Proof Assistants

Thomas Bauereiss (tb592), Meven Lennon-Bertrand (mgapb2)

Part III CST – 2024-2025

Who are you?

Proof Assistants

Proof Assistants

- precise formal notion
- machine-checked

Proof Assistants

- precise formal notion
- machine-checked

- develop
- maintain & evolve
- *partly* automated

Proof Assistants

- precise formal notion
- machine-checked

- 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 Assistants

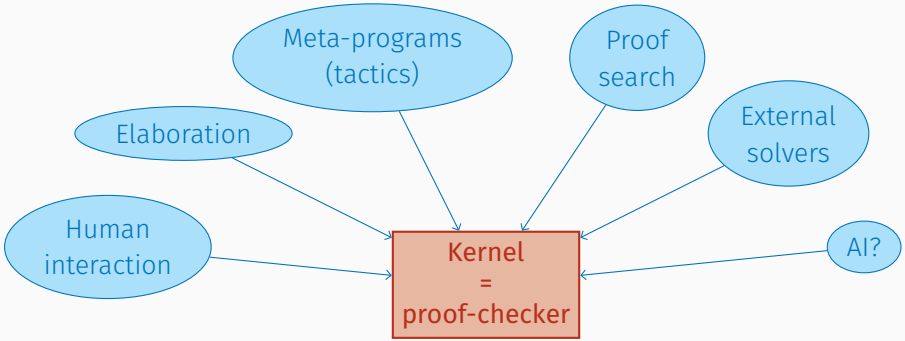
- precise formal notion
- machine-checked

- develop
- maintain & evolve
- *partly* automated

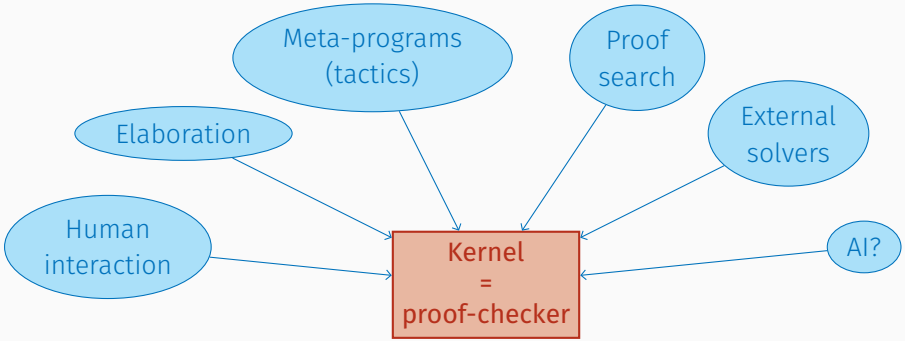
This is about developing computer tools [...] to help researchers and students in new ways. — Kevin Buzzard, 2022 International Congress of Mathematicians

... and programmers too!

The kernel and the rest



The kernel and the rest



Demo in a minute

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

BoringSSL (2017-...), Everest (2016-...) integration in mainstream applications
HoTT, Liquid Tensor Experiment (2021) proof assistants for cutting-edge maths

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

BoringSSL (2017-...), Everest (2016-...) integration in mainstream applications
HoTT, Liquid Tensor Experiment (2021) proof assistants for cutting-edge maths

... and more papers/projects than I can name!

Higher-order logic

HOL Light

PVS

A family picture

Higher-order logic

HOL Light

PVS

Dependent type theory

Coq → Rocq

general purpose

Agda

dep. typed programming

program verification

A family picture

Higher-order logic

HOL Light

PVS

Dependent type theory

Coq → Rocq

general purpose

Agda

Idris

dep. typed programming

program verification

And many many more

...

This course

+

This course

+

goals basic autonomy & familiarity, transferable knowledge

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

This course

+

goals basic autonomy & familiarity, transferable knowledge

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

Resources on the course webpage!

Structure

- ~6 Isabelle/HOL lectures (Bauereiss)
- ~5 Coq lectures (Lennon-Bertrand)
- 4 practical sessions (bring your computer)

Structure

- ~6 Isabelle/HOL lectures (Bauereiss)
- ~5 Coq lectures (Lennon-Bertrand)
- 4 practical sessions (bring your computer)

Assignements: two small projects, one in Isabelle/HOL, one in Coq.

Install the proof assistants

NOW !

Install the proof assistants

NOW !

Instructions on the course webpage.