Computational Proof Assistants

Kevin Liu

Canadian Undergraduate Mathematics Conference, July 2024

Table of Contents

Motivation

- Writing correct software is hard!
- Theorem provers can ensure mathematical correctness of code (Compcert)
- Formal verification is becoming widely used in industry for critical tasks (Microsoft, Intel)
- Can formally prove many results in mathematics (4-color theorem)

Coq

- Coq is an interactive proof assistant for formal verification
- Developed in 1984 by INRIA (France)
- Includes a programming language (Gallina) and can check proofs for correctness
- Can "extract" Coq proofs into OCaml or Haskell scripts

How Coq Works

Cheatsheet

The Curry-Howard Isomorphism

Theorem

Examples

- $$A \implies B \equiv f : A \to B$$
- $$A \wedge B \equiv (A, B)$$

Remark

- Direct link between computation and logic
- Programs (functions) are equivalent to Proofs
- Proofs can be run!

References

- Coq Website
- Coq GitHub
- Software Foundations
- Coq in a Hurry
- Curry Howard for Dummies
- CS 3110 Textbook @ Cornell