Restricted Quantification in Bit-Vector Problems*

Gergely Kovásznai[a]

[a]Vienna University of Technology
kova@forsyte.tuwien.ac.at

Abstract

Solving quantified bit-vector formulas containing uninterpreted functions (UFBV) is a difficult decision problem, being 2-NExpTime-complete [2]. Nevertheless, it is considered to be one of the "holy grails" in software (and hardware) verification, since UFBV provides a very natural formalism for expressing, e.g., program invariants, ranking functions, arrays, etc. There exists a common attempt to simplify this complex decision problem by restricting the way of quantification in UFBV. In this paper we investigate the complexity of two such fragments.

The SMT-LIB standard supports the usage of non-recursive macros, which actually involve a restricted way of quantification. In previous work [3] we showed that, by allowing only this kind of quantification in bit-vector formulas, the complexity drops to NExpTime-complete.

Since recursion is essential in formalizing several verification problems, one can also try to allow a restricted form of recursion in macro definitions, similar to [1], where macro definitions are Horn clauses. In this paper we show that using macros that implement monotone fixed point formulas (i.e., a generalization of Horn clauses) results in an ExpSpace-complete fragment. The proof gives a reduction to symbolic word-level model checking.

References

[1] N. Bjorner, K. McMillan, and A. Rybalchenko. Program verification as satisfiability modulo theories. In *Proc. SMT'12*, pages 3–11, 2012.

[2] G. Kovásznai, A. Fröhlich, and A. Biere. On the complexity of fixed-size bit-vector logics with binary encoded bit-width. In *Proc. SMT'12*, pages 44–55, 2012.

[3] G. Kovásznai, A. Fröhlich, and A. Biere. Complexity of fixed-size bit-vector logics. *Theory of Computing Systems*, 2013. Submitted, review in progress.

*Supported by the NFN grant S11403-N23 (RiSE) of the Austrian Science Fund (FWF) and by the grant ICT10-050 (PROSEED) of the Vienna Science and Technology Fund (WWTF).