Big Proof Workshop

27–31 May 2019

International Centre for Mathematical Sciences, Edinburgh

Abstracts

Avigad, Jeremy

The Mechanization of Mathematics

The phrase "formal methods" is used to describe a body of methods in computer science for specifying, developing, and verifying complex hardware and software systems. The word "formal" indicates the use of formal languages to write assertions, define objects, and specify constraints. It also indicates the use of formal semantics, that is, accounts of the meaning of a syntactic expression, which can be used to specify the desired behavior of a system or the properties of an object sought. For example, an algorithm may be expected to return a tuple of numbers satisfying a given constraint, expressed in some specified language, whereby the logical account spells out what it means for an object to satisfy the symbolically expressed constraint. Finally, the word "formal" suggests the use of formal rules of inference, which can be used to verify claims or guide a search. Such methods hold great promise for mathematical discovery and verification of mathematics as well. In this talk, I will survey some applications, including verifying mathematical proofs, verifying the correctness of mathematical computation, searching for mathematical objects, and storing and communicating mathematical results.

Barany, Michael

Janus in the mathematics library: foundations, communities, meaning, and scale in the mathematics literature

In principle, the mathematics literature is a repository of settled claims, reliably demonstrated and connected in a foundationally coherent whole. This principle is recognizable across much of academic and work-a-day philosophy and practice of mathematics, and often taken for granted. Formal approaches to big proof tend to take this principle as starting point and develop practical tools and frameworks for realizing it more completely and effectively. My talk will develop a historical and ethnographic perspective on distributed and large-scale proof that takes an opposite view: not that existing practices are imperfect realizations of a natural principle for the mathematics literature but rather that many the most vital aspects of mathematical practice and its relationship to the mathematical literature are precisely those that trouble the principle of literature as foundation. Casting a range of familiar habits and customs of mathematical research and communication in a different light, I will show how the mathematics literature furnishes research communities with a means of orienting around and destabilizing concepts, methods, and programmes. These dynamic and future-facing relations to the mathematics literature belie the principle of a static and settled foundation, demanding different metaphors and different visions for the work of proving at scale.

Buzzard, Kevin

Mathematical objects in dependent type theory

Anyone who has used a formal proof verification system knows that it is possible to make a basic theory of groups, rings, vector spaces and other elementary mathematical objects in these systems. But many research mathematicians spend a lot of their time manipulating objects which are vastly more complex to define, such as etale cohomology groups or perfectoid spaces. I was genuinely surprised when I entered this area to find very little evidence of anyone attempting to encode such objects in theorem provers, so I attempted to do so myself. I view such projects as crucial to the success of Tom Hales' Formal Abstracts project. Let me stress that no knowledge of etale cohomology or perfectoid spaces is necessary to follow this talk; the talk is about the obstacles that a mathematician runs into when attempting to translate their "normal" mathematical way of thinking into dependent type theory.

De Toffoli, Silvia

Diagrammatic Notations in Mathematical Proofs

The aim of my talk is to investigate the role of diagrams, and in particular of diagrammatic notations in the context of proving in mathematics. First of all, I will address the preliminary issue of characterizing mathematical diagrams and I will propose a technical definition to delineate the phenomenon under investigation. I will then focus on the features of diagrams that underwrite the possibility for them to enter in the inferential structure of proofs. My main philosophical point is that in some cases not only proof presentations, but proofs as well are dependent on certain features of the notations they deploy, the ones which I will label constitutive features. I will argue for this point through examples of diagrams used in different areas of contemporary mathematics.

Douglas, Michael

String theory, mathematical databases and formal methods

In several fields of mathematics, for example finite group theory, databases of mathematical structures have been developed and maintained as a resource for researchers. An example from theoretical physics is the Kreuzer-Skarke database of reflexive polytopes in four dimensions, objects which correspond to the Calabi-Yau manifolds used in compactification of superstring theory. This was developed in the mid-90's and continues to be a much-used resource, and there is significant interest in developing comparable databases for other mathematical constructs used in string theory. After a short survey of this area, we discuss various ideas for how automated theorem verification and other formal methods could empower this line of work.

Dowek, Gilles
Logipedia: a system-independent encyclopedia of formal proofs

Logipedia (http://logipedia.inria.fr/) is at the beginning of an online encyclopedia of formal proofs expressed in various theories. It is based on three ideas: expressing the theories implemented in various proof systems in the logical framework Dedukti, importing in Dedukti libraries of proofs developed in these systems, analyzing which axiom and which rule is used in each proof, in order to understand to which system this proof can be exported.

Ford, Ian
Mathematical Knowledge Representation and Reasoning in the Wolfram Language

We will discuss progress in the semantic representation of mathematical knowledge in the Wolfram Language as well as demonstrate new automated reasoning capabilities. Topics discussed include axiomatic theories, equational logic provers, 2D Euclidean geometry, ontology representation and reasoning, and more.

