

PROOF ASSISTANTS

Thomas BAUEREISS (tb592), Leo STEFANESCO (lads2)

ACS / Part III CST – 2026-2027

INTRODUCTIONS:

WHO ARE YOU?

Proof Assistants

Proof Assistants



- precise formal notion
- machine-checked

Proof



- precise formal notion
- machine-checked

Assistants



- develop
- maintain & evolve
- *partly* automated

Proof



- precise formal notion
- machine-checked

Assistants



- develop
- maintain & evolve
- *partly* automated

This is about developing computer tools [...] to help researchers and students in new ways. — Kevin Buzzard, 2022 International Congress of Mathematicians

Proof



- precise formal notion
- machine-checked

Assistants



- develop
- maintain & evolve
- *partly* automated

This is about developing computer tools [...] to help researchers and students in new ways. — Kevin Buzzard, 2022 International Congress of Mathematicians

... and programmers and computer scientists too!

A SHORT HISTORY

Prehistory ('70s) AUTOMATH, MIZAR, LCF

A SHORT HISTORY

Prehistory ('70s) AUTOMATH, MIZAR, LCF

Four colour theorem (2005) first “important” certified proof

CompCert (2005), seL4 (2009) “real-life” certified programs

Odd order theorem (2012), Flyspeck (2014) first big mathematical theorems

A SHORT HISTORY

Prehistory ('70s) AUTOMATH, MIZAR, LCF

Four colour theorem (2005) first “important” certified proof

CompCert (2005), seL4 (2009) “real-life” certified programs

Odd order theorem (2012), Flyspeck (2014) first big mathematical theorems

HoTT, Liquid Tensor Experiment (2021) proof assistants for cutting-edge maths

Fiat Crypto (2017-...), Everest (2016-...), Cedar (2023-...), AWS Nitro (2025-...) formal proofs
in large tech companies, integration in mainstream applications

A SHORT HISTORY

Prehistory ('70s) AUTOMATH, MIZAR, LCF

Four colour theorem (2005) first “important” certified proof

CompCert (2005), seL4 (2009) “real-life” certified programs

Odd order theorem (2012), Flyspeck (2014) first big mathematical theorems

HoTT, Liquid Tensor Experiment (2021) proof assistants for cutting-edge maths

Fiat Crypto (2017-...), Everest (2016-...), Cedar (2023-...), AWS Nitro (2025-...) formal proofs
in large tech companies, integration in mainstream applications

LLM-based autoformalisation Fermat's last theorem, Navier-Stokes (2026)

A SHORT HISTORY

Prehistory ('70s) AUTOMATH, MIZAR, LCF

Four colour theorem (2005) first “important” certified proof

CompCert (2005), seL4 (2009) “real-life” certified programs

Odd order theorem (2012), Flyspeck (2014) first big mathematical theorems

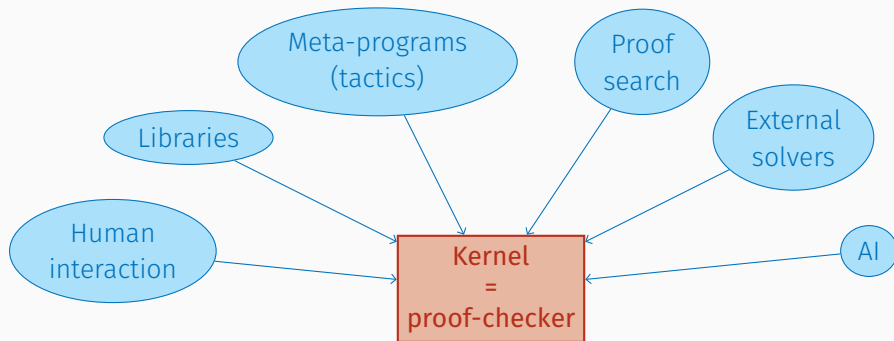
HoTT, Liquid Tensor Experiment (2021) proof assistants for cutting-edge maths

Fiat Crypto (2017-...), Everest (2016-...), Cedar (2023-...), AWS Nitro (2025-...) formal proofs
in large tech companies, integration in mainstream applications

