A quick introduction to proof assistants

Pieter Belmans

December 3 2024

University of Luxembourg

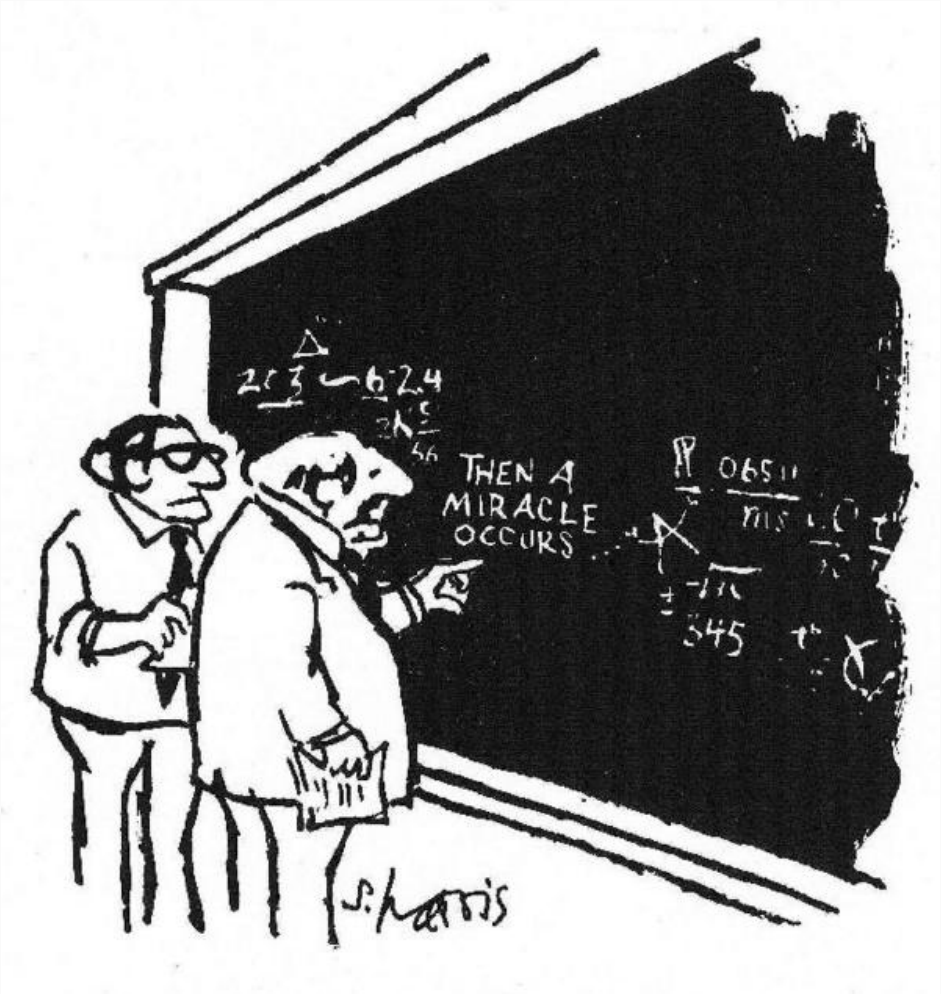
Plan: become superheroes

1. introduce your superpower: Lean
2. motivation and a showcase
3. ~~prove Fermat's last theorem~~
4. some advanced examples

On proofs in mathematics

What is a proof?

- a social construct: convince yourself and other humans
- usually **not** a complete and completely rigorous chain of implications...



Three stages according to Terrence Tao

pre-rigorous intuitive manner, based on examples, fuzzy notions, and hand-waving
high school, early undergraduate

rigorous work and think in a much more precise and formal manner; emphasis is now primarily on theory
undergraduate, early graduate

post-rigorous comfortable with rigorous foundations, revisit one's pre-rigorous intuition on the subject
graduate and beyond

most of us in the latter stage, but serious mistakes might happen there!

plausible-looking lemma without complete proof by senior mathematician?

Mistakes

often intuition still leads to

- correct(ish) statements
- incomplete proofs
- *locally* incorrect proofs

but sometimes not!

