Course Document for Topics in Model Checking

Somesh Jha
Computer Sciences Department
University of Wisconsin
Madison, WI 53706.
email: jha@cs.wisc.edu

1 Course Overview

Model checking is a technique for verifying finite state concurrent systems such as sequential circuit designs and communication protocols. It has a number of advantages over traditional approaches that are based on simulation, testing, and deductive reasoning. In particular, model checking is automatic and usually quite fast. Also, if the design contains an error, model checking will produce a counterexample that can be used to pinpoint the source of the error. Model checking has been used successfully in practice to verify real industrial designs, and companies are beginning to market commercial model checkers.

The main challenge in model checking is dealing with the state space explosion problem. This problem occurs in systems with many components that can interact with each other or systems with data structures that can assume many different values. In such cases the number of global states can be enormous. Researchers have made considerable progress on this problem over the last ten years.

We will cover basic topics in model checking, such as temporal logics, model checking algorithms, BDDs, symbolic model checking and automatic-theoretic techniques for model checking. We also cover advanced topics, such as symmetry, abstraction, and verifying real-time and probabilistic systems.

1.1 Book

The required text for this class is given below.

> Edmund M. Clarke, Orna Grumberg and Doron A. Peled, *Model Checking*, MIT Press (January 2000).

I will hand out extra articles and reading material as the class progresses.

2 Grading criteria (Not Finalized)

- **Homeworks (40%):** Homeworks will be assigned during the class.
- **Project (60%):** This will be a significant project related to model checking. Projects can be done in groups of upto two students.