SMT Solvers: Foundations and Applications

Nikolaj Bjørner
Microsoft Research, Redmond, USA

Satisfiability Modulo Theories (SMT) solvers are used in many modern program verification, analysis and testing tools. They owe their scale and efficiency thanks to advances in search algorithms underlying modern SAT solvers and first-order theorem provers. They owe their versatility in software development applications thanks to specialized algorithms supporting theories, such as numbers and algebraic data-types, of relevance for software engineering. This lectures introduces algorithmic principles of SMT solving, taking as basis modern SAT solvers and integration with specialized theory solvers and quantifier reasoning. We detail some of the algorithms used for main theories used in current SMT solvers and survey newer theories and approaches to integrating solvers. The lectures also outline some application scenarios where SMT solvers have found use, including program verification, network analysis, symbolic model checking, test-case generation, and white-box fuzzing.

We plan to cover the following topics:

SAT solving basics Elements of modern SAT solvers: Unit propagation, Conflict Directed Clause Learning, Variable heuristics, indexing data-structures, pre- and in-processing.

Theory Combination Techniques Nelson-Oppen combination, Model-based theory combination.

Theories - Algorithms and Integration Arithmetic, Uninterpreted functions, Bit-vectors, arrays, algebraic data-types, strings and sequences, collections.

Quantifier Reasoning E-matching Based Quantfier Instantiation, Model Based Quantifier Instantiation, Quantifier Elimination, Quantifier Satisfiability, Super-position.

Horn Clauses Modulo Theories Top-down, bottom-up search methods, PDR/IC3 solvers for Horn clause, Symbolic Datalog engines.

Introductory Reading

- Boolean Satisfiability: *From Theoretical Hardness to Practical Success*. Sh. Malik, L. Zhang. Communications of the ACM; Vol.52 no.8; 2009.
- Satisfiability Modulo Theories: *Introduction and Applications*. L. de Moura, N. Bjørner. CACM 2011.
  `http://dl.acm.org/citation.cfm?id=1995394`
- Applications of SMT solvers: N. Bjørner, L. de Moura. Notes 2013.
  `http://research.microsoft.com/en-US/people/nbjorner/smt-application-chapter.pdf`
- Horn Clause Solvers for Program Verification: N. Bjørner, A. Gurfinkel, K. McMillan, A. Rybalchenko. 2015.
  `http://research.microsoft.com/en-US/people/nbjorner/yurifest.pdf`

In addition to the suggested introductory reading, participants are welcome to also take a look at other papers including (1) Model-based Theory combination, (2) Efficient Pattern-based quantifier instantiation, (3) Model Based Quantifier Instantiation (there are several papers, including a higher-level overview from IJCAR 2010, and a paper applying model based quantifier instantiation to reason about bit-vectors in FMCAD by Wintersteiger et.al.), (4) Efficient Combinatory Array Logic, (5) Generalized Property Directed Reachability.

Most relevant pointers to reading material is available from:

`http://github.com/z3prover/z3/Documents`