



25 April, 2025

# Mathematics without proof assistants will be bizarre

Pim Otte PhD Candidate

# Outline

Introduction

Proof assistants: Why?

Proof assistants: How?

Conclusion



# Outline

#### Introduction

Proof assistants: Why?

Proof assistants: How?

Conclusion



#### About me

- Pim Otte
- PhD candidate at Utrecht University & Technical University of Eindhoven
- Topic "Type Theory for Education"
- Webpage: https://pim.otte.dev



# Outline

Introduction

#### Proof assistants: Why?

Proof assistants: How?

Conclusion





Photo by Gode Nehler



Year	Work in progress	Published work
1670	Pen and paper	Pen and paper



Year	Work in progress	Published work
1670	Pen and paper	Pen and paper
1930	Pen and paper	Typewriter



Year	Work in progress	Published work
1670	Pen and paper	Pen and paper
1930	Pen and paper	Typewriter
2025	(Virtual) Pen and paper	LaTeX



Year	Work in progress	Published work
1670	Pen and paper	Pen and paper
1930	Pen and paper	Typewriter
2025	(Virtual) Pen and paper	LaTeX
2075	?	Proof assistant



### **Proof assistants**

• Interactively encode mathematics in a formal system



### **Proof assistants**

- Interactively encode mathematics in a formal system
- Why? To help mathematicians with better tools



• Verification



- Verification
- Help scale mathematical collaboration



- Verification
- Help scale mathematical collaboration
- Theorem search



- Verification
- Help scale mathematical collaboration
- Theorem search
- Automated (partial) proof



• What is the role of a proof?



- What is the role of a proof?
  - Convey truth of a theorem



- What is the role of a proof?
  - Convey truth of a theorem
  - Explain a mathematical idea



• Computer assisted proofs: The four colour theorem [G<sup>+</sup>08]



- Computer assisted proofs: The four colour theorem [G<sup>+</sup>08]
- Mathematical doubt: The Liquid Tensor Experiment [Buz22] [Com21]



• Liquid Tensor Experiment (29 contributors)



- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)



- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat's Last Theorem (ongoing) (44 contributors)



- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat's Last Theorem (ongoing) (44 contributors)
- Equational Theories (56 contributors)



- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat's Last Theorem (ongoing) (44 contributors)
- Equational Theories (56 contributors)
- Mathlib (413 contributors)



• Problem: Generative AI is hit or miss



- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification



- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification
- Positive feedback loop (during training and at runtime)



- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification
- Positive feedback loop (during training and at runtime)
- Examples: AlphaProof [AA24], Deepseek Prover [XGS<sup>+</sup>24]



# Outline

Introduction

Proof assistants: Why?

Proof assistants: How?



• Core idea: Encode mathematical statements as types in a programming language



- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B:  $A \implies B$



- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B:  $A \implies B$
- A function  $f : \mathbb{R} \to \mathbb{Z}$  turns a real number into an integer



- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B:  $A \implies B$
- A function  $f:\mathbb{R}
  ightarrow\mathbb{Z}$  turns a real number into an integer
- A function  $f : A \rightarrow B$  turns a proof of A into a proof of B.



- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B:  $A \implies B$
- A function  $f:\mathbb{R}
  ightarrow\mathbb{Z}$  turns a real number into an integer
- A function  $f : A \rightarrow B$  turns a proof of A into a proof of B.
- Similarly: for P : ℝ → Prop, ∀x : ℝ, P(x) corresponds to a function that provides a proof of P(x) on an input x.



```
theorem example1 {A : Prop} : A \rightarrow A := fun (a : A) => a
```

```
theorem example2 {P : \mathbb{N} \rightarrow \text{Prop}} :
(\forall (n : \mathbb{N}), P n) \rightarrow P 37 :=
fun Pforall => Pforall 37
```



#### **Theorem Search: Demo**



# Automated proof: Demo



### Tactics

```
theorem rearranging (x y z : R) :
    (5*x + y) * z + (3*z)*y = 5*x*z + 4*y*z := by
    ring
theorem integer_inequalities (n m : Z)
    (h : n < 5 * m) (h2 : 5 + n > -m) : m > -1 := by
    omega
theorem linear_inequalities (a b : R) (h : 5*a + b < 10) (h2
    : 9*a - 5*b > -20) : b < 6 := by
    linarith</pre>
```



#### Interactive

```
theorem set_theory (A B C : Set \mathbb{R}) : A \cup (B \cap C) = (A \cup C) \cap
      (A \cup B) := by
  ext v
  constructor
  · intro hv
    simp at hv
    cases' hy with hyA hyBC
    · simp
       constructor <;> left <;> assumption
    \cdot obtain \langle hB, hC \rangle := hvBC
       simp
       constructor <;> right <;> assumption
  · intro hv
    simp at *
    by_cases hvA : v \in A
    · left; assumption
    · simp [hvA] at hv
      right
      exact hv.symm
```



# Outline

Introduction

Proof assistants: Why?

Proof assistants: How?





• Teaching computers mathematics: verification, tools and collaboration



- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda



- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/



- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/
  - Do/join/supervise a project (in Groningen: Marcello Seri)



- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/
  - Do/join/supervise a project (in Groningen: Marcello Seri)
  - Utrecht Summer School



#### References

- AlphaProof and AlphaGeometry, Ai achieves silver-medal standard solving international mathematical olympiad problems, 2024.
- Kevin Buzzard, *Beyond the liquid tensor experiment*, 2022.
- Johan Commelin, *Liquid tensor experiment*, Nieuw Archief voor Wiskunde **22** (2021), no. 4, 231–234.
- Georges Gonthier et al., *Formal proof-the four-color theorem*, Notices of the AMS **55** (2008), no. 11, 1382–1393.
- Huajian Xin, Daya Guo, Zhihong Shao, Zhizhou Ren, Qihao Zhu, Bo Liu, Chong Ruan, Wenda Li, and Xiaodan Liang, Deepseek-prover: Advancing theorem proving in Ilms through large-scale synthetic data, 2024.





#### Utrecht Sharing science, University shaping tomorrow





pim.otte.dev



#### Utrecht Sharing science, University shaping tomorrow



pim.otte.dev