IOWA STATE UNIVERSITY
Department of Computer Science

Chuan Jiang

Location: Atanasoff Hall - 213
Time: Wednesday April 17, 2019 1-3
Title: Witness Generation in Existential CTL Model Checking

Abstract

Hardware and software systems are widely used in applications where failure is prohibitively costly or even unacceptable. The main obstacle to make such systems more reliable and capable of more complex and sensitive tasks is our limited ability to design and implement them with sufficiently high degree of confidence in their correctness under all circumstances. As an automated technique that verifies the system early in the design phase, model checking explores the state space of the system exhaustively and rigorously to determine if the system satisfies the specifications and detect fatal errors that may be missed by simulation and testing. One essential advantage of model checking is the capability to generate witnesses and counterexamples. They are simple and straightforward forms to prove an existential specification or falsify a universal specification. Beside enhancing the credibility of the model checker's conclusion, they either strengthen engineers' confidence in the system or provide hints to reveal potential defects.

In this dissertation, we focus on symbolic model checking with specifications expressed in computation tree logic (CTL), which describes branching-time behaviors of the system, and investigate the witness generation techniques for the existential fragment of CTL, i.e., ECTL, covering both decision-diagram-based and SAT-based.

Since witnesses provide important debugging information and may be inspected by engineers, smaller ones are always preferable to ease their interpretation and understanding. To the best of our knowledge, no existing witness generation technique guarantees the minimality for a general ECTL formula with nested existential CTL operators. One contribution of this dissertation is to fill this gap with the minimality guarantee. With the help of the saturation algorithm, our approach computes the minimum witness size for the given ECTL formula in every state, stored as an additive edge-valued multiway decision diagrams (EV+MDD), a variant of the well-known binary decision diagram (BDD), and then builds a minimum witness. Though computationally intensive, this has promising applications in reducing engineers' workload.

SAT-based model checking, in particular, bounded model checking, reduces a model checking problem problem into a satisfiability problem and leverages a SAT solver to solve it. Another contribution of this dissertation is to improve the translation of bounded semantics of ECTL into propositional formulas. By realizing the possibility of path reuse, i.e., a state may build its own witness by reusing its successor's, we may generate a significantly smaller formula, which is often easier for a SAT solver to answer, and thus boost the performance of bounded model checking.