Gonthier, George
On the Impact of Big Proofs on Provers

The “big proof” program set out to exploit the advances in computer theorem proving made over their 50 -year development to have some tangible impact on real mathematics. Perhaps unsurprisingly this new focus on bigger proofs had a reverse impact on the proof assistants themselves, on nearly all aspects of their design, from core logic and algorithms to programming interface, library design, and community building.

In this talk I’ll discuss examples of all of these, mostly (but not exclusively) based on my experience with the Mathematical Components project, and lay out perspectives for future evolutions ahead.

Hales, Tom
Mathematical Definitions, Formally Speaking

This talk will give an introduction to my current project, which aims to write all the theorem statements and definitions of mathematics in a computer-readable form. By ""computer-readable,"" we mean more than TeX or code in a computer algebra system. We mean that the math is expressed in terms of the rules of logic and foundations of mathematics. This project is expected eventually to encompass all branches of mathematics.

Harrison, John
The HOL Light Mathematical Libraries

The HOL Light theorem prover has been under development for over 20 years, building also on earlier work by the late Mike Gordon and his many colleagues and students that contributed to the original HOL system. Much of this work has been devoted to building up libraries of formalized mathematics that have seen active use, not only in formal verification but in pure mathematics too, most notably in the Flyspeck project to formalize the proof of the Kepler Conjecture. The resulting mathematical libraries cover a wide range of topics in topology, analysis and geometry, including a recent development of singular homology. We will present an overview of these libraries and some of the lessons learned (often painfully) from their development, as well as speculating on some possible future developments.

Kerjean, Marie
A formal, classical proof of the Hahn-Banach theorem

We present and discuss a formalization of the Hahn-Banach theorem, developed using the Coq proof assistant and based on the Mathematical Components libraries, extended with some axioms. In particular, this sheds light on the particularisation of the axiom of choice needed for classical analysis in Coq. This is joint work with Assia Mahboubi.

Koepke, Peter
Modeling human proof checking in the Naproche-SAD system

Checking an ordinary mathematical proof text is a highly interlinked process involving natural language and formula parsing and logical analyses and checks. Processing a single statement is broken down into smaller proof obligations like proving well-definedness of terms ("type checking") and proofs of sub-statements. The Evidence Algorithm project started by V. Glushkov aimed at developing mathematical software imitating this process. It lead to the SAD system of Andrei Paskevich, that checks mathematical miniatures in a pseudo-natural mathematical language. Our Naproche project has adopted SAD and increased its efficiency, covering and usability. My talk describes how various stages of text checking are implemented in Naproche-SAD and presents our natural formalization of the 30-page appendix of John Kelley's textbook "General Topology" on Kelley-Morse set theory.

Kohlhase, Michael

FAIRMath: Making mathematical Data FAIR (Findable, Accessible, Interoperable, and Reusable)

Over the last years the publication and management of research data have gained increasing attention and support. There are large research data initiatives at the national (e.g. NFDI; Germany) and European level (e.g. EOSC and EUDATA). Even though there are large data mathematical collections like the OEIS, LMFDB, GAP small groups library, or the House of Graphs, by and large Mathematicians are unaware and unaffected by the whole trend. This talk discusses notions of mathematical data, their role in mathematical practice, and their inter-dependence with mathematical knowledge and proof. Based on this we discuss what it would take to make mathematical (research) data FAIR. We will present a paradigm for establishing a unified data infrastructure, and building mathematical services on this.

Komendentskaya, Katya

Verification of Neural Networks for the masses: are our programming languages ready?

In this talk, I will give an overview of state of the art of verification of neural networks from a programming language perspective. I will identify weaknesses and strengths of the existing approaches, based on the recent experience of teaching neural network verification to MSc students specialising in AI. I will conclude by summarising the challenges and possible directions for research in this area.

Koutsoukou-Argyraki, Angeliki

Formalising Mathematics-In Praxis: First Experiences with Isabelle/HOL

This talk is an overview of my first eighteen months of Isabelle/HOL, working within the ALEXANDRIA project at the University of Cambridge, as a pure mathematician with no prior formalisation experience.

I focus mainly on the difficulties I encountered, as my goal is to point out some suggestions that could make Isabelle more practical for current and future users as well as to share with new users some observations of both technical and conceptual nature that might prove to be helpful in their early learning stages.

Löwe, Benedikt
Why did mathematicians not embrace the vision of the QED manifesto?

The QED manifesto was published in 1994 and proposed a vision of a transformed mathematical practice based on a computer system, the "QED system" that uses "mechanical methods to check proofs of the correctness of all entries in the system". It promised mathematical search engines, more time for research, teaching opportunities, and more. The QED program was not a success; in 2007, Wiedijk discussed the reasons for this lack of success in his paper "The QED Manifesto Revisited".

Martin, Ursula
The craft and culture of proof

We look at how Anglophone mathematicians have, over the last hundred years or so, presented their activities using metaphors of landscape and journey. We contrast romanticised self-presentations of the isolated genius with ethnographic studies of mathematicians at work, both alone, and in collaboration, looking particularly at on-line collaborations in the “polymath” format. The latter provide more realistic evidence of mathematicians daily practice, consistent with the the “growth mindset” notion of mathematical educators, that mathematical abilities are skills to be developed, rather than fixed traits.

Paulson, Larry
Formalising Mathematics In Simple Type Theory

Despite the considerable interest in new dependent type theories, simple type theory (which dates from 1940) is sufficient to formalise serious topics in mathematics. After a brief history of the concept of types, the talk focuses on the main techniques used to formalise mathematical concepts using simple type theory. These include Harrison's type-indexed vectors, axiomatic type classes and direct formalisation of abstractions. The talk concludes by discussing the problem of proving the obvious.

Pease, Alison
Automating "human-like" example-use in mathematics

We describe our investigations into ways in which human mathematicians use mathematical examples in their research. Firstly, we bring together theoretical and empirical approaches, concluding that examples are used for conjecture invention, understanding, plausibility-testing, disproof and modification. We then supplement these ideas with an investigation based on grounded theory into example-use during an online mathematical conversation. These studies suggest ways in which "human-like" example-use in mathematics could be automated, in order to help to close the gap between human and automated reasoning. We discuss our work in developing a computational system based on our findings.

Sangwin, Chris
Online proof and elementary mathematics from an educational perspective

In this talk I will review existing online assessment systems which start to ask students to reason line by line, and which expect more from them than a final algebraic answer. Online assessment is increasingly common, but the systems often do not have access to formal representations of mathematical knowledge. By reviewing current practice, I hope to address the following question: should students bend to the technology, or should the technology bend to the student? Lastly I report my own work examining the reasoning which occurs in school examination questions and the extent to which assessment of students' answers can be automatically assessed.

Saxton, David
Teaching machines to do mathematics like humans

Can we teach machines to do mathematics following the same curriculum that we use for humans? We released a dataset of synthetic school level mathematical questions - what happens when we try to train standard state-of-the-art learning models (without any prior mathematical knowledge) to answer these? (Spoiler: they can do well on many but not all problem types - and their perceptual reasoning process is still a long way off from the power of humans.) We also look at motivations for doing this, and speculate on what next steps might be for learning models that could do harder mathematics (perhaps eventually things like conjectures and proofs) in a human-like fashion.

Shankar, Natarajan
Proofs and Things

As abstract mathematics has gained popularity for the formal modelling of scientific, engineering, and computational concepts, the benefits of proofs have spilled over to these disciplines as well. We now prove theorems about (mathematical models of) processes and things. Conversely, the objectification of proof (in the form of metamathematics) has supported the automation of proof construction and validation. Automation of this kind is useful in engineering and computation for coping with the sheer scale of formalization. Proof automation can be a significant aid in the curation and construction of mathematical content across a growing range of disciplines. The talk explores some of the applications of proofs to things, including proofs themselves.

Tanswell, Fenner
The Social Epistemology of Mathematical Collaboration

Big proofs, involving many collaborators and large amounts of work, pose a new kind of challenge for the epistemic status of the proofs. Unlike traditional proofs, these cannot easily be checked and verified by an individual mathematician, so seemingly cannot become known in the usual way. With bigger proofs, the probability of errors and gaps also increases. There is then the question of what kinds of errors and gaps are tolerable, without undermining the status of the proof. We draw on the tools of social epistemology, seeing a group of mathematicians as the relevant object of study, and use this to reject the potential negative conclusions about big proofs.

Urban, Josef
Learning and Reasoning over Big Proof Corpora

The talk will give a brief overview of recent methods that combine learning and reasoning over large formal libraries. I will mention the "hammer" linkups between ITPs and ATPs, systems that learn and perform direct tactical guidance of ITPs, discuss learning of premise selection over large libraries and learning-based guidance of saturation-style and tableau-style automated theorem provers (ATPs) trained over the large proof corpora. I will also mention feedback loops between proving and learning in this setting, and show our auto formalization experiments.

Big Proof Workshop

27-31 May 2019

International Centre for Mathematical Sciences, Edinburgh

Watt, Stephen

The NASA Effect of a Global Digital Math Library

Many benefits have been touted of having a global digital mathematics library, usually from the point of view of developers who want to build one or mathematicians who want to use one. But developing the necessary technology should have larger consequences, in the same way that NASA has both space and non-space impact. We examine some of the obvious and less obvious potential subsidiary outcomes of developing a global digital mathematics library, including examples drawn from Waterloo's on-line digital education initiative.