Some Hot Topics in Scilex-3: From High-level to Low-level Certification

Digicosme Research Days

Virgile Prevosto

November 10th, 2020

Université Paris Saclay, CEA, List

Current Perimeter

Program Verification Techniques

- Deductive Verification
- Abstract Interpretation
- Model Checking
- Testing
- ...

Certification Methodologies

- Combining techniques on a given artifact ("Horizontal" composition)
- Verification at various abstraction levels ("Vertical" composition)

Security and Privacy Properties

- Strong links with Scilex-1 and Comex
- Differences between safety-oriented and security-oriented formal properties
- New specification languages
- New verification techniques

New programming paradigms

Distributed Computing

- Blockchain and Smart Contracts
- Formal semantics of high-level smart contracts
- Formal verification of low-level transactions

Quantum Computing

- New programming languages
- New verification techniques

New Development Processes

DevOps and Continuous Integration

- Need far more modularity
- Assess impact of changes on proofs, abstract states, ...
- Reuse analysis results

Certified Certification Tools

Quis Custodiet Ipsos Custodes

- Few actual formal verification tools are themselves formally certified
- Formal semantics of actual programming languages
- Certified Analyzers in Coq or Isabelle, or ...
- Proof certificates from automated theorem provers that can be independently checked

Trusted Artificial Intelligence

- Strong links with IID
- Explainable AI
- How to specify the correctness of an algorithm based on learning techniques?
- Once specification is done, how to verify the implementation (including training material) is correct?

Artificial Intelligence in Software Verification

- Strong links with IID
- Exploit NLP techniques to extract information from informal document and help write formal specifications
- Train algorithms to partition programs according to various characteristics
  - fine-tuning analyzers
  - generate auxiliary specifications (loop invariants)