CS 652: Computer Aided Verification

1.Overview

Correctness of the hardware, software and cyber-physical systems is of prime importance to prevent financial loss or loss of life. With the increase in the complexity of the systems, ensuring the correctness of the systems becomes a significant challenge and entails algorithmic methods that can automatically ensure correctness of the systems without manual intervention. This course will discuss the mechanisms for modeling a system and capturing its requirements formally, and algorithms and techniques for verifying the model with respect to its formal specification. The course will also look into various software tools that have been successful in utilizing the algorithmic techniques to solve practical verification problems.

2. Prerequisites

The course does not have any formal prerequisites. The students are expected to have mathematical maturity of the level of an undergraduate degree in engineering. However, some familiarity with finite state machines and graph algorithms, and programming experience will be helpful.

3. Topics

Modeling of Systems: Modeling of concurrent systems, timed systems, hybrid systems and probabilistic systems.
Specification Languages: Linear time properties, regular properties, Linear Temporal Logic (LTL), Computation Tree Logic (CTL), Timed Computation Tree Logic (TCTL), Probabilistic Computational Tree Logic (PCTL)
Techniques for Model Checking: Explicit-State Model Checking, Symbolic Model Checking, Bounded Model Checking, Equivalence and Abstraction, Partial Order Reduction
BDD, SAT and SMT: Binary Decision Diagrams, Satisfiability Solvers, Satisfiability Modulo Theories (SMT) Solvers.
Software Tools: Popular formal methods tools such as Spin, NuSMV, SAL, UPPAAL, SpaceX, Prism, Z3 and CUDD.

4. Lecture & Venue

Wed-Fri 5:00-6:30 PM, KD102

5. Office Hours

Office Hour: Thursday 5:00 pm to 6:00 pm
and by appointment.

6. Evaluation Components & Policies

Assignments - 20%
Project - 30%
Mid-Semester Examination - 20%
End-Semester Examination - 30%

7. Course Policies

No attendance
Honesty Practices and Withdrawal – in accordance with the Institute and DOAA norms.
Anti-cheating policy https://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html

8. References

[BK08] C. Baier and J.-P. Katoen. Principles of Model Checking. The MIT Press, 2008.
[CGP99] E. M. Clarke, Jr., O. Grumberg, and D. A. Peled. Model Checking. MIT Press, 1999.
Research papers assigned by the instructor.

9. Course Webpage

https://www.cse.iitk.ac.in/users/isaha/Courses/cav17.shtml/