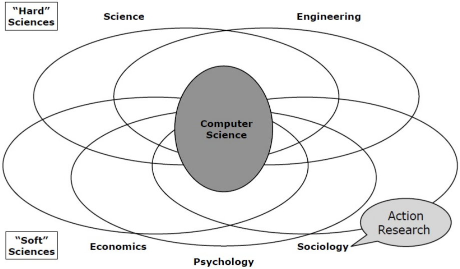
Formal Verification Tools



Lucien Ngalamou

Outline

References

Limitations of Testing and Simulation

Formal Methods Overview

Review of Tools

Highlighted Projects

References

- Formal Methods In Software Product Lines: Concepts, Survey, and Guidelines (http://sat.inesc-id.pt/ mikolas/Lero-TR-SPL-2008-02.pdf)
- Survey of Existing Tools for Formal Verification, Sandia National Lab (http://prod.sandia.gov/techlib/access-control.cgi/2014/1420533.pdf)
- Formal Methods: Practice and Experience (http://homepage.cs.uiowa.edu/ tinelli/classes/181/Fall14/Papers/W

Limitations of Testing and Simulation

- Testing and simulation consist of providing a system with a variety of input conditions and ensuring that the output is as predicted.
- The inputs to be provided may be crafted by a designer or randomly generated (test vectors). These methods sample the response of the systems to chosen inputs.
- How do you know assure the completeness of test vectors?
- What are functional, safety, and security properties?
- Other issues such as safety and security properties cannot be verified by testing or simulation

Definition

- Formal methods are mathematical techniques, often supported by tools, for developing software and hardware systems.
- Mathematical rigour enables users to analyse and verify these models at any part of the design(HW or SW) life-cycle.
- Life-cycle elements: Requirements engineering, specification, architecture, design, implementation, testing, maintenance, and evolution.

Steps of the General Process using Formal Methods (FM)

- Create a formal model of the studied system
- Formally express the desired properties of that system
- Attempt prove (show) that the model satisfies these properties.
- If the proving process failed, analyze the cause so the model can be amended or the property adjusted.
- To create a formal model, one needs an underlying formal system in which to build the model. Formal methods are mathematical techniques, often supported by tools, for developing software and hardware systems.

Logics

- Logics are the languages of mathematics used to formally capture the concepts about which one wishes to reason. Often, FM practitioners are not writing in a logic directlyrather they are using a language tailored for the particular domain.
- There are two main properties of a logic that determine its suitability for a particular problem. One property is its expressiveness, i.e., which concepts are expressible in that logic and how easily such is done. A second property is the difficulty of constructing proofs for statements in that logic.

Logics (2)

- Propositional logic is a logic with two-values for each variable1, true and false, and the formulas are typically expressed using Boolean connectives (!, ", etc.) and negation.

- Propositional logic is decidable, meaning that there exists an algorithm that decides whether a given formula is a tautology (evaluates to true under any valuation of variables, also known as being valid) or not.
- First-order logics (FOL or predicate logic) are propositional logics embellished with quantifiers used to express things such as multiplication by 0 yields 0

Logics (3)

- FOL are (in the general case) semi-decidable, meaning that there exists an algorithm that, for a given formula, terminates if that formula is valid.
- Higher-order logics (HOL), of which second-order logics are a common variant, enable quantification over functions and predicates, rather than just over variables.

Reasoning

- FOL Logics are used to describe the objects about which one wants to reason. The reasoning itself is an attempt to construct a proof of the desired claim.
- FM provide us with a number of tools with the support of different logics, varying in the degree of automation and time requirements, etc.
- The table below provides an overview of some of the main tools supporting reasoning.

Reasoning (1)

Tool Category	Logic
SAT solvers	propositional logic
Constraint solvers	constraints over finite domains
Model checkers	temporal logic and state transition systems
SMT solvers	decidable fragments of FOL
Automated theorem provers	FOL
Proof assistants	HOL

Class Discussion

- FOL Review of the Article: "Survey of Existing Tools for Formal Verification."
- Identify among the tools presented one that can be used to solve a current problem at your job/profession (Define clearly the rationale).

Formal Methods: Practice and Experience

- Formal Methods: Practice and Experience (Pages 12 to 21)
- A. Haxthausen. An Introduction to Formal Methods for the Development of Safety-critical Applications. Technical report, 2010.