SMT-RAT 2.2

June 8, 2018

SMT-RAT [2] 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 first-order formulas with a focus on nonlinear real and integer arithmetic. Further supported theories include linear real and integer arithmetic, difference logic, bit-vectors and pseudo-Boolean constraints. A more detailed description of SMT-RAT can be found at https://github.com/smtrat/smtrat/wiki. There will be two versions of SMT-RAT that employ different strategies that we call SMT-RAT and SMT-RAT-MCSAT.

SMT-RAT focuses on nonlinear arithmetic. As core theory solving modules, it employs interval constraint propagation (ICP) as presented in [5], virtual substitution (VS) [1] and the cylindrical algebraic decomposition (CAD) [9]. For ICP, lifting splitting decisions and contraction lemmas to the SAT solving and aided by the other approaches for nonlinear constraints in case it cannot determine whether a box contains a solution or not. For nonlinear integer problems, we employ bit blasting up to some fixed number of bits [8] and use branch-and-bound [7] afterwards. The SAT solving takes place in an adaption of the SAT solver minisat [4] and we use it for SMT solving in a less-lazy fashion [10].

For linear inputs we use the Simplex method equipped with branch-and-bound and cutting-plane procedures as presented in [3]. Furthermore, we apply several preprocessing techniques, e.g., using factorizations to simplify constraints, applying substitutions gained by constraints being equations or breaking symmetries. We also normalize and simplify formulas if it is obvious.

SMT-RAT-MCSAT uses our preliminary implementation of the MCSAT framework [6], equipped with an NLSAT-style CAD-based explanation function, enhanced with a simpler explanation function based on Fourier-Motzkin variable elimination. Further extensions, for example a VS-based explanation or a OneCellCAD-based explanation are being worked on, but not yet ready. The general MCSAT framework is integrated in our adapted minisat [4] solver, but is not optimized yet. For example, explanations are still generated eagerly and always added to the clause database which is presumably inferior to the version described in the original MCSAT approach and almost no work has been invested in finding a good variable ordering yet.

Authors

- Erika Ábrahám
- Gereon Kremer
- Rebecca Haehn
- Florian Corzilius
- Sebastian Junges
- Stefan Schupp
- Andreas Krüger
- Christopher Lösbrock

References

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

[2] Florian Corzilius, Gereon Kremer, Sebastian Junges, Stefan Schupp, and Erika Ábrahám. SMT-RAT: An Open Source C++ Toolbox for Strategic and Parallel SMT Solving. In *Proc. of SAT'15*, pages 