SMT-RAT 2.0

June 12, 2015

SMT-RAT is an open-source C++ toolbox for strategic and parallel SMT solving consisting of a collection of SMT compliant implementations of methods for solving quantifier-free (non)linear real and integer arithmetic as well as the logics of bit-vectors and uninterpreted functions. A more detailed description of SMT-RAT can be found at https://github.com/smtrat/smtrat/wiki.

Main solving procedures The SAT solving within SMT-RAT takes place in an adaption of the SAT solver minisat [3] and we use it for SMT solving in a less-lazy fashion [7].

The main focus of SMT-RAT is nonlinear arithmetic. For the linear constraints we use the Simplex method equipped with (currently very naively implemented) branch-and-bound and cutting-plane procedures as presented in [2]. For the nonlinear constraints SMT-RAT uses Gröbner bases [5], virtual substitution [1] and the cylindrical algebraic decomposition [6]. Moreover, it uses interval constraint propagation similar as presented in [4], lifting splitting decisions and contraction lemmas to the SAT solving and aided by the aforementioned approaches for nonlinear constraints in case it cannot determine whether a box contains a solution or not. Furthermore, we apply some naive preprocessing, (1) using factorizations and sum-of-square decompositions of polynomials to simplify them and (2) applying substitutions gained by constraints being equations. We also normalize and simplify formulas if it is obvious.

Our current implementation for the logic of uninterpreted functions is the result of a practical course within the winter term 2014/2015. The theory solver as well as the preprocessing techniques for this logic have been implemented and optimized solely by four master students that are listed below.

To broaden the scope of SMT-RAT and demonstrate its expandability to other logics, we offered a master thesis to implement a decision procedure for bit-vector logic. Our current implementation for this logic was solely written by the master student listed below.

Authors

- Erika Ábrahám
- Florian Corzilius
- Gereon Kremer
- Sebastian Junges
- Stefan Schupp
- Phillip Keldenich (uninterpreted functions)
- Oliver Major (uninterpreted functions)
- Sascha Müller (uninterpreted functions)
- Daniel Neuen (uninterpreted functions)
- Andreas Krüger (bit-vector)

References

[1] F. Corzilius and E. Ábrahám. Virtual substitution for SMT solving. In *Proc. of FCT'11*, volume 6914 of *LNCS*, pages 360–371. Springer, 2011.

[2] B. Dutertre and L. de Moura. A fast linear-arithmetic solver for DPLL(T). In *Proc. of CAV'06*, volume 4144 of *LNCS*, pages 81–94. Springer, 2006.

[3] N. Eén and N. Sörensson. An extensible sat-solver. In *Proc. of SAT'03*, volume 2919 of *LNCS*, pages 502–518. Springer, 2004.

[4] S. Gao, M. K. Ganai, F. Ivancic, A. Gupta, S. Sankaranarayanan, and E. M. Clarke. Integrating ICP and LRA solvers for deciding nonlinear real arithmetic problems. In *Proc. of FMCAD'10*, pages 81–89. IEEE, 2010.

[5] S. Junges, U. Loup, F. Corzilius, and E. Ábrahám. On Gröbner bases in the context of satisfiability-modulo-theories solving over the real numbers. Technical Report AIB-2013-08, RWTH Aachen University, 2013.

[6] U. Loup, K. Scheibler, F. Corzilius, Erika E. Ábrahám, and Bernd Becker. A symbiosis of interval constraint propagation and cylindrical algebraic decomposition. In *Proc. of CADE-24*, volume 7898 of *LNCS*, pages 193–207. Springer, 2013.

[7] Roberto Sebastiani. Lazy Satisfiability Modulo Theories. *Journal on Satisfiability, Boolean Modeling and Computation*, 3:141–224, 2007.