Formal Verification – The Big Picture

Paul Jackson
Paul.Jackson@ed.ac.uk

University of Edinburgh

Formal Verification
Autumn 2023

Hardware FV in industry

Internal

- Intel
- AMD

Heavy use made of model checking.
Proof assistants also used for floating-point units.

EDA (Electronic Design Automation) companies

- Cadence
- Mentor
- Synopsys
- Many specialised start-ups . . .

Offer formal and semi-formal verification tools, integrated with simulators for hardware design languages.

Software FV in Industry

Microsoft Research

- RISE group (Research in Software Engineering)
- Many in-house applications of FV
- Tools: Z3 SMT solver, Corral (Boogie, whole concurrent program), Verisol (Solidity), ...

Facebook

- Infer Static Analyzer freely available
- Works with Android, Java, C, C++, iOS/Objective-C

Amazon Web Services

- Automated Reasoning Group
- Enhancing security assurances is key to winning customers

Software FV in Industry (continued)

- Imandra
  FV for high-frequency trading. Ensuring traders play fair

- DiffBlue
  Originally commercialising CBMC & extensions
  Focus now on automatic generation of unit tests

- AdaCore
  - SPARK Pro (GNATprove)
  - CodePeer – an abstract interpretation-based formal tool that can establish simpler program properties. Can reduce effort required for using GNATprove.

Conferences & Organisations

- CAV(Computer-Aided Verification)
- FMCAD (Formal Methods for Computer-Aided Design)
- Formal Methods Europe
  - FM 2022
  - 2019 World Congress on Formal Methods
- NFM (Nasa Formal Methods)
- ITP (Interactive Theorem Proving)
  - Tools such as Isabelle, Coq, Agda, Lean, HOL4, HOL Light, PVS, ACL2
- VSTTE (Verified Software: Theories, Tools, Experiments)

Projects

- CompCert
  (Formally-verified C compiler)

- DeepSpec
  (US multisite project – FV for hardware & software stack),

- Peter Sewell's group, Cambridge
  (FV for hardware,
  CHERI project with ARM – secure programming with unsafe languages)

- Sel4 MicroKernel
  (Formally-proven correct and secure)