2 April, forms part of the Midlands Regional Workshop Harmonic Analysis on Manifolds on 3-5 April 2024. The Regional Meeting speakers will be Jonathan Bennett (University of Birmingham), Oana Ivanovici (Sorbonne Université) and Christopher Sogge (Johns Hopkins University). See the website for details of the workshop speakers. Funds are available for partial support to attend the meeting and workshop. Requests for support, including an estimate of expenses, as well as all queries about the two events may be addressed to one of the organisers, Dr Jean-Claude Cuenin: J.Cuenin@lboro.ac.uk.

Mathematical Modelling for Environmental Challenges

Location: University of Warwick
Date: 21 – 22 March 2024
Website: https://bit.ly/429MjmS

With the current environmental challenges it is crucial to take action in order to achieve a sustainable future, and mathematical modelling will play a central role in understanding and tackling such issues. In this workshop we will hear about the most recent mathematical advances on three particular themes related to environmental challenges: natural flows, decontamination and energy. Registration deadline: 1 March 2024.

Modern Topics in Stochastic Analysis and Applications Conference

Location: Imperial College London
Date: 22-26 April 2024
Website: tinyurl.com/ds4zmbw6

The purpose of the five-day conference is to gather experts from different areas of theoretical and applied stochastic analysis to investigate and discuss current and future directions of this field, with special emphasis on the interplay between theory and applications. A special session is planned with presentations from industrial and academic practitioners. This conference will mark the 70th birthday of Professor Terry Lyons. This event is partially funded by an LMS Conference Grant.

LMS Meeting

LMS Spitalfields History of Mathematics Meeting & Hirst Lecture 2024

26 April, De Morgan House, London, and online via Zoom

Website: lms.ac.uk/events/lms-spitalfields-hirst-lecture-2024

The LMS is delighted to announce the 2024 Spitalfields History of Mathematics Meeting and Hirst Lecture. The meeting features the Hirst Lecture 2024, given by the winner of the Joint LMS-BSHM Hirst Prize and Lectureship 2023, Professor Erhard Scholz.

The meeting will open with Society Business, which will be followed by two lectures.

First Lecture: Jeremy Gray (The Open University)

Title: *F.S. Macaulay and Modern Commutative Algebra*

Abstract:
This talk, which is based on joint work with David Eisenbud in Berkeley, discusses the life and work of the English algebraic geometer Francis Sowerby Macaulay (1862–1937). His early work on plane algebraic curves is a response to that of Max Noether and Alexander Brill, and attempts to extend it in a more rigorous way to arbitrary plane curves. He was invited to speak at the Heidelberg ICM in 1904, but his ideas were naïve and he then plunged into a deep study of what, in modern terms, are ideals in polynomial rings in any number of dimensions. The crucial theorem here is Lasker's primary decomposition theorem (1905), which Macaulay explored in his breakthrough paper of 1913 and in his Cambridge Tract of 1916, where he introduced many ideas that interested Emmy Noether and her followers in the 1920s. In his final paper (1934) he repaid the compliment by being the first to present many of Emmy Noether's ideas to an English audience.

Hirst Lecture: Erhard Scholz (Bergische Universität Wuppertal)

Title: *From Grassmann Complements to Hodge Duality*

Abstract:
When William D. Hodges introduced the duality named after him between alternating forms on Riemanian manifolds in the early 1930s (the Hodge-* operator) related ideas in Maxwellian electrodynamics and the linear algebra of the 19th century had prepared this move from different sides. M. Atiyah emphasized the first background (electromagnetism) in his talks, while it remains largely unnoticed that already Hermann Grassmann had introduced a linear algebraic precursor of the *-operator in his study of extensive quantities ('Ausdehnungsgrössen') in 1866. Grassmann talked about it as the respective complement ('Ergänzung') of an alternating product. In this talk I will give a short outline of the long story of this concept between Grassmann and Hodge.

These lectures are aimed at a general mathematical audience. All interested, whether LMS members or not, are most welcome to attend this event.

The meeting will be followed by a reception at De Morgan House.

LMS Members' Book: Members can sign the Members' Book, which dates from 1865 when the Society was founded, and contains signatures of members throughout the years, including Augustus De Morgan, Henri Poincaré, G.H. Hardy, and Mary Cartwright.

Registration: for further details and to register, see the website above.

UK Operator Algebras Conference

Location: Newcastle University
Date: 12-14 June 2024
Website: sites.google.com/view/ukoaconference

The UK Operator Algebras Conference will provide a forum to showcase the breadth of research in operator algebras and related areas across the UK. The focus of this event will be on shorter contributed talks, and we have funding to support UK-based researchers who wish to present. This will foster a supportive and inclusive community in which early career researchers have the opportunity to promote their work. Registration closes 29 February 2024. This event is partially funded by an LMS Conference Grant.

