

Invited Talk: Local Search for Bit-Precise Reasoning and Beyond

Aina Niemetz

Stanford University, 450 Jane Stanford Way, Stanford, CA, 94305

Abstract

Reasoning about quantifier-free bit-vector constraints in Satisfiability Modulo Theories (SMT) has been an ongoing challenge for many years, especially for large bit-widths. Current state-of-the-art for bit-precise reasoning is a technique called bit-blasting, where bit-vector constraints are eagerly translated into propositional logic (SAT). Bit-blasting is very efficient in practice but does not generally scale well for large bit-widths due to fact that the translation is in general exponential in the size of the input formula, which potentially (and in practice) overwhelms the underlying SAT solver. For these instances, we need alternative approaches for bit-precise reasoning that do not rely on translations to the SAT level. In this talk, I will present such an alternative approach, a propagation-based local search procedure, which relies on propagating target values from top-level constraints towards the inputs while utilizing so-called invertibility conditions. Invertibility conditions precisely characterize when bit-vector constraints are invertible, a core concept of our approach. Our procedure is, as expected for local search, incomplete in the sense that it can only determine satisfiability but was shown to be effective on hard satisfiable instances, in particular in combination with bit-blasting in a sequential portfolio setting. I will talk about the strengths and potential weaknesses of this approach, and how to address these weaknesses. I will further give some insight into how we identified invertibility conditions for bit-vector operators via utilizing syntax-guided synthesis techniques. I will also present more applications of invertibility conditions, even outside of local search bit-vector reasoning. First, we have embedded invertibility conditions into quantifier instantiations in a counterexample-guided procedure for quantified bit-vectors. Second, we have provided invertibility conditions for a majority of operators in the theory of floating-point arithmetic, which will allow us to lift our local search procedure to quantifier-free floating-point reasoning in the future.

SMT'22: 20th International Workshop on Satisfiability Modulo Theories, August 11–12, 2022, Haifa, Israel


✉ niemetz@cs.stanford.edu (A. Niemetz)

🌐 <https://cs.stanford.edu/people/niemetz> (A. Niemetz)

🆔 0000-0003-2600-5283 (A. Niemetz)



© 2022 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)