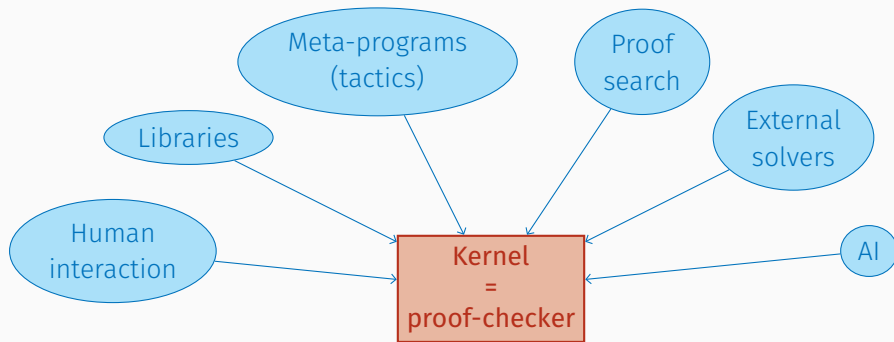
LLM-based autoformalisation Fermat's last theorem, Navier-Stokes (2026)

...and many more

THE KERNEL AND THE REST



THE KERNEL AND THE REST



Demo in a minute

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs
- But formal verification experts still needed to guide AI

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs
- But formal verification experts still needed to guide AI
 - to decide what is worth verifying (and maintaining)

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs
- But formal verification experts still needed to guide AI
 - to decide what is worth verifying (and maintaining)
 - to specify properties

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs
- But formal verification experts still needed to guide AI
 - to decide what is worth verifying (and maintaining)
 - to specify properties
 - to recognise when AI agents are going down a dead end and steer them back on track

- Huge increase in demand for formal verification, e.g.
 - of security properties of software in defense against hacking AI agents
 - of correctness properties of AI-generated code
- Huge increase in capability of AI agents writing proofs
- But formal verification experts still needed to guide AI
 - to decide what is worth verifying (and maintaining)
 - to specify properties
 - to recognise when AI agents are going down a dead end and steer them back on track
 - to structure proofs and come up with useful abstractions

Higher-order logic



HOL Light

PVS

Higher-order logic



HOL Light

PVS

Dependent type theory



} general
purpose

} dep. typed
programming

program
verification

A FAMILY PICTURE

Higher-order logic



HOL Light

PVS

Dependent type theory



general
purpose

dep. typed
programming

program
verification

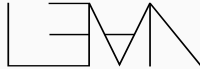
And many many more



...

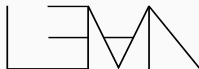


+





+

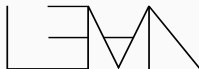


goals basic autonomy & familiarity, transferable knowledge

subject basic PL theory *à la* Part IB – Semantics



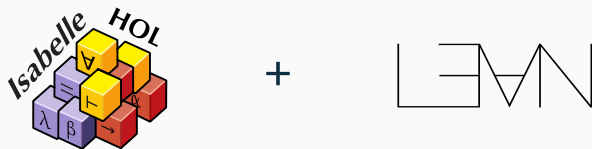
+



goals basic autonomy & familiarity, transferable knowledge

subject basic PL theory *à la* Part IB – Semantics

Resources on the course webpage!



goals basic autonomy & familiarity, transferable knowledge

subject basic PL theory *à la* Part IB – Semantics

Resources on the course webpage!

Thanks to Meven Lennon-Bertrand (now at ENS Rennes) for co-lecturing a previous version of this course and providing material for this year's course.

- 6 ISABELLE/HOL lectures (Bauereiss)
- 5 LEAN lectures (Stefanescu)
- 4 practical sessions (bring your computer)

- Two assignments
 - each with a small verification project
 - one in ISABELLE/HOL, one in LEAN.

- Two assignments
 - each with a small verification project
 - one in ISABELLE/HOL, one in LEAN.
- Focus on learning how to use the proof assistants with your own fingertips
 - No AI tools, except where explicitly permitted in the task description
 - Vivas after submission of both assignments

INSTALL THE PROOF ASSISTANTS

TODAY !

INSTALL THE PROOF ASSISTANTS
TODAY !

Instructions on the course webpage.