The rise of formalism in mathematics.

K. Buzzard, Imperial College London

9th July, International Congress of Mathematicians

Before we start

Thank you to the organisers for the invitation, and thanks to you all for coming!

Mathematics and computers

Computers have been better than humans at *computing* for 60 years.

For 25 years they have been better than us at chess.

For a couple of years they have been better than us at go.

When will they be better than us at proving theorems?

nature

Explore content ⌄ About the journal ⌄ Publish with us ⌄ Subscribe

nature > news > article

NEWS | 18 June 2021

Mathematicians welcome computer-assisted proof in ‘grand unification’ theory

Proof-assistant software handles an abstract concept at the cutting edge of research, revealing a bigger role for software in mathematics.

Davide Castelvecchi

nature

Explore content ⌄ About the journal ⌄ Publish with us ⌄ Subscribe

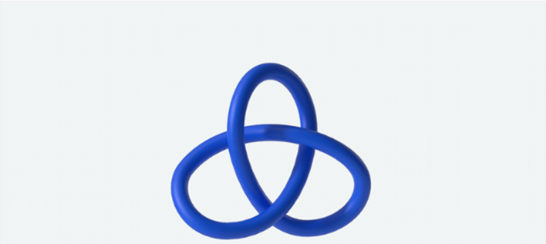
nature > news > article

NEWS | 01 December 2021

DeepMind's AI helps untangle the mathematics of knots

The machine-learning techniques could benefit other areas of maths that involve large data sets.

Davide Castelvecchi



The beginning of the end?

Will computers soon be better than humans at proving theorems in research level mathematics?

Are our jobs as mathematical researchers at risk?

No. (in my opinion).

The beginning of the beginning.

However, will computers soon be *helping* humans to prove theorems?

Not just by working out examples, but by *reasoning*?

Finding proofs or counterexamples in databases, constructing simple proofs themselves, doing diagram chases?

Will computers make it easier for humans to *learn* mathematics?

Will they enable humans to *explore* proofs in new ways?

My guess: yes.

Overview of the talk

- Live demo of a computer theorem prover;
- Some history of the area;
- The state of the art;
- How to get involved.

What is a computer proof assistant?

We're about to see "Lean" in action.

Lean is a free and open source *interactive theorem prover* written principally by Leonardo de Moura at Microsoft Research (with help from Sebastian Ullrich, Gabriel Ebner, . . .).

Many other such systems exist (Coq, Isabelle/HOL, HOL Light, Agda, cubical Agda, Metamath, Mizar. . .).

You can use such systems to *formalize* mathematical proofs.

There are also *automatic theorem provers* such as Prover9, Otter, E, Waldmeister, Vampire,. . . .

Lean demo

What did we just see?

We all know that computers can be used to *compute*.

We've just seen that they can now be used to *reason*.

Proof assistants: turning mathematical questions into levels of a computer puzzle game.

We've just seen them doing undergraduate level topology. Are these things just toys?

History (pre-2000)

1970s: first computer-verified construction of the real numbers as a complete ordered field (Jutting's thesis).

1990s: Systems could *check* human-entered proofs of simple theorems (at undergraduate level).

History (21st century)

Some milestones in the 2000s:

- 2004: Avigad et al formally verified the prime number theorem in Isabelle/HOL (also Harrison 2009 in HOL Light).
- 2004: Gonthier formally verified the four colour theorem in Coq.
- 2005: Hales formally verified the Jordan Curve theorem in Isabelle/HOL.
- 2013: Gonthier et al formally verified the odd order theorem in Coq.

Very little reaction from the mathematics community.

My hope is that the results I'll talk about today will provoke a bigger reaction.

The Kepler Conjecture

In 1998 Hales and Ferguson proved the Kepler conjecture (optimal density for sphere packing in 3 dimensions).

Part of the proof involved checking 23,000 nonlinear inequalities on a computer. (Note that Viazovska's work in 8 and 24 dimensions is more conceptual).

Five years later the Annals of Mathematics told Hales that the referees were not able to completely certify the proof.

Hales' extraordinary response: he put a team of 20+ people together and spend the next 12 years formalising the result in an interactive theorem prover.

They succeeded in 2015.

Hales' conclusions

Hales, now an expert in the area, spoke at the Newton Institute on the story in July 2017.

He had concluded that the following project was now *feasible*:

Create a system which was capable of understanding the *statements* of all the theorems being published currently in the serious pure mathematics journals.

Statements are easier than proofs!

Statements are a *necessary first step*.

How can computers help us find the answer, if they can't even understand the *question*?

Harder than it looks

To formalise the statements of 2022 research level mathematics, we'd better have a full undergraduate degree formalised first!

If there is no definition of smooth manifolds, vector bundles, class groups, and various basic homology and cohomology theories in your prover (singular cohomology, de Rham cohomology,...), then what chance have you got?

