

METU Department of Computer Engineering

CENG-794 Computer Aided Formal Verification

Instructor: Ebru Aydin Gol

Catalogue description: Modeling systems, linear time properties, linear temporal logic, computational tree logic, model checking, abstraction techniques, state-space explosion problem, model-checking tools, recent topics in formal methods.

Background requirements: Familiarity with propositional logic and automata theory. Basic programming skills. Fundamentals of discrete structures.

Course objectives: By the end of this course the students will be able to

- Explain fundamental concepts in computer-aided formal verification.
- Create mathematical models for sequential and concurrent systems.
- Write and analyze formal properties of the developed models.
- Prove formal specifications of the model to validate system's correctness.
- Use automated verification tools.

Course schedule Monday, 13:40- 16:30

Course outline

Week 1: Introduction to formal methods

Week 2: Modeling sequential systems

Week 3: Linear time properties and regular properties

Week 4: Omega-regular properties and Linear Temporal Logic

Week 5: LTL and model checking

Week 6: LTL model checking - SPIN (tool)

Week 7: Overview & midterm week

Week 8: Computation tree logic (CTL) and CTL model checking

Week 9: CTL model checking tool and CTL*, counter examples

Week 10: Symbolic model checking, equivalences

Week 11: Equivalences and abstractions, challenges in industry

Week 12: Introduction to probabilistic model checking

Week 13: Introduction to formal methods in control and verification of hybrid systems

Week 14: Introduction to metric logics and runtime verification

Textbooks: None

Reference material

Books:

Model Checking, by Edmund M. Clarke, Jr., Orna Grumberg, and Doron A. Peled, Second edition (The MIT Press, 2000)

Principles of Model Checking, by C. Baier and J.-P. Katoen (The MIT Press, 2008)

Logic in Computer Science: Modelling and Reasoning about Systems, Michael Huth and Mark Ryan, Second edition, (Cambridge Univ. Press, 2004)

Grading

Homework (written + tools): %10 + %20

Project: %20

Midterm: %20

Final: %30