METU Department of Computer Engineering
CENG-510 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 conduct: In class. Participation is important. There will be discussions and in-class exercises.

Course outline

1- **Introduction to formal methods**
2- **Modeling sequential and concurrent systems**
3- **Formal specifications (**~2 weeks**)**
4- **Linear Temporal Logic (LTL), LTL model checking, and SPIN (**~ 3 weeks**)**
5- **Computation tree logic (CTL), CTL model checking, CTL* (**~1-2 weeks**)**
6- **Model checking of distributed systems with TLA+ (**~2 weeks**)**
7- **Advanced topics in formal methods**

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 (tentative)

Homeworks (written + tools) + Project: %50
Midterm: %20
Final: %30