From Incremental Determinization to Synthesis

Markus N. Rabe and Sanjit A. Seshia

University of California, Berkeley
rabe@berkeley.edu

Abstract. We report on a recent fundamentally new idea in 2QBF solving and its applications in synthesis. The new algorithm lifts the solving principles of SAT from the space of assignments to the space of Skolem functions. We present experimental data on the usage of solvers for quantified boolean formulas (QBFs) for different synthesis problems.

1 Introduction

Quantifier alternations are at the heart of many formulations of synthesis problems, such as syntax-guided synthesis [1] and reactive synthesis [3,5,10]. Yet even in the boolean theory, quantifier elimination algorithms often perform unsatisfactory. For example, the formula $\forall X.\exists Y.\ X = Y$, where X and Y are bit-vectors of width 32, cannot be solved in a reasonable time by many of the competitive solvers for quantified boolean formulas (QBF). Even though preprocessors for QBF can solve this problem, this indicates that there is still an problem with the underlying solving principles.

Currently most of the competitive solvers for QBF, such as RAReQS [7], CAQE [9], and Qesto [6], rely on counter-example guided abstraction refinement. In the example above, these algorithms rule out only a single pair of assignments to X and Y in every iteration and thus take unreasonably long to solve this simple instance.

We present the incremental determinization algorithm that can directly derive the unique parts of the Skolem functions for 2QBFs and introduces additional clauses when the Skolem functions are not unique [8]. The algorithm is closely related to the CDCL algorithm for propositional boolean formulas [11]. We lift the concepts of partial assignments, propagation, decisions, conflicts, and conflict analysis from the level of assignments of values to variables to the level of assignments of Skolem functions to variables.

We implemented the algorithm in a prototype we named CADET. The experimental evaluation shows that CADET is faster and more effective than the existing QBF solvers on the 2QBF instances collected in QBFLIB [4]. Finally, we present experimental results for CADET on various benchmarks derived from synthesis problems, such as SyGuS [1] and safety games [2].

References

1. Rajeev Alur, Rastislav Bodik, Garvit Juniwal, Milo MK Martin, Mukund Raghothaman, Sanjit A Seshia, Rishabh Singh, Armando Solar-Lezama, Emina

Torlak, and Abhishek Udupa. Syntax-guided synthesis. *Dependable Software Systems Engineering*, 40:1–25, 2015.

2. Roderick Bloem, Uwe Egly, Patrick Klampfl, Robert Könighofer, and Florian Lonsing. SAT-based methods for circuit synthesis. In *Proceedings of FMCAD*, pages 31–34, 2014.
3. Alonzo Church. Application of recursive arithmetic to the problem of circuit synthesis. In *Summaries of the Summer Institute of Symbolic Logic*, pages 3–50. Cornell University, 1957.
4. E. Giunchiglia, M. Narizzano, L. Pulina, and A. Tacchella. Quantified Boolean Formulas satisfiability library (QBFLIB), 2005. `www.qbflib.org`.
5. Lawrence H. Landweber J. Richard Büchi. Solving sequential conditions by finite-state strategies. *Transactions of the American Mathematical Society*, 138:295–311, 1969.
6. Mikolás Janota and Joao Marques-Silva. Solving QBF by clause selection. In *Proceedings of IJCAI*, pages 325–331. AAAI Press, 2015.
7. Mikolás Janota and João P. Marques Silva. Abstraction-based algorithm for 2QBF. In *Proceedings of SAT*, pages 230–244, 2011.
8. Markus N. Rabe and Sanjit A. Seshia. Incremental determinization. In *Proceedings of SAT (to appear)*, Berlin, Heidelberg, 2016. Springer-Verlag.
9. Markus N Rabe and Leander Tentrup. CAQE: A certifying QBF solver. In *Proceedings of FMCAD*, pages 136–143, 2015.
10. Michael Oser Rabin. *Automata on Infinite Objects and Church's Problem*. American Mathematical Society, Boston, MA, USA, 1972.
11. João P Marques Silva and Karem A Sakallah. GRASP - A new search algorithm for satisfiability. In *Proceedings of CAD*, pages 220–227. IEEE, 1997.