Formalising Undergraduate Mathematics

K. Buzzard

CICM-13, 27th July 2020

Thank you to the organizers for the invitation!

Overview of talk:

- Research mathematicians and theorem provers.
- Why formalise undergraduate mathematics?
- How is Lean doing?

Who am I?

For over 20 years I was a traditional number theorist.

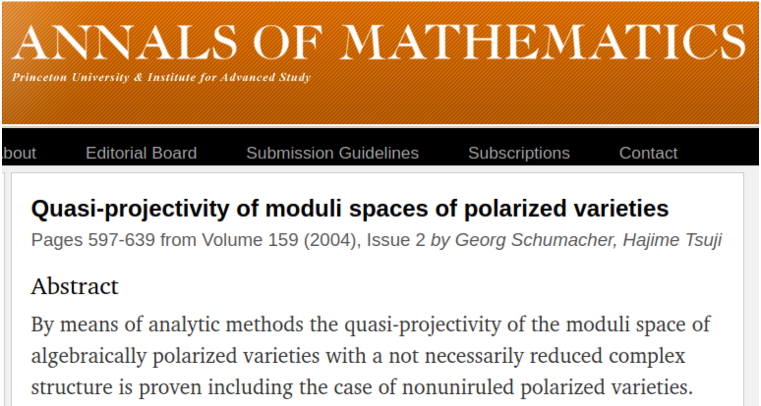
More recently I got interested in formal proof verification. Why?

- Pedagogical reasons (UG teaching / projects);
- Research-related reasons (worries about rigour).

None of my colleagues had used formal proof software, and most had never heard of it.

Unfortunately, my first attempt (in 2018) to convince them to use it was a failure. Let me tell you about it.

The Annals of Mathematics is the most prestigious pure mathematics journal.



ANNALS OF MATHEMATICS

Princeton University & Institute for Advanced Study

bout Editorial Board Submission Guidelines Subscriptions Contact

Quasi-projectivity of moduli spaces of polarized varieties

Pages 597-639 from Volume 159 (2004), Issue 2 *by Georg Schumacher, Hajime Tsuji*

Abstract

By means of analytic methods the quasi-projectivity of the moduli space of algebraically polarized varieties with a not necessarily reduced complex structure is proven including the case of nonuniruled polarized varieties.

[from the Annals of Mathematics website]

ANNALS OF MATHEMATICS

Princeton University & Institute for Advanced Study

About | Editorial Board | Submission Guidelines | Subscriptions | Contact

Non-quasi-projective moduli spaces

Pages 1077-1096 from Volume 164 (2006), Issue 3 *by János Kollár*

Abstract

We show that every smooth toric variety (and many other algebraic spaces as well) can be realized as a moduli space for smooth, projective, polarized varieties. Some of these are not quasi-projective. This contradicts a recent paper (Quasi-projectivity of moduli spaces of polarized varieties, *Ann. of Math.* **159** (2004) 597–639.).

[also from the Annals of Mathematics website]

No retraction of either paper was ever published AFAIK.

The incorrect paper has some really profound ideas in, used to great effect by other mathematicians to prove deep theorems.

Mathematicians find this situation amusing.

It is also disempowering.

In 2018 I put together a “bad mathematics” talk.

Proofs with holes, unpublished proofs, errors in the literature. . . .

I went round the UK giving this talk. How did it go down?

- Many people did not recognise my objections (“the experts are on top of things”).
- Others said that it did not matter (“mathematics is about ideas”).
- Others told me to go and learn some history (“it has always been like this”).

Elegant exposition of the two sides of the argument:

- Jaffe and Quinn “Theoretical mathematics”;
- Thurston “On proof and progress in mathematics”.

Examples of talking-points for research mathematicians.

- I believe that no one person understands all the details of the full proof of Fermat's Last Theorem, but it is undoubtedly completely rigorously proved.
- Mochizuki's proof of ABC will be published by PRIMS.
- The classification of finite simple groups is unpublished.
- "The full proof of theorem X is known to the experts."
- "The system has worked for thousands of years. Why change it?"
- Digitising mathematics is pointless/the future/both.
- "Can they tell us anything new?" NO. Not yet.

It's not clear to my community whether there is a problem with research mathematics. And if there is, it's *certainly* not clear if formalisation is the solution.

Students – more easily led

Whilst doing this, I had independently started working with undergraduates on formalisation of undergraduate level mathematics, using a system called Lean.

Lean's mathematics library was (just) ready for undergrad mathematicians.

Undergraduates were *far more receptive* to the idea of formalising mathematics in a theorem prover, than staff members.

I started a formalising club – the Xena Project. "Mathematicians learning Lean".

Weekly Thursday meetings, currently on Discord. All undergraduate mathematicians welcome.

And this is how I got interested in formalising undergraduate mathematics.

We started by formalising the material I was teaching to the 1st years.

Some of it was essentially impossible in Lean at that time ($\sin$, $\cos$). And some of it was a joy to formalise (equivalence relations).

Realisation: one should not formalise mathematics in the order it is taught to mathematics undergraduates.

$e^{i\theta} = \cos(\theta) + i\sin(\theta)$ seemed a very long way away, and the derivative of $\sin(x)$ being $\cos(x)$ seemed even further. “First year stuff”.

Localising rings

On the other hand, Lean had rings and equivalence relations, so localisation of rings should be easy. “Third year stuff”.

First year undergraduate Kenny Lau started on this theory, and effortlessly added it to Lean.

