Challenges in Bit-Precise Reasoning

Armin Biere

Institute for Formal Models and Verification
Johannes Kepler University, Linz, Austria

ABSTRACT OF TUTORIAL TALK

Bit-precise reasoning (BPR) precisely captures the semantics of systems down to each individual bit and thus is essential to many verification and synthesis tasks for both hardware and software systems. As an instance of Satisfiabiliy Modulo Theories (SMT), BPR is in essence about word-level decision procedures for the theory of bit-vectors. In practice, quantiers and other theory extensions, such as reasoning about arrays, are important too. In the first part of the tutorial we gave a brief overview on basic techniques for bit-precise reasoning and then covered more recent theoretical results, including complexity classification results. We discussed challenges in developing an efficient SMT solver for bit-vectors, like our award winning SMT solver Boolector, and in particular presented examples, for which current techniques fail. Finally, we reviewed the state-of-the-art in word-level model checking, and argued why it is necessary to put more effort in this direction of research.