An overview of Coq

What is Coq?

- A proof assistant developed by INRIA
  - https://coq.inria.fr/

  - Coq is a formal proof management system. It provides a formal language to write mathematical definitions, executable algorithms and theorems together with an environment for semi-interactive development of machine-checked proofs …

What is Coq?

- A functional programming language with rich type system
  - Define inductive data types and write algorithms manipulating them.
  - All programs must terminate.
- A higher-order logic with interactive theorem prover
  - Allows you to reason about mathematical structures and your programs
  - Generates machine-checkable proofs
- A meta-language/logic
  - Allows you to encode another language/logic and prove the properties of that language/logic

Why Coq?

- To have more rigorous formal reasoning
  - For mathematics and program verification
  - Tools like Coq boost program verification

Program verification under attack

Reports and Articles

Social Processes and Proofs of Theorems and Programs

[CACM 1979]

Richard A. De Millo
Georgia Institute of Technology

Richard J. Lipton and Alan J. Perlis
Yale University

Mathematical proofs can often be wrong!

Program verification would never work …

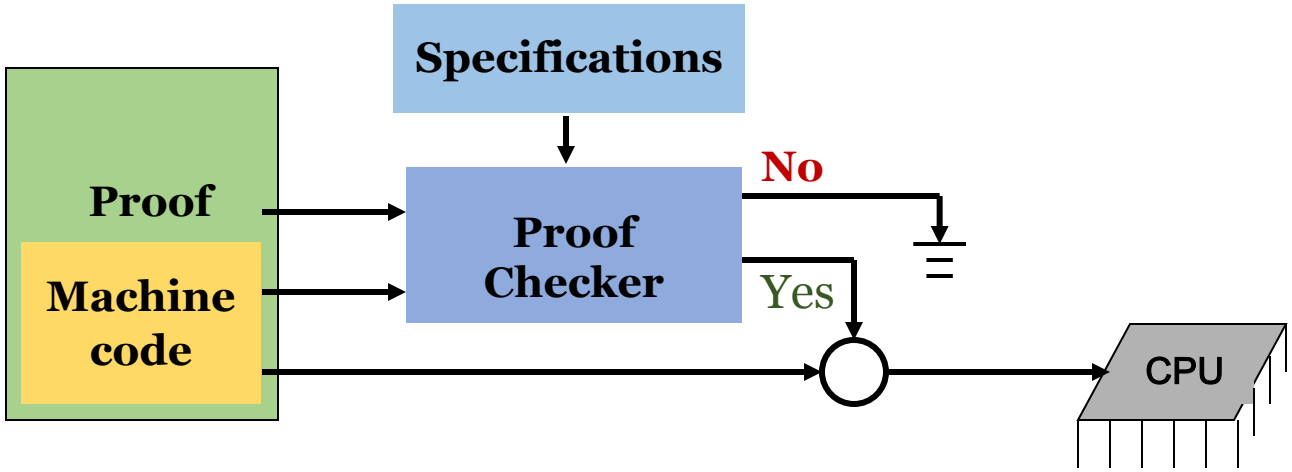
Mathematics is trustworthy because of the social process to check/validate proofs.

But nobody would care or check proofs for programs: "*The verification of even a puny program can run into dozens of pages, and there's not a light moment or a spark of wit on any of those pages. Nobody is going to run into a friend's office with a program verification … Nobody is ever going to read it.*"

Problem addressed by tools like Coq

- Proofs are mechanized and machine-checkable
  - through Curry-Howard isomorphism [first published paper in 1980]
  - Proof checking is as simple as type checking
    - Fully automatic
    - Very simple algorithm
  - No longer need to trust the proofs
    - Check them!
    - Only need to trust the proof checker
      - Simple, can be reviewed by human experts …

A framework for certified software



- certified code (code + proof)
- specifications:
  lang. semantics + program safety / security / correctness …
- automated proof checker
  need not trust the correctness of proofs

Applications of Coq

- Formal proofs of mathematical theorems
  - Formal proof of 4-color theorem
    - By Georges Gonthier and Benjamin Werner, 2004
  - Other: Feit–Thompson theorem proved in Coq in 2012
- Formal verification
  - OS kernels and hypervisors
    - CertiKOS project at Yale
    - seL4 in Isabelle at NICTA
  - Compilers
    - CompCert at INRIA and following projects
    - LLVM verification and Upenn
  - Others
    - Web servers (bedrock projects @ MIT)
    - Certified software tool chains (e.g., analysis algorithms) @ Princeton
- Teaching: logic, programming languages, …

Gains lots of popularity

Coq Selected As Recipient Of The 2013 Software System Award

Other recipients of the award:
Unix、TCP/IP、World-Wide Web、Java、Make、VMWare、Eclipse、LLVM …

Demo:

- Small examples

- Imp in Coq (syntax and operational semantics)