The Lean Theorem Prover

And Formal Mathematics

What is proof?

Historical failures of the social process of proof

- The italian school of algebraic geometry (~1930s, ~1950s)
- Mochizuki's proof of the ABC conjecture with IUTT (2010s)
- Motivic cohomology/homotopy theory (1986-2000)
- Me (last week, also many other times)

"Starting from 1993, multiple groups of mathematicians studied my paper at seminars and used it in their work and none of them noticed the mistake. And it clearly was not an accident. A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail." - Voevodsky

Historical failures of the social process of proof

Frequently people announce subtly flawed proofs that are caught.

- P=NP
- Fundamental theorem of algebra
- FLT
- Jacobian conjecture
- Many many many others

What about ones that aren’t caught?

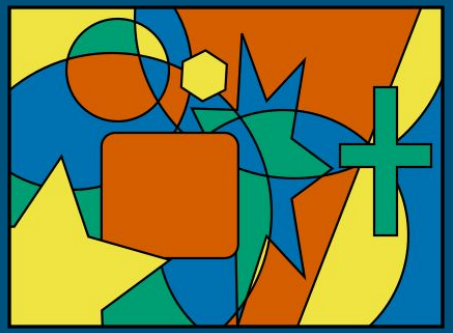
What is Lean?

- A general purpose, dependently typed programming language, developed by Microsoft Research
  - Whose type system is expressive enough to encode mathematics
- A notation for writing mathematical proofs, like LaTeX
- A community of mathematicians & computer scientists
- A tool for gaining greater confidence in the correctness of proofs/validity of mathematical results

What isn’t Lean?

- Lean is an *interactive* theorem prover, not an *automatic* one
- Lean is not the *first* or *only* tool of its kind
  - Coq, Agda, Isabelle/HOL, Metamath, Mizar
  - Agda, Idris, ATS, F*, Haskell, Rust
- Lean is not *mathlib*, the community mathematics library

Some history of formal verification



The Four Color Theorem (Appel and Haken, 1976)

- “Mathematicians usually know when they have gotten too deep into the forest to proceed any further. That is the time Haken takes out his penknife and cuts down the trees one at a time.”
- History of brute force methods, based on Heesch’s method of discharge
- Idea: come up with a big set of (local) configurations of countries where one such configuration appears in any minimal counterexample, then show the configurations are ‘reducible’

Very ad hoc!

Some history of formal verification

The Coq theorem prover (1989)

- Still in active use!
- Formally verified proof of the four color theorem (2002)
- CompCert (2005)
- Formally verified proof of the odd order theorem (2012)

What math has been done in Lean?