A month later, first year undergraduate Chris Hughes started formalising results in the 1st year group theory course (and finiteness is hard in type theory).

I realised that I was building a team, and proposed that we formalised the theory of schemes (MSc level algebraic geometry). It took us about three months, working on and off at it.

Once we had finished, I started asking about how schemes were done in other theorem provers.

Turned out that they weren't there.

This shocked me to the core.

This stuff is 50 years old and "standard stuff" where I come from (a maths department).

Things get worse: class groups of number fields aren't in any theorem prover. The basics of this stuff were known to Gauss.

I teach class groups to my 3rd year *undergraduates*. "The class group of a number field is finite".

Can these systems prove it? *No prover can currently state it.*

No research mathematician is going to take these systems seriously if they cannot do UG mathematics.

Computer proof checkers

Computer proof checkers, or ITPs (Coq, Lean, Agda, Isabelle/HOL, HOL Light, Mizar, Metamath, many many more) have been around for 50 years or so.

- Many small projects are written in these systems.
- Also, some highly non-trivial mathematical projects.
- But no systematic development of an undergraduate degree.

Why not?

Will the mathematicians do it?

Mathematicians see that software like this will, *one day*, change mathemaatics.

But we have a long way to go.

“Self-evident”: formalising an undergraduate degree is the place to start.

Serious Research Mathematicians not interested in doing it.

Serious Research Mathematicians control where the funding goes in pure mathematics.

Computer scientists do other things.

A team of (mostly) computer scientists formalised a proof of the Feit–Thompson theorem.

Thompson was awarded the Fields Medal in 1970 for this and other work.

Parts of undergraduate group theory, number theory and representation theory were formalised, as part of a much bigger proof.

Researchers just did the bits they needed.

- ITP users seem to focus on proving theorems.
- You formalise what you need to prove the theorem.
- Computer scientists can't see any publications in formalising UG mathematics.
- Mathematicians need the material but don't want to do it themselves.
- AI people would like to train on the material but it doesn't exist.
- No funding available (I have only been funded to formalise PhD level mathematics)
- We could wait until computers can read books, but I can't wait that long.
- How about using undergraduates? They type up their lecture notes in LaTeX after all. . .

Formalizing undergraduate mathematics in Lean: not as easy as telling undergraduates to type up their lecture notes into Lean.

We teach the first years the Riemann Integral in basic analysis.

The Lean experts assured me that the correct thing to do was construct a far more general integration theory first (the Bochner integral, taking values in topological vector spaces).

This rules out most undergraduates.

However, we had far more success with algebra.

A lot of 2nd and 3rd year undergraduate algebra is now in Lean. Examples:

- rings,
- unique factorization domains,
- Euclidean domains,
- Principal Ideal Domains,
- modules,
- Noetherian rings and modules.

This is “unpublishable work”.

It taught us a *lot* about how to formalise mathematics in Lean.

Implementation v specification is a thing.

Implementations: We got group homomorphisms wrong, we got subgroups wrong, we got polynomials wrong, we got modules over a ring wrong. Some stuff is fixed, subgroups are still being fixed. Mario Carneiro refactored modules.

By formalising lots of undergraduate mathematics in one Lean library, we learnt:

- Which parts were easy in Lean;
- Which parts were hard in Lean;
- pros and cons of various implementation decisions in Lean.

Added benefit: we have one library which students can use to do homework problems.

F. Wiedijk, in “The QED manifesto revisited” (2007), points out that any system aiming to formalise a substantial corpus of mathematics needs to be able to “integrate work by multiple people into a nice coherent whole”.

Lean’s maths library is doing precisely this, because of a Zulip chatroom and GitHub.

How far have we got?

The undergraduate degree taught in Paris Sud (Saclay, Orsay) is very well-specified.

Thanks to Patrick Massot and others, we can take a detailed look. (link)

Undergraduate mathematics in mathlib

This gives pointers to undergraduate maths topics that are currently covered in mathlib. There is also a page listing undergraduate maths topics that are not yet in mathlib.

Linear algebra

Group Theory

Ring Theory

Fundamentals

Ideals and Quotients

Algebra

Divisibility in integral domains

Polynomial rings

$K[X]$ is a euclidean ring when K is a field, irreducible polynomial, Eisenstein's criterion, polynomial algebra in one or several indeterminates over a commutative ring, roots of a polynomial, multiplicity, polynomial derivative,

Missing undergraduate mathematics in mathlib

This gives pointers to undergraduate maths topics that are currently missing in mathlib. There is also a page listing undergraduate maths topics that are already in mathlib.

If you want to work on an item from this list then you should first check the pull requests list to see whether it is already coming, then the issues list to see whether it is discussed there, and finally talk about this idea on Zulip.

Linear algebra

Group Theory

Ring Theory

Algebra

Divisibility in integral domains

Polynomial rings

cyclotomic polynomials in $\mathbb{Q}[X]$, relationship between the coefficients and the roots of a split polynomial, Newton's identities, decomposition into sums of homogeneous polynomials, symmetric polynomials

Undergraduates are involved.

If we order mathlib contributors by lines of code added, then in the top 20 contributors to mathlib we see three Imperial College London mathematics undergraduates (KennyLau, Chris Hughes, Amelia Livingston).

Many more Imperial undergraduates have contributed.

My idea: keep telling young mathematicians about this software.

And then wait for the paradigm shift.

Prove a theorem. Write a function. @XenaProject