# Introduction to Model Checking

**Instructor**
Ali Movaghar

**Overview**

Model checking has evolved into a widely used verification and validation technique for software and hardware systems in the last 40 years. This is especially true for safety-critical applications such as operating systems, high-speed computer networks, wireless mobile systems, cyber-physical systems, the Internet of Things, avionics, industrial process control, nuclear plants, etc. Common properties of such systems are concurrency, timeliness, high performance and dependability needs, and security requirements. The latter two specifications usually require that these systems behave correctly in different scenarios. On the other hand, due to concurrency, the process of proving such correctness is usually very complex. Subtle faults that remain undiscovered using simulation, testing, or peer-reviewing can potentially be revealed using model checking. Model checking is thus an effective technique to expose such potential design faults and to improve software and hardware reliability. Students will get familiar with some popular model-checking tools such as NuSMV, PRISM, and SPIN.

**Topics**

1. **System verification** (1 week)
2. **Models of concurrent systems** (1 week)
3. **Structural Operational Semantics** (1 week)
4. **Linear time properties** (1 week)
5. **Safety and liveness Properties** (1 week)
6. **Regular properties** (1 week)
7. **Model checking regular properties** (1 week)
8. **Linear temporal logic (LTL)** (1 week)
9. **Model checking LTL properties** (2 weeks)
10. **Computational tree logic (CTL)** (1 week)
11. **Model checking CTL properties** (1 week)
12. **Symbolic model checking** (1 week)
13. **Equivalence and abstraction** (1 week)
14. **Probabilistic systems** (1 week)
15. **Probabilistic model checking** (2 weeks)

**Grading Policy**

- Midterm exam 20%
- Final exam 20%
- 6 assignments 30%
- Tools and Presentations: 20%
- Term paper: 10%

**Main Reference**

- C. Baier and J.P. Katoen*, Principles of Model Checking.* MIT Press, 2008.

**Supplementary References**

- E. Clarke, O. Grumberg, and D.A. Peled, *Model Checking*. MIT Press, 1999.
- M. Huth and M. Ryan, *Logic in Computer Science: Modelling and Reasoning about Systems*. Cambridge University Press, 2000.
- R. Alur and T.A. Henzinger, *Computer-Aided Verification*, Draft. 1999.
- Z. Manna and A. Pnueli, *The Temporal Logic of Reactive and Concurrent Systems: Specification*. Springer-Verlag, 1992.
- C. Hoare, *Communicating Sequential Processes*. Prentice-Hall, 1985.
- R. Milner, *Communication and Concurrency*. Prentice-Hall, 1989.