Formal Proofs

Monsoon Math Camp 2021

Koundinya Vajjha

July 10, 2021

Welcome!

This course will be an introduction to computer-assisted formal proofs, using the L∃∀N theorem prover.

Welcome!

This course will be an introduction to computer-assisted formal proofs, using the L∃∀N theorem prover. What should you expect from this mini-course?

Welcome!

This course will be an introduction to computer-assisted formal proofs, using the L∃∀N theorem prover. What should you expect from this mini-course?

- Four 50 min lectures on Lean. Two by me, two by Ashvni.

Welcome!

This course will be an introduction to computer-assisted formal proofs, using the L∃∀N theorem prover. What should you expect from this mini-course?

- Four 50 min lectures on Lean. Two by me, two by Ashvni.
- Bonus: Kevin Buzzard's talk immediately after Ashvni's last lecture.

Welcome!

This course will be an introduction to computer-assisted formal proofs, using the L∃∀N theorem prover. What should you expect from this mini-course?

- Four 50 min lectures on Lean. Two by me, two by Ashvni.
- Bonus: Kevin Buzzard's talk immediately after Ashvni's last lecture.
- Lots of hands-on exercises. We'll be checking Discord through the week if you have questions.

Welcome!

Prerequisites and advice:

- An installed Lean+VS Code(+ Mathlib) setup.

Welcome!

Prerequisites and advice:

- An installed Lean+VS Code(+ Mathlib) setup.
- Instructions available at https://github.com/kodyvajjha/lean-mmc2021

Welcome!

Prerequisites and advice:

- An installed Lean+VS Code(+ Mathlib) setup.
- Instructions available at https://github.com/kodyvajjha/lean-mmc2021
- Follow the instructions, if something breaks, ask in the #tech-support channel.

Welcome!

Prerequisites and advice:

- An installed Lean+VS Code(+ Mathlib) setup.
- Instructions available at https://github.com/kodyvajjha/lean-mmc2021
- Follow the instructions, if something breaks, ask in the #tech-support channel.
- Please ask questions! Formal verification is fun when done collaboratively.

Today's agenda

- A bit of history: Why formal proofs?
- Live Lean demo: Tactics in Lean
- Time permitting: infinitude of even numbers.

You will leave today's lecture with an impression for why formal proofs matter and should see Lean in action.

Formal proof

A formal proof is a mathematical proof in which every logical inference is checked all the way down to the fundamental axioms of mathematics. No appeal to intuition is made, even if the translation from intuition to logic is routine.[1]

[1] Hales, *Formal Proof*, 2008

Foundational crisis – Russell's paradox.

In 1905, Bertrand Russell discovered his famous paradox which showed that one needed to be a bit more careful when dealing with sets naively.

Let $R = \{A \mid A \notin A\}$ be the set of all sets that do not contain themselves. We can now ask, does $R \in R$?

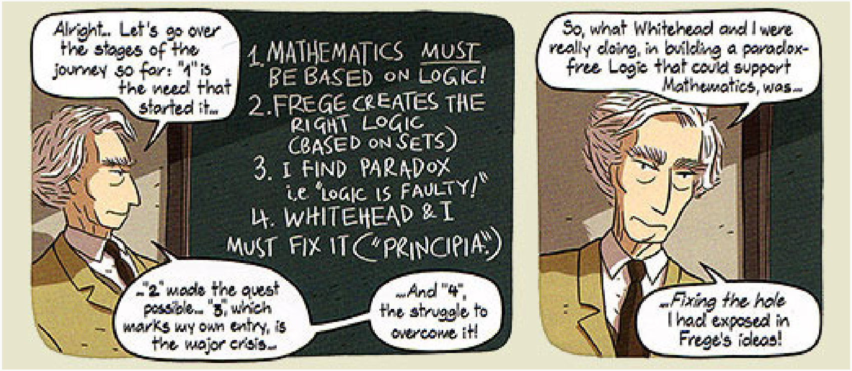
Russell found that $R \in R \iff R \notin R$. A contradiction!

Foundational crisis

Hardly anything more unfortunate can befall a scientific writer than to have one of the foundations of his edifice shaken after the work is finished. This was the position I was placed in by a letter of Mr. Bertrand Russell, just when the printing of this volume was nearing its completion.
– Gottlob Frege (Appendix of Grundgesetze der Arithmetik)

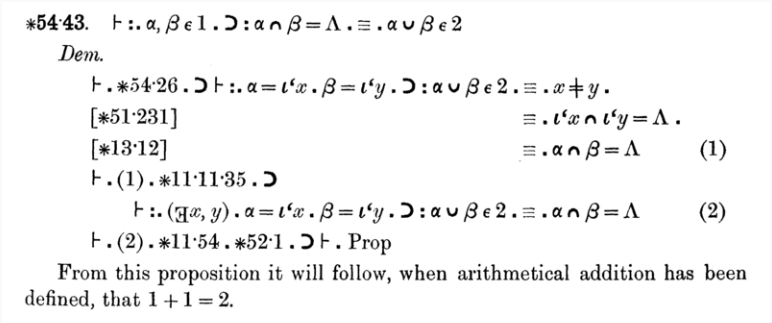
Foundational crisis

After discovering it, Russell along with Whitehead, decided to fix it.


