Formal Methods for System Design
-
Outline for AAs 1 and 2

Mickael Randour
Mathematics Department, UMONS

September 2023

Detailed contents of each chapter, as well as their structure, may be adapted to the actual learning curve and particular topics of interest of the class.

Theory

Chapter 1: Formal verification

- Introduction, motivations, background
  - ▷ Specification, model, verification, model checking, synthesis
  - ▷ Tool support, usage in industry
- Course organization

Chapter 2: Modeling systems

- Transition systems: concepts and examples
- Comparing transition systems
  - ▷ Trace inclusion and equivalence
  - ▷ Bisimulation
  - ▷ Simulation preorder and equivalence

Chapter 3: Linear temporal logic

- Linear time properties: safety, liveness, persistence, fairness
- Linear temporal logic (LTL)
- Automata on infinite words: Büchi automata
- From LTL to Büchi automata
- LTL model checking

Chapter 4: Computation tree logic

- Branching time properties
- Computation tree logic (CTL)
- CTL model checking
- CTL vs. LTL
- CTL*

Chapter 5: Symbolic model checking

- State explosion problem
- Symbolic CTL model checking via ROBDDs
  - ▷ CTL model checking through switching functions
  - ▷ Efficient encoding through ROBDDs
- A glance at other techniques

Chapter 6: Model checking probabilistic systems

- Probabilistic systems and Markov chains (MCs)
- Reachability and limit behavior
- Probabilistic CTL (PCTL)
  - ▷ Semantics
  - ▷ Model checking
  - ▷ PCTL vs. CTL
- Weighted MCs: venturing into the land of quantitative specifications
  - ▷ Shortest path
  - ▷ Mean-payoff

Chapter 7: TBD

For the last part of the course, students will be asked to read and understand a book chapter / article, using their newly acquired knowledge. They will be accompanied by the teaching staff in this task. The precise topic will be chosen by the teaching staff after discussion with the students and based on their interest.

Exercises

Exercise set 1: Modeling systems

- Transition systems
- Trace equivalence
- Bisimulation
- Simulation

Exercise set 2: Linear temporal logic

- Modeling
- Syntax
- Semantics
- Transformations

Exercise set 3: Büchi automata and LTL model checking

- ω-regular expressions
- Büchi automata
- LTL formulae
- Generalized Büchi automata
- LTL to NBA
- Product TS
- LTL model checking

Exercise set 4: Computation tree logic

- Modeling
- Syntax
- Semantics
- Model checking
- Transformations
- CTL vs. LTL, CTL*

Exercise set 5: Symbolic CTL model checking via BDDs

- Switching functions
- Symbolic model checking algorithm
- ROBDDs, SOBDDs

Exercise set 6: Model checking probabilistic systems

- Modeling using Markov chains
- Reachability
- Limit behavior, BSCCs
- PCTL
- Weighted Markov chains: shortest path, mean-payoff

Exercise set 7: TBD