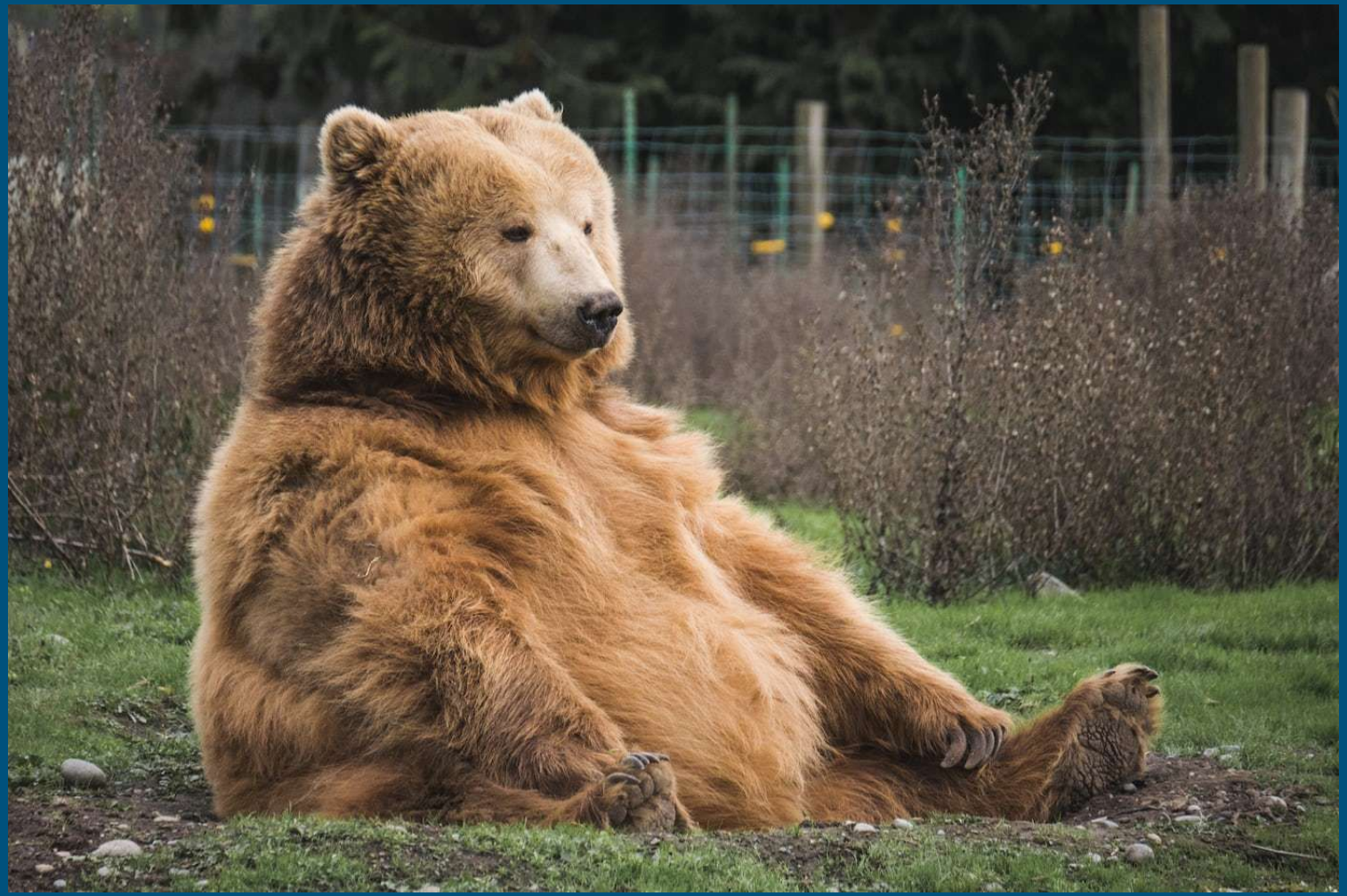
- Fundamental Theorem of Calculus
- Classification of Modules over a PID
- Fundamental Theorem of Algebra
- Abel-Ruffini Theorem
- The Law of Large Numbers
- Sylow’s Theorems
- Existence of Fourier series for L^2 functions

What math has been done in Lean?

- Gromov's h-principle & sphere eversion (geometric topology)
- The main theorem of liquid vector spaces (condensed math)
  - The snake lemma (homological algebra)
- Phragmen-Lindelöf principle (complex analysis)
- Brouwer fixed point theorem (algebraic topology, by me!)
- Hilbert's Nullstellensatz (commutative algebra/AG)

Brouwer Fixed Point Theorem

- Proof adapted from Algebraic Topology by Tammo tom Dieck. Minor indexing error was found!
- Over 14k LOC 🤯
- ~Three months of dedicated work by one person
- Required developing homological algebra, some theory of convex bodies, basic lemmas in general topology
- Every project makes the next one easier!



Further Resources

- https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/
- MacKenzie, D. A. (2001). Mechanizing Proof.
- On proof and progress in mathematics
- ”Theoretical Mathematics”: Toward a cultural synthesis of mathematics and theoretical physics
- Social Processes and Proofs of Theorems and Programs
- https://www.ias.edu/ideas/2014/voevodsky-origins
- https://retractionwatch.com/category/by-subject/physical-sciences-retractions/math-retractions/