A story in 3 stages: 2004

Annals of Mathematics, **159** (2004), 597–639

Quasi-projectivity of moduli spaces of polarized varieties

By Georg Schumacher and Hajime Tsuji

A story in 3 stages: 2006

Annals of Mathematics, **164** (2006), 1077–1096

Non-quasi-projective moduli spaces

By János Kollár

A story in 3 stages: 2023

Annals of Mathematics **198** (2023), 1305
https://doi.org/10.4007/annals.2023.198.3.7

Retraction: "Quasi-projectivity of moduli spaces of polarized varieties"

By Georg Schumacher and Hajime Tsuji

Some other examples

- Italian school of algebraic geometry: too much intuitive arguments, using inadequate foundations
- Kapranov–Voevodsky:
  1. paper from 1991
  2. counterexample by Simpson in 1998
  3. mistake was only found in 2013
  4. convinced Voevodsky of spending last decade of his life on foundations and formal proofs
- Inter-Universal Teichmüller Theory...

Lean

Formal proof verifiers

in the rigorous stage, mathematics is about careful manipulation of axioms and beyond

one can teach a computer these rules!

formal proof verifier

or **interactive theorem prover**: it *helps* you to prove (new) theorems

many exist, we'll talk about Lean, and do an example

Pascal's triangle

$\mathrm{P}_{a,b}$ for $a \geq 0, b \geq 0$ defined by

- $\mathrm{P}_{a,0} = 1$
- $\mathrm{P}_{0,b+1} = 1$
- $\mathrm{P}_{a+1,b+1} = \mathrm{P}_{a+1,b} + \mathrm{P}_{a,b+1}$


```
def pascal : ℕ → ℕ → ℕ
  | a, 0 => 1
  | 0, b + 1 => 1
  | a + 1, b + 1 => pascal (a + 1) b + pascal a (b + 1)
termination_by _ a b => a + b
```

An inequality

Theorem for all $a, b \geq 0$ we have

$$\mathrm{P}_{a,b} \leq (a+b)!$$

or in Lean:

```
theorem pascal_le (a b : ℕ) : pascal a b ≤ (a + b)!
```

Lean is interactive! let's see it in action

Success stories of Lean

Elementary vs. advanced

elementary does not mean easy, just less machinery

- formal proof verifiers have always been good at elementary things, and only get better
- Freek's 100 theorems:
  `https://www.cs.ru.nl/~freek/100/`
- Lean and mathlib know basically all undergraduate material!
- Lean and mathlib are strong enough to do formalization of Annals-worthy research: cap-set problem
  `https://lean-forward.github.io/e-g/`

however, modern mathematics is usually not elementary...

2019: formalization of definition of Scholze's perfectoid spaces

Beyond the basics?

but can Lean do advanced proofs for advanced objects?

Peter Scholze proved a theorem that he was unsure about:

- scope too large to fit it at once in your head
- advanced result in a new area of mathematics using very advanced tools

Statement

Theorem Let $0 < p' < p \leq 0$ be real numbers, let S be a profinite set, and let V be a p-Banach space. Let $\mathcal{M}_{p'}(S)$ be the space of p'-measures on S. Then

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

for $i \geq 1$.

```
variables (p' p : ℝ≥0)
[fact (0 < p')] [fact (p' < p)] [fact (p ≤ 1)]

theorem liquid_tensor_experiment
  (S : Profinite) (V : pBanach p) :
  ∀ i > 0, Ext i (M_{p'} S) V ≅ 0 :=
```

combination of homological algebra, functional analysis, category theory

Liquid Tensor Experiment: result

Liquid Tensor Experiment: challenge to formalize the proof

took only a year and a half! contributions by many people: problem can be broken into many pieces and Lean guarantees that things are correct

- a proof can be done by many people
- without any one of them understanding or worrying about the entire proof
- mathematics becomes more like engineering: an airplane isn't designed by one person either

Lean and AI

large-language models can be trained using formal proofs

- let AI suggest steps in the proof
- Lean is there to make sure that the AI does not hallucinate

AlphaProof and AlphaGeometry 2 (AIs like AlphaGo, trained by Google) can win a silver medal at the IMO!

`https://deepmind.google/discover/blog/ai-solves-imo-problems-at-silver-medal-level/`

Lean and AI can become excellent support for research:

- no more lemmas “left to the reader” which turn out to have issues: **interactive theorem prover**
- refereeing with proof assistants becomes easier

Lean at Uni.lu

Lean within GRACE and Uni.lu

- get familiar with Lean, and use it in teaching
- not (necessarily) for research-level mathematics
- future more in-depth events will be organized

want to get hands-on experience? supervise EML projects! (not just Lean either)