Alright.. Let's go over the stages of the journey so far: "1" is the need that started it..
1. MATHEMATICS MUST BE BASED ON LOGIC!
2. FREGE CREATES THE RIGHT LOGIC (BASED ON SETS)
3. I FIND PARADOX i.e "LOGIC IS FAULTY!"
4. WHITEHEAD & I MUST FIX IT ("PRINCIPIA")
.."2" made the quest possible.. "3", which marks my own entry, is the major crisis..
..And "4", the struggle to overcome it!
So, what Whitehead and I were really doing, in building a paradox-free Logic that could support Mathematics, was..
..Fixing the hole I had exposed in Frege's ideas!

Formal proof – Some history

Thus started the *Pricipia Mathematica*, which is considered to be the first formalization effort.



$*54{\cdot}43.\quad \vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[*51{\cdot}231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$

$[*13{\cdot}12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . *11{\cdot}11{\cdot}35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . *11{\cdot}54 . *52{\cdot}1 . \supset \vdash . \mathrm{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

It took them 360 pages (in the abridged second edition) to prove that $1 + 1 = 2$.

Formal proof – Some history

"...my intellect never quite recovered from the strain of writing [Principia Mathematica]. I have been ever since definitely less capable of dealing with difficult abstractions than I was before."
– Bertrand Russell

Formal proof – Some history

Perhaps twenty or thirty people in England may be expected to read this book. It has many claims to be widely read; all professional mathematicians, for example, can and ought to read it; but it will have to contend with an immense mass of prejudice and misconception, and we should probably be over-sanguine if we supposed that there are half a dozen who will. It is a strange and discouraging fact that mathematicians as a class are utterly impatient of inquiries into the foundations of their own subject.
– G. H. Hardy, Times Literary Supplement, Sept 7th, 1911

Few mathematicians were interested in it, and even fewer read it fully.

Computer-checked Formal Proof

The advent of the computer brought about a renewed interest in formalization, and also in systems in which formalization is carried out.

The computer could now be used to automate away some of the tedium such as proof-checking.

The foundation of mathematics used differs among different systems and come in various flavours: Tarski-Grothendieck Set Theory (*Mizar*), Calculus of Inductive Constructions (*Coq*,*Lean*,*Agda*), Homotopy Type Theory etc.

Computer-checked Formal Proof

- Some of these foundations have *computational content* – their implementations double up as programming languages.
- "Formalizing a theorem/program" = "Getting an implementation of the foundations to accept the (correctly stated) theorem/program as valid".
- The process is labor-intensive, but has a big payoff: *highest possible level of trust*.

Why formal proof?

The long-term goal: the mathematician of the future proves a theorem on paper, formally verifies it in a proof assistant, and sends it to publication, thus bypassing the referee.

Why formal proof?

The long-term goal: the mathematician of the future proves a theorem on paper, formally verifies it in a proof assistant, and sends it to publication, thus bypassing the referee.

This is good even for the referees. They can now simply focus on the “high-level” arguments without worrying about the details. But the details are available to them if they wanted to inspect them.

Why formal proof?

There have been many examples of bugs in mathematical papers which have gone unnoticed, sometimes for decades.

Why formal proof?

There have been many examples of bugs in mathematical papers which have gone unnoticed, sometimes for decades.

If mathematics is an edifice built layer by layer, and we better be sure that there are no cracks in the edifice anywhere – for the whole structure may come crumbling down if the cracks are serious enough.

Why formal proof?

There have been many examples of bugs in mathematical papers which have gone unnoticed, sometimes for decades.

If mathematics is an edifice built layer by layer, and we better be sure that there are no cracks in the edifice anywhere – for the whole structure may come crumbling down if the cracks are serious enough.

I argue that this isn't as paranoid as one may first think: we've already seen an example of Frege's structure collapsing because of Russell's paradox.

Examples

- Formal Proof of the Kepler Conjecture (HOL Light + Isabelle).
- Odd-order theorem (Coq).
- Perfectoid Spaces (Lean).
- Prime Number Theorem (Isabelle)

⋮

- CompCert (Coq)
- seL4 (Isabelle)
- Q^*cert (Coq)

⋮

LEAN DEMO