TUTORIAL 2

BOOLEAN SATISFIABILITY SOLVING AND ITS APPLICATION IN EQUIVALENCE AND MODEL CHECKING

Speakers:

Joao Marques-Silva - Technical Univ. of Lisbon, Lisboa, Portugal
Per Bjesse - Prover Tech., Portland, OR
Wolfgang Kunz - Univ. of Frankfurt, Frankfurt, Germany

Background: This tutorial covers the most recent work in Boolean Satisfiability algorithms and its application in two key Design Automation applications: Equivalence Checking and Model Checking. The target audience consists of circuit designers interested in a better understanding of SAT technology, CAD engineers, and academic researchers working on SAT or on applications of SAT.

Description: The first section reviews the basic definitions for Boolean Satisfiability (SAT), surveys the more well-known applications of SAT in Electronic Design Automation (EDA), and introduces basic SAT algorithms and techniques.

The second section addresses state-of-the-art algorithms for SAT, covering the most well-known and used search techniques: non-chronological backtracking, clause recording, randomization, and restarts. Moreover, this section details the techniques recently proposed for fast implementation of SAT solvers. In addition, this section surveys recent research work in SAT, highlighting the techniques that show promise for the near future.

The third section focuses on algorithms and data structures for applying SAT in synthesis and combinational verification. In this application domain, SAT algorithms operate on CNF formulas representing circuits. This can be taken into account by specific heuristics. In this context we also discuss algorithms of automatic test pattern generation (ATPG) and compare them with related SAT algorithms.

The fourth section describes the application of SAT-algorithms in equivalence checking. We give an introduction to state-of-the-art equivalence checking algorithms, and focus on the role of SAT in equivalence checking.

The fifth section focuses on how SAT methods can be used to check properties of sequential circuits. We first demonstrate how to model synchronous gate-level circuits and safety properties. After this, we introduce a technique called bounded model checking. Given a circuit and a safety property, this analysis uses SAT algorithms to search for paths leading to a state where the safety property is violated.

Finally, in the sixth section, we continue our investigation of SAT-based model checking. A troublesome aspect of bounded model checking is that although it excels at finding failures, it is not a practical method for proving that a given system is safe. We therefore demonstrate how bounded model checking can be generalized to SAT-based induction---a complete proof method for safety properties. Finally, we conclude by discussing SAT-based reachability analysis.