Model Checking

Doron Peled
Bar Ilan University, Ramat Gan, Israel

"Model Checking" is a generic name for methods for automatically checking the compatibility between a model and its formal specification. It is used to verify the correctness of software and hardware systems. The method has been successfully adopted by the hardware and software industry, and provides an automatic exhaustive alternative to software and hardware testing. Model checking usually compares a finite state model of a system (software or hardware against a specification given in some formal notation such as automata or logic.

In this series of lectures we will learn the basic methods and algorithms for model checking and how to use them. We focus on the following topics:

- Modeling of software and hardware systems.
- Software specification using temporal logic and Buchi Automata.
- Translation between logic and automata.
- Model Checking Algorithms.
- How to make it work in practice: abstraction/reduction/BDDs

References

1. E. M. Clarke, O. Grumberg, D. A. Peled. *Model Checking.* MIT Press; 2000.
2. D. Peled. *Software Reliability Methods.* Springer; 2001.
3. C. Baier, J-P. Katoen. *Principles of Model Checking.* MIT Press; 2008.
4. E. A. Emerson, E. M. Clarke. *Using Branching Time Temporal Logic to Synthesize Synchronization Skeletons.* Science of Computer Programming, Vol. 2; pp. 241-266; 1982.
5. J.Queille, J.Sifakis. *Specification and Verification of Concurrent Systems in Caesar.* 5th International Symposium on Programming; LNCS 137; Springer; pp. 337-351; 1981.
6. R. Gerth, D. Peled, M. Vardi, P. Wolper. *Atomatic Simple on-the-fly Automatic Verification of Linear Temporal Logic.* PSTV'95; pp. 3-18; 1995.
7. `http://www.dcs.warwick.ac.uk/∼doron/big.ppt`