Tackling Scalability Issues in Bit-Vector Reasoning

Aina Niemetz
Stanford University
Stanford, CA
niemetz@cs.stanford.edu

***Abstract*—Efficiently reasoning about bit-vector constraints in Satisfiability Modulo Theories (SMT) has been an ongoing challenge for many years. The dominant state-of-the-art approach for solving bit-vector formulas in SMT is bit-blasting, an eager reduction to propositional logic that is typically combined with aggressive simplifications of the input constraints prior to the actual reduction step. Even though this eager reduction may come at the cost of significantly increasing the formula size, it is surprisingly efficient in practice—thanks to state-of-the-art SAT solvers, which are usually able to efficiently deal with complex formulas over millions of variables. This size increase, however, is a potential bottleneck and the main reason why bit-blasting does not generally scale well for increasing bit-widths, especially in the presence of arithmetic operators, which translate to large and complex Boolean circuits on the bit-level.**

To tackle these scalability issues, there are two (orthogonal) avenues to explore: developing alternative approaches that do not (mainly) rely on translations to the SAT level, and improving the scalability of bit-blasting itself. In this talk, we will highlight techniques in each category: a propagation-based local search procedure as an alternative to bit-blasting, which can only determine satisfiability but improves performances over bit-blasting on satisfiable instances, and a CEGAR-style abstraction-refinement procedure that significantly improves the scalability of bit-blasting. We extended the state-of-the-art SMT solver Bitwuzla with both techniques and show that they significantly improve solver performance on a variety of benchmark sets across all logics supported by Bitwuzla, including combinations of bit-vectors with arrays, uninterpreted functions and floating-point arithmetic.

https://doi.org/10.34727/2024/isbn.978-3-85448-065-5_2