Program verification and logic

Aleksy Schubert

What is HAHA?

- HAHA is a tool to teach Hoare logic
- one can write small programs
- one can write Hoare logic assertions
- one can write loop invariants etc.
- one can push a button to have a program verified

HAHA demonstration

Small demo. . .

How to debug specifications in HAHA?

We can use Coq proof assistant for that!!!

but to do this we need support in comprehensible tactics...

Tactics

We developed a number of Coq tactics that solve simple problems and make it possible to perform basic operations on inequalities that we know from the primary school.

But we need more!

Interpreter for HAHA

We can verify programs in HAHA.

We can even compile them!

But we cannot execute them step by step.

We need an interpreter written in Coq/Ocaml.

Verification with Frama-C/Why3

Small demo

Verification with Frama-C/Why3

We have a small code base written in C (a type checker).

We have an advanced verification project around the code.

We can find some important tasks in verification:

- verification of memory management,
- verification of correctness of substitution.

Intuitionistic propositional logic and connectives

Intuitionistic propositional logic...

$$p \to q, \quad (p \to q) \to p \to p, \quad (p \to q) \to p \to q, \quad p \vee \neg p$$

is PSPACE-complete, but...

- It is PSPACE-complete when there are arbitrary many atoms.
- It is PSPACE-complete when there are two atoms and $\to, \vee$ connectives.
- It is PTIME-complete when there is $\to$ and two atoms (any fixed number of atoms).

Questions?

- What about two atoms and $\to, \wedge$?
- What about two atoms and $\neg, \vee$?

Intuitionistic predicate logic and automata

We have an automata model such that

> *Automaton A_φ has an accepting run if and only if φ is provable.*

These automata accept languages of proofs.

- What are the complexities of the operations to construct the sum of two languages, intersection, etc.
- What is the relation of the automata to so called automata with atoms?
- What is the relation of the automata to DPLL?

Summary

- HAHA
  - Develop tactics for Coq support
  - Develop interpreter for HAHA in Coq/Ocaml
- Frama-C/Why3
  - Verification of memory management using Frama-C/Why3
  - Verification of correctness of substitution in a typechecker
- Intuitionistic propositional logic
  - What is the complexity of the logic with two atoms and $\rightarrow, \wedge$?
  - What is the complexity of the logic with two atoms and $\neg, \vee$?
- Intuitionistic predicate logic
  - What are the complexities of the operations to construct the sum of two languages, intersection, etc.
  - What is the relation of the automata to so called automata with atoms?
  - What is the relation of the automata to DPLL?