Bit-Blasting for SMT-NIA with AProVE*

Karsten Behrmann[1], Andrej Dyck[1], Fabian Emmes[1], Carsten Fuhs[2], Jürgen Giesl[1], Patrick Kabasci[1], Peter Schneider-Kamp[3], René Thiemann[4]

[1] RWTH Aachen University, Germany
[2] University College London, United Kingdom
[3] University of Southern Denmark, Denmark
[4] University of Innsbruck, Austria

In automated termination provers like our tool AProVE [4], often the need arises to solve Boolean combinations of constraints in non-linear (integer) arithmetic to perform a proof step for a successful termination proof. Examples for prominent termination techniques where this is the case are well-founded orders based on polynomial [3] or matrix interpretations [2]. In order to facilitate this task, AProVE features a dedicated SMT-solver for SMT-NIA. The approach we are using at SMT-COMP for the QF_NIA category is based on a reduction to a SAT problem (see [3] for details) and a subsequent invocation of the SAT solver MiniSAT[1]. This kind of approach is commonly known as *bit-blasting*.

Since satisfiability of SMT-NIA is undecidable in general, we search for solutions from a finite domain for the variables in the SMT-NIA instances. In case a satisfying assignment is found by the SAT solver, we return the corresponding integer solution. If the SAT solver detects unsatisfiability of the generated SAT instance, we know that there is no solution for the SMT-NIA instance with the used domain, and we restart the search with an extended domain. In this way, we obtain a semi-decision procedure for SMT-NIA. We additionally use information from global constraints (i.e., atomic top-level assertions like $x \geqslant 42$) of the SMT-NIA instance to bound the search space for certain variables.

References

1. N. Eén and N. Sörensson. An extensible SAT-solver. In *Proc. SAT 2003*, volume 2919 of *LNCS*, pages 502–518, 2004.
2. J. Endrullis, J. Waldmann, and H. Zantema. Matrix interpretations for proving termination of term rewriting. *Journal of Automated Reasoning*, 40(2-3):195–220, 2008.
3. C. Fuhs, J. Giesl, A. Middeldorp, R. Thiemann, P. Schneider-Kamp, and H. Zankl. SAT solving for termination analysis with polynomial interpretations. In *Proc. SAT 2007*, volume 4501 of *LNCS*, pages 340–354, 2007.
4. J. Giesl, M. Brockschmidt, F. Emmes, F. Frohn, C. Fuhs, C. Otto, M. Plücker, P. Schneider-Kamp, T. Ströder, S. Swiderski, and R. Thiemann. Proving termination of programs automatically with AProVE. In *Proc. IJCAR 2014*, LNAI, 2014. To appear. See also http://aprove.informatik.rwth-aachen.de.

---

* System description for *SMT-COMP 2014*.