SS 2017
Software Verification
Wrap Up

Prof. Dr. Holger Schlingloff ¹,²
Dr. Esteban Pavese ¹

(1) Institut für Informatik der Humboldt Universität
(2) Fraunhofer Institut für offene Kommunikationssysteme FOKUS
Recap

- What is the idea of bounded model checking?
- How to code the transition relation in PL?
- How to describe maximal paths in a model?
- How to translate temporal formulas into PL?
- How to construct a variable assignment?
- What is the diameter of a model? How can it be determined?
- What else needs to be considered for model checking of (C, Java, Python, ...) programs?
What has been discussed

• In this class, we learned about
  ▪ propositional, predicate, modal logic
  ▪ models and relations between models
  ▪ linear and branching temporal logics
  ▪ specification of safety and liveness
  ▪ model checking by depth-first search
  ▪ symbolic model checking with BDDs
  ▪ timed automata and TCTL model checking
  ▪ probabilistic systems and logics
  ▪ model checking of sequential software
  ▪ parallelism and partial order reductions
  ▪ bounded model checking and applications

• Thanks to Esteban, we were completely in time!
What we have learned

• Thanks for the active participation
  ▪ and thanks for answering all my questions 😊

• For the exercises, we all have learned a lot
  ▪ the world is changing fast

• You now have some solid knowledge on software verification by model checking
  ▪ formal background
  ▪ formalization of specifications
  ▪ underlying algorithms, and
  ▪ some tools (established and experimental)

• You also saw some pointers to further topics
  ▪ advanced
  ▪ applied
Where is this Knowledge Useful?

• Industry
  ▪ safety-critical systems (e.g., train control)
  ▪ “formal thinking”, avoiding errors before they are made (“certified system verifier”)
  ▪ dealing with advanced SE tools

• Academia
  ▪ improvement of current tools, new tools
  ▪ usability and capability enhancement, e.g., combination with interactive verification
  ▪ main challenge: applicability to industrial-sized systems
Typical Projects

- Current industrial projects in this area
  - Modelling correctness of autonomous transport robots and self-driving cars
  - Correctness of future internet middleware
  - Enhancing the FRAMA-C verification environment
  - Safety and security in collaborative systems
  - Verification and testing of medical devices
  - ...

- If you are looking for a bachelor or master’s thesis, or if you are looking for a student’s job, just drop me a note!
Questions and Answers

• Q: date for recap session? A: 7.9.2017
• Q: How is the exam? A: 😊