British Isles Graduate Workshop V: Mathematical General Relativity

Location: Coalport, Shropshire
Date: 8-12 July 2024
Website: enric-sf.github.io/BIGW_V/

The fifth instalment of the British Isles Graduate Workshop will focus on Mathematical General Relativity. It is targeted at PhD students and postdocs but open to all. During the workshop junior researchers will work with three experienced mentors who will propose three topics, split into six talks each. Participants then sign up for the talks in advance, prepare their talks before the meeting, and deliver them during the meeting. Application deadline: 25 February.

The Interplay of Geometric Group Theory and K-Theory

Location: University of Southampton
Date: 24-28 June 2024
Website: dkasprowski.github.io/Conference/

The aim of the workshop is to generate new research opportunities at the intersection of geometric group theory and algebraic K-theory. Besides the lectures from the invited speakers, there will be an opportunity for early career researchers to give short talks. Limited funding for PhD students is available. The deadline for registration is 30 April 2024 while the deadline to apply for funding is 15 March 2024. This event is partially supported by an LMS Conference grant.

Facets of Algebraic Geometry: A Celebration of Combinatorial Techniques

Location: Queen Mary University of London
Date: 25 April 2024
Website: sites.google.com/view/facets-ag

This one-day conference will showcase combinatorial techniques applied to a diverse set of problems in algebraic geometry. It will consist of three research talks, an informal "Small Group Talks" session, and a wine reception. Speakers: Navid Nabijou (QMUL), Rohini Ramadas (Warwick), Evgeny Shinder (Sheffield). Please register by 1 April 2024. Limited funding is available for PhD students.

LMS Meeting

LMS Invited Lecture Series 2024

1-5 July 2024, Imperial College, London

Website: sites.google.com/view/lms-invited-lectures-2024

The biennial Invited Lecturers Series aim to bring a distinguished overseas mathematician to the United Kingdom to present a small course of about ten lectures spread over a week. The event is for graduate students beginning research and at established mathematicians who wish to learn about a new field. The 2024 LMS Invited Lecturer will be Dan Abramovich (Brown University), who will talk on *Logs and Stacks in Birational Geometry and Moduli*. Funds are available for partial support to attend. Requests with an estimate of expenses should be addressed to the organisers: Alessio Corti (a.corti@imperial.ac.uk).

Society Meetings and Events

March 2024

28 LMS Northern Regional Meeting & Workshop, Durham

April 2024

2 LMS Midlands Regional Meeting & Workshop, Loughborough
26 LMS Spitalfields History of Mathematics Meeting and Hirst Lecture, London

May 2024

9 LMS Popular Lecture 2024, Speaker: Sarah Hart, Birmingham

June 2024

28 LMS General Meeting and Kelvin 200th Anniversary Lecture, London

July 2024

1-5 LMS Invited Lecture Series 2024, Imperial College London

Calendar of Events

This calendar lists Society meetings and other mathematical events. Further information may be obtained from the appropriate LMS Newsletter whose number is given in brackets. A fuller list is given on the Society's website (www.lms.ac.uk/content/calendar). Please send updates and corrections to calendar@lms.ac.uk.

February

23 Microlocal Analysis & PDEs: Advances and Perspectives, Bayes Centre, Edinburgh

March

9-10 Tomorrow's Mathematicians Today 2024, Online
14 International Day of Mathematics
15 16+ Where Can Mathematics Take You? Online
18-20 Evolution in Structured Populations: Recent Progress and New Challenges, University of Oxford

April

8-12 Young Geometric Group Theory XII, University of Bristol
9-11 Mathematical Epidemiology: BAMC 2024, Newcastle University
9-11 British Applied Mathematics Colloquium 2024, Newcastle University
15-19 Gauge Fields in Arithmetic, Topology and Physics, ICMS Edinburgh
22-26 2024 Conference on Modern Topics in Stochastic Analysis and Applications (in honour of Terry Lyons' 70th birthday), Imperial College London

June

12-14 UK Operator Algebras Conference, Newcastle University
24-28 The Interplay of Geometric Group Theory and K-Theory, University of Southampton

July

8-12 British Isles Graduate Workshop V: Mathematical General Relativity, Coalport, Shropshire

8-12 Simple-Mindedness, Silting, and Stability, University of Cumbria, Ambleside

August

12-16 International Workshop on Operator Theory and its Applications (IWOTA)

September

4-6 Groups & Representations: after Roger Carter, University of Warwick