Because our community was largely uninterested in this work, no system in 2017 had these definitions. This is *our fault.*

More recent history

In 2017 I started a Lean club called the Xena Project, at Imperial College London.

The goals were (a) to teach undergraduates how to use the software and (b) to formalise parts of our undergraduate curriculum.

Students quickly wanted to take on projects in finite group theory, and then more ambitious projects.

The Lean community welcomed us in and taught us how to use the software.

They invited us to help build a mathematics library for Lean, called `mathlib`.

Undergraduate mathematicians defined linear maps, matrices, subgroups,. . . and added them to Lean's mathematics library.

Schemes

In the 1960s Grothendieck revolutionised algebraic geometry with his introduction of the concept of a scheme.

In 2018 me and some undergraduates (Kenny Lau, Chris Hughes, Amelia Livingston, Ramon Fernández Mir) from the club defined schemes in Lean.

We then started doing the exercises in Hartshorne's algebraic geometry textbook.

This was harder than you think, but it was not too hard.

The Lean community encouraged us to publish (which we did, with Scott Morrison, who reformulated everything using the language of categories).

But we still needed more to impress mathematicians.

Perfectoid spaces

In 2018 Peter Scholze won a Fields Medal.

This was in part for his work on perfectoid spaces.

In 2019, Johan Commelin, Patrick Massot and myself formalised the definition of a perfectoid space in Lean.

Perfectoid spaces

Why did we formalise perfectoid spaces?

- A new way of using the software (simple theorems about complex objects, not complex theorems about simple objects).
- To check that a modern computer proof system could handle such a complex definition.
- An interesting way of *learning* the definition properly.
- Publicity stunt.

But it worked: it brought the area to the attention of more mathematicians.

Lean is not me.

Lean is not “Kevin Buzzard’s project”, and its mathematics library isn’t either.

Lean’s mathematics library `mathlib` is a gigantic collaborative project.

It is a huge database of undergraduate mathematics and more, built by hundreds of volunteers and led by the Lean Prover Community, of which I am but one small part.

Recent projects

I will now quickly run through a large list of just *some* of the mathematics which people in the theorem prover community have been doing recently, mostly at post-undergraduate level.

The Liquid Tensor Experiment

In December 2020 Peter Scholze challenged the theorem prover community to verify the fundamental theorem of liquid vector spaces (proved by Clausen and Scholze):

$$\mathrm{Ext}^i_{\mathrm{Cond}(Ab)}(\mathcal{M}_{p'}(S), V) = 0$$

for $i \geq 1$.

It's a technical result about higher extensions in the category of condensed abelian groups.

Six months later a team led by Johan Commelin had formalised, in Lean, the proof of the key technical lemma which Scholze felt was the heart of the matter.

The community (Commelin, Topaz, many other people) are on the verge of finishing the job.

The Liquid Tensor Experiment

What did we learn from this work?

Firstly, Commelin greatly simplified a part of Clausen-Scholze's proof (the "Commelin complex").

Secondly, Scholze claimed that the experience taught him "what actually makes the proof work".

"...this made me realize that actually the key thing happening is a reduction from a non-convex problem over the reals to a convex problem over the integers."

Thirdly, we see that the systems can now handle complex proofs about complex objects.

Recent projects

2013: Vladimir Shchur proved a quantitative version of the Morse Lemma for Gromov-hyperbolic spaces.

Proof published in the Journal of Functional Analysis.

Sébastien Gouëzel tried to formalise the result in Isabelle/HOL and discovered a fundamental error.

Gouëzel and Shchur found a new (more complex) argument.

2018: joint paper, with a better estimate, together with a completely formalised proof.

Recent projects

2016 : Ellenberg and Gijswijt solved the Cap Set conjecture.

The work was published in the Annals of Mathematics.

In 2019 Dahmen, Hölzl and Lewis formalised the proof in Lean.

Recent projects

December 2021: Thomas Bloom proved that a set $A \subseteq \{1, 2, 3, 4, \ldots\}$ with positive upper density contained a finite subset $S \subset A$ such that $\sum_{n \in S} \frac{1}{n} = 1$.

This answered a question of Erdős and Graham.

He then learnt how to use Lean, by talking to Bhavik Mehta (a PhD student of Gowers in Cambridge).

Six months later Bloom and Mehta had formalised the entire proof in Lean.

The work includes a formalisation of an instance of the Hardy-Littlewood circle method.

Bloom's paper is still awaiting a referee's report.

Recent projects

2021: Baanen, Dahmen, Narayanan and Nuccio formalised Dedekind domains and their class groups in Lean.

They also formalised the proof that the class group of a global field was finite.

2022 : de Frutos Fernández formalised the adeles and ideles of a global field in Lean.

She proved the relationship between the idele class group and the ideal class group.

Sebastian Monnet formally defined the Krull topology on a Galois group and proved it was profinite.

de Frutos Fernández then went on to state the main conjectures of global class field theory, in a non-cohomological form.

Recent projects

In the last few months Livingston defined group cohomology and Galois cohomology.

She's currently working on stating the cohomological form of the local and global theorems.

De Frutos Fernandez has outlined an approach to formalising the proofs of main theorems of local class field theory, which is a natural next project.

Recent projects

Narayanan is currently working on Iwasawa theory.

She has defined p-adic L-functions and is currently proving that their special values are related to generalised Bernoulli numbers.

Recent projects

Gardam disproof of Kaplansky's unit conjecture was published in the Annals of Mathematics in 2021.

The argument was formalised in Lean by Siddhartha Gadgil and Anand Rao Tadipatri in 2022.

Recent projects

Gouëzel, Kudryashov, Macbeth, Degenne and Ying have been formalising analysis and probability in Lean.

Notable recent achievements have been the strong law of large numbers, change of variables in multivariable calculus, Lebesgue differentiation theorem, Cauchy's integral theorem and definitions and basic properties of martingales.

Recent projects

In 2020 Commelin and Lewis formalised the ring $W(R)$ of Witt vectors of a commutative ring R.

Using their work, de Frutos Fernández is working on the definitions of Fontaine's rings, for example B_{dR}.

Natural next step: divided power ideals and B_{cris}.

Also in p-adic Hodge theory: Dupuis, Lewis and Macbeth classified 1-dimensional isocrystals over an algebraically closed field of positive characteristic.

Recent projects

1999: Warwick Tucker proved that the Lorenz attractor was chaotic.

Tucker's argument involved a lot of computations, written in C++.

In 2017 Immler formally verified the calculations using Isabelle/HOL.

Recent projects

Scott Morrison has built a gigantic category theory library (basics, monoidal categories etc).

Using it, Commelin, Himmel, Morrison, Topaz and Yang have built abelian categories, derived functors and homological algebra.

(This was essential for the Liquid Tensor Experiment).

Recent projects

Nash formalised Lie algebras in Lean and came up with what seems to be a new and more conceptual proof of Engel's theorem along the way.

Recent projects

2022: Jujian Zhang formalised projective schemes in Lean and is currently defining sheaf cohomology.

Étale cohomology is most definitely on the horizon (the underlying commutative algebra is in a good place).

Recent projects

I defined elliptic curves in Lean, and Birkbeck defined modular forms and stated the modularity conjecture.

Karatarakis and I are slowly beginning the journey towards the proof. This will take many many person-years. Whether it takes many many years depends a lot on the number of persons who get involved.

In the mean time, Brasca is leading a project to formalise the old proof of Fermat's Last Theorem for *regular* primes.

You can monitor the progress by looking at the dependency graph.

Recent projects

1978: Apéry proved that $\zeta(3) = \sum_{n>0} \frac{1}{n^3}$ was irrational.

In 2019, Mahboubi and Sibut-Pinote (following earlier work of these authors with Chyzak and Tassi) formalised the proof in Coq.

Recent projects

2019: Manuel Eberl formalised the vast majority of Apostol's book on analytic number theory in Isabelle/HOL.

Examples of what he did: the statement of the Riemann Hypothesis, and the proof of Dirichlet's theorem on primes in arithmetic progression.

Recent projects

2021: Bordg, Paulson and Li formalised the definition of a scheme in Isabelle/HOL.

(interesting for foundational reasons)

Recent projects

Mehta and Dillies formalised Szemerédi's Regularity Lemma and Roth's theorem on arithmetic progressions in Lean, and Edmonds, Koutsoukou-Argyraki and Paulson formalised the same results in Isabelle/HOL.

Recent projects

Many of the previous projects have had a number-theoretic or algebraic flavour.

This is merely a reflection of the interests of the mathematicians within the theorem prover community.

A highly non-trivial project in a completely different area is the *sphere eversion project* of Massot, van Doorn and Nash.

Sphere eversion project

Theorem (Smale, ’50s): A sphere can be everted.

There are videos on the internet visually demonstrating the construction.

Is it really possible to formalise such a result in a computer theorem prover?

Massot observed that what one should be formalising is Gromov’s *h*-principle, via convex integration.

You can see their current progress here.

Getting involved

A fun place to start is my natural number game, written for undergraduates at my university.

Many modern theorem provers have online communities on Discord or Zulip. Some examples:

- Coq: coq.zulipchat.com
- Lean: leanprover.zulipchat.com
- Isabelle: isabelle.zulipchat.com
- Agda: agda.zulipchat.com

The future?

They digitised music (CD, mp3) but at the time nobody foresaw the consequences (Napster, Spotify).

We're digitising mathematics, and I believe this will inevitably change mathematics.

You are welcome to join us.

Thank you very much for your attention.