SMT-Based Model Checking

Cesare Tinelli[*]

Department of Computer Science
The University of Iowa
cesare-tinelli@uiowa.edu

It is widely recognized that the field of model checking owes much of its great success and impact to the use of symbolic techniques to reason efficiently about the reachable states of a hardware or software system. Traditionally, these techniques have relied on propositional encodings of transition systems and on propositional reasoning engines such as BDDs and SAT solvers. More recently, a number of these techniques have been adapted, and new ones have been devised, based instead on first-order encodings and reasoners for Satisfiability Modulo Theories (SMT).

SMT is an area of automated deduction that studies methods for checking the satisfiability of first-order formulas with respect to some logical theory T of interest. For being theory-specific and restricting their language to certain classes of formulas (such as quantifier-free formulas), these specialized methods can be implemented in solvers that are in practice more powerful than SAT solvers and more efficient than general-purpose theorem provers. The most sophisticated SMT solvers combine together and integrate in a fast propositional engine several *theory solvers*, decision procedures each focused on checking the satisfiability of conjunctions of literals in a particular theory—such as, for instance, linear integer or rational arithmetic, the theory of equality over uninterpreted function symbols, of bit-vectors, of arrays, and so on.

SMT encodings of model checking problems provide several advantages over propositional encodings. For instance, they are more natural and close to the level of abstraction of the original system; they allow one to model finite-state systems compactly; and they can be used to model infinite-state systems directly, without resorting to finite state abstractions. At the same time, they largely fall within logical fragments that are efficiently decidable.

This talk will highlight a few model checking approaches and techniques based on SMT encodings and relying on SMT solvers as their main reasoning engine. We will see that SMT-based model checking methods blur the line between traditional (propositional) model checking and traditional (first or higher order) deductive verification. More crucially, they combine the best features of both by offering the scalability and scope of deductive verification while maintaining the high level of automation of propositional model checking.

[*] The author's research on this subject is largely the result of past and on-going collaborations with C. Barrett, M. Deters, G. Hagen, P.-L. Garoche, Y. Ge, T. Kahsai, S. Miller, and M. Whalen, and was made possible in part by the support of grant #FA9550-09-1-0517 from the Air Force Office of Scientific Research and grants #1049674 and #0551646 from the National Science Foundation.

A. Goodloe and S. Person (Eds.): NFM 2012, LNCS 7226, p. 1, 2012.