Reachability Analysis with QBF

Armin Biere, biere@jku.at
Institute for Formal Models and Verification
Johannes Kepler Universität, Linz, Austria

One motivation behind bounded model checking (BMC) was to overcome some of the restrictions of reachability analysis based on binary decision diagrams (BDDs). However, in order to be able to replace BDDs by more scalable techniques such as satisfiability solving (SAT), the original formulation of BMC had to sacrifice completeness, at least in practice.

Completeness means being able to verify the correctness of a circuit with respect to a sequential property as opposed to just being able to falsify the property. Even today, with more sophisticated SAT based model checking techniques, such as *k*-induction and interpolation, and better SAT solvers, BDDs are still the prevalent technique for complete automatic verification of sequential properties.

Since model checking of simple safety properties, more specifically checking reachability of certain bad states, is a PSPACE hard problem, it seems to be obvious to solve such verification problems by mapping them to the decision problem for Quantified Boolean Formulae (QBF), which is the standard PSPACE hard problem. In contrast to purely propositional problems, QBF allows quantification over boolean variables.

Beside modelling alternating quantifiers within the logic, QBF can be used to represent verification problems exponentially more succinct. For instance, if a subcircuit is instantiated with two different sets of signals, a flat propositional formulation contains two copies of the subcircuit, while the QBF formulation needs only one. In this way QBF can be used to represent symbolic reachability and hierarchical descriptions exponentially more succinct than their flat propositional expansions.

Efficient QBF solvers are starting to emerge. In 2006 the first QBF competition is organized. The number of benchmarks and solvers is rapidly increasing and it is hoped that QBF will play as an important role as core verification technology as SAT does today. Recently there have been mixed results on the efficiency of using QBF for model checking.

We review different approaches on using QBF for reachability analysis. First, as proposed in the original work on BMC, QBF can be used as termination check for BFS in symbolic reachability analysis. Then, given a circuit, with a bad state monitor, following Savitch's PSPACE proof of hardness of symbolic reachability, there is a QBF formula, quadratic in the size of the circuit, which is valid, if and only if a bad state is reachable. Finally, bottom up elimination of quantifiers in QBF can be used for efficient time frame expansion in BMC.

We discuss relevant QBF solver techniques, and present initial experimental results on applying QBF to symbolic reachability. We strongly believe that many applications not only in circuit verification but also in synthesis can benefit from a reformulation as QBF problem.