EPFL

CS-550

Formal verification

Kuncak Viktor

Cursus	Sem.	Type
Computer and Communication Sciences		Obl.
Computer science	MA1, MA3	Opt.
Cybersecurity	MA1, MA3	Opt.
Data Science	MA1, MA3	Opt.
SC master EPFL	MA1, MA3	Opt.

Language of teaching	English
Credits	6
Session	Winter
Semester	Fall
Exam	During the semester
Workload	180h
Weeks	14
Hours	**6 weekly**
Courses	2 weekly
Exercises	2 weekly
TP	2 weekly
Number of positions	

Summary

We introduce formal verification as an approach for developing highly reliable systems. Formal verification finds proofs that computer systems work under all relevant scenarios. We will learn how to use formal verification tools and explain the theory and the practice behind them.

Content

Topics may include among the others some of the following:

- Importance of Reliable Systems. Methodology of Formal Verification. Soundness and Completeness in Modeling and Tools. Successful Tools and Flagship Case Studies
- Review of Sets, Relations, Computability, Propositional and First-Order Logic Syntax, Semantics, Sequent Calculus.
- Completeness and Semi-Decidability for First-Order Logic. Inductive Definitions and Proof Trees. Higher-Order Logic and LCF Approach.
- State Machines. Transition Formulas. Traces. Strongest Postconditions and Weakest Preconditions.
- Hoare Logic. Inductive Invariants. Well-Founded Relations and Termination Measures
- Modeling Hardware: Verilog to Sequential Circuits
- Linear Temporal Logic. System Verilog Assertions. Monitors
- SAT Solvers and Bounded Model Checking
- Model Checking using Binary Decision Diagrams
- Loop Invariants. Hoare Logic. Statically Checked Function Contracts. Relational Semantics and Fixed-Point Semantics
- Symbolic Execution. Satisfiability Modulo Theories
- Abstract Interpretation and Predicate Abstraction
- Information Flow and Taint Analysis
- Verification of Security Protocols
- Dependent and Refinement Types

Learning Prerequisites

Recommended courses

Computer Language Processing / Compilers

Important concepts to start the course

Discrete Mathematics

Learning Outcomes

By the end of the course, the student must be able to:

- Formalize specifications
- Synthesize loop invariants
- Specify software functionality
- Generalize inductive hypothesis
- Critique meaningless course description forms

Teaching methods

Instructors will present lectures, conduct whiteboard or blackboard exercises, and supervise labs on student laptops.

Expected student activities

Attend lectures (optional but highly recommended), solve exercises on whiteboard and continue at home as needed, complete computer labs.

Assessment methods

We will assign written exams and grade labs.

Supervision

Office hours	Yes
Assistants	Yes
Forum	Yes

Resources

Bibliography

- Michael Huth and Mark Rayan: Logic in Computer Science - Modelling and Reasoning about Systems. Cambridge University Press 2004.
- Handbook of Model Checking, https://www.springer.com/de/book/9783319105741 Springer 2018. Including Chapter Model Checking Security Protocols by David Basin.
- Tobias Nipkow, Gerwin Klein: Concrete Semantics with Isabelle/HOL. http://concrete-semantics.org/concrete-semantics.pdf
- Aaron Bradley and Zohar Manna: The Calculus of Computation - Decision Procedures with Applications to Verification, Springer 2007.
- Nielson, Flemming, Nielson, Hanne R., Hankin, Chris: Principles of Program Analysis. ISBN 978-3-662-03811-6. Springer 1999.
- Peter B. Andrews: An Introduction to Mathematical Logic and Type Theory (To Truth Through Proof), Springer 2002.
- http://logitext.mit.edu/tutorial

Ressources en bibliothèque

- Handbook of Model Checking
- Aaron Bradley and Zohar Manna: The Calculus of Computation - Decision Procedures with Applications to Verification
- Tobias Nipkow, Gerwin Klein: Concrete Semantics with Isabelle/HOL

- Peter B. Andrews: An Introduction to Mathematical Logic and Type Theory
- Nielson, Flemming, Nielson, Hanne R., Hankin, Chris: Principles of Program Analysis
- Michael Huth and Mark Rayan: Logic in Computer Science - Modelling and Reasoning about Systems

Websites

- https://lara.epfl.ch/w/fv

Moodle Link

- https://moodle.epfl.ch/course/view.php?id=13051

Videos

- https://youtu.be/mm6CCGSDmOw?t=39
- https://www.youtube.com/watch?v=oLS_y842fMc
- https://www.youtube.com/channel/UCP2eLEql4tROYmIYm5mA27A