Karlsruher Institut für Technologie

Demo of AlgoVer

Institut für Theoretische Informatik

Motivation

- Proofs conducted on different levels
  - the code itself (needs insight if not closing)
  - the logic level (needs relation back to original program)
- state of the art user interfaces focus only on one level, supporting features for other levels often insufficient
- may hinder users from using/understanding it

AlgoVer: Seamless Program Verification

- allows to inspect different parts of the proof in individual views
- supports insight into unfinished proof attempts
- seamless transition between different views
- conduction proofs possible via
  - direct manipulation
  - script based
  - annotation based

Demo

DEMO

Future Work

- more rules and strategies
- better smt-support
- feedback back to source code
- evaluation on larger examples
- ...