Mechanization of Proof:
From 4-Color Theorem to Compiler Verification

Chung-Kil Hur (허충길)

Department of Computer Science and Engineering
Seoul National University

My passion towards rigorous math

My question when I was young:

Can we do math rigorously?

In a set theory course:

Yes! We can do math only using first-order logic with ZFC.

But, I was disappointed:

because it looked practically impossible to do math in such a way.

Formal math thanks to computers

Now I do math formally using Coq:
Computers do such tedious details for me!

I will talk about Coq today.

What Is A Proof Assistant?

- Underlying Logic for constructing Propositions & Proofs
- Set theory in the Logic for defining Sets & Elements
- Tool that implements such a logic and a set theory
- Independent Proof Checker that checks validity of given definitions and proofs

Examples of Proof Systems

- Conventional Mathematics
  - First-order logic
  - Zermelo–Fraenkel set theory with the axiom of choice (ZFC)
  - No Mechaniztion
- Isabelle/HOL
  - Higher-order logic
  - Function Space + Inductive Set
  - Tool and Proof Checker
  - Developed at University of Cambridge & Technical University of Munich
- Coq
  - Calculus of Construction (Logic = Set Theory = Programming Language)
  - Tool and Proof Checker
  - Developed at INRIA, France

Demo of Coq

Set Theory

= Logic

= Programming

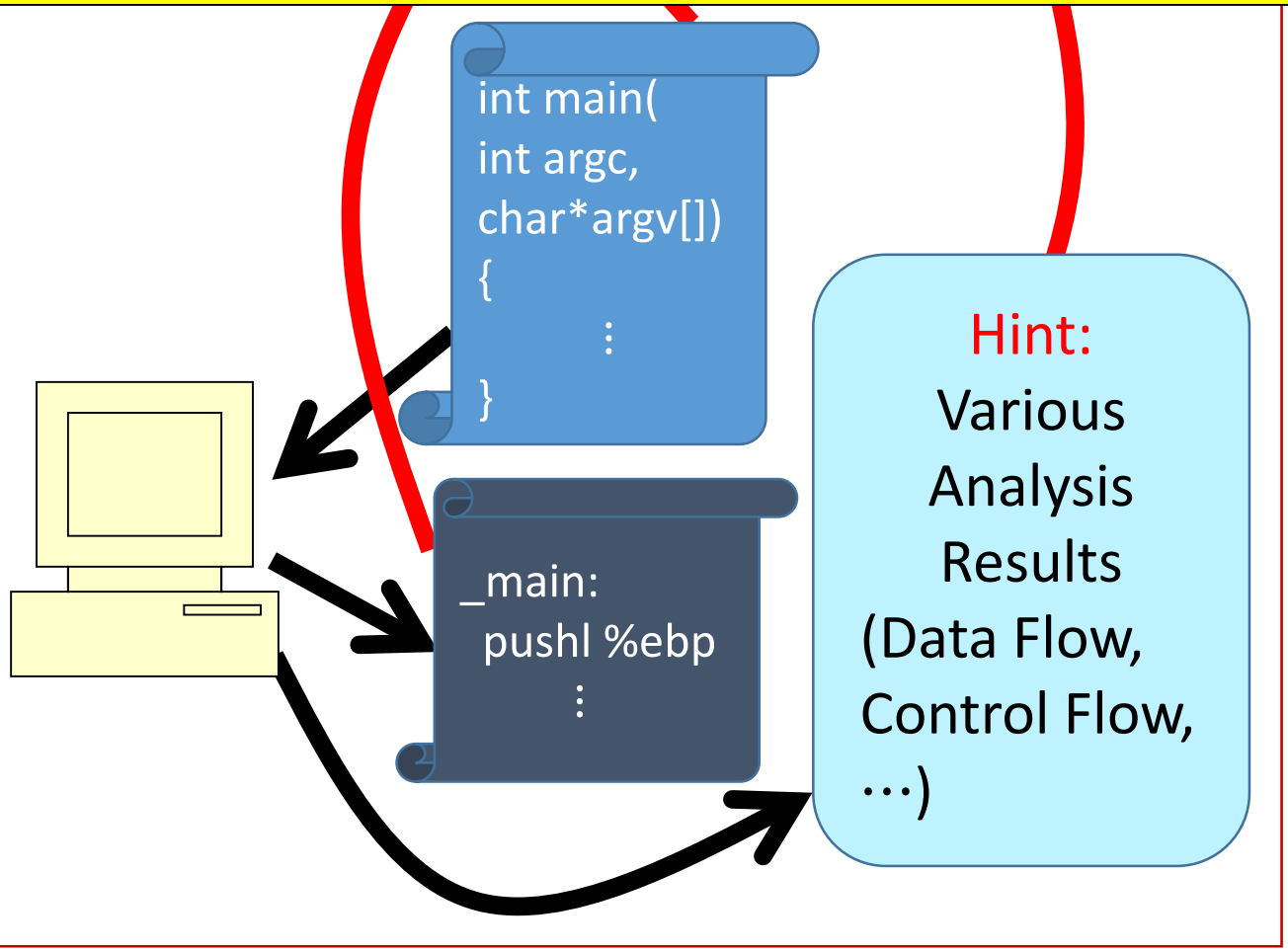
Applications of Proof Assistants

- 4-Color Theorem & Feit-Thompson theorem
  - Any map in a plane can be colored using four-colors.
  - Every finite group of odd order is solvable.
  - Mechanized in Coq by Georges Gonthier.
  - (Note) Kenneth Appel and Andrew Appel.
- seL4 (secure embedded L4)
  - Fully verified highly-optimized Microkernel based on L4
  - at NICTA, Isabelle/HOL
- CompCert
  - Fully verified optimizing C compiler
  - at INRIA, Coq (by Xavier Leroy)
  - 79 bugs in GCC, 202 bugs in LLVM, no bugs in CompCert
  - Its use in Airbus is being investigated.
- Security Protocols, Homotopy Type Theory, …

My Research: Compilation Validation

Validators can guarantee absence of bugs.

We are currently developing
a Verified Validator for LLVM Compiler.



∀ S T H, validator(S,T,H) →
equivalent_prog(S,T).
Proof.
…
Qed.

Proof Checker

Let me now talk about Calculus of Construction

Calculus of Constructions (CoC)

- Calculus of (Inductive & Coinductive) Construction
  - The type theory behind Coq
  - Introduced by Thierry Coquand (1985)
  - Constructive mathematics, intuitionistic logic
- History of Coq
  - 1984: Coquand and Huet start to develop Coq
  - 1989: Coquand and Paulin extend CoC to CIC
  - 1994: Eduardo Giménez extends CIC to CICC
  - 2014: Coq version 8.4 (still actively being developed)
  - Extract to a program (only constructive part)
  - Story behind the name Coq
    1. Coq is the symbol of France.
    2. Coq ~ COC (Calculus Of Construction)
    3. Thierry COQuand

Type: The Set of All Sets

Type Formation Rules

Term Formation Rules (1)

Term Formation Rules (2)

Computation Rule (Equational theory)

As a Set Theory

As a Programming Language

As a Logic

Size Problem

Proposition

Subset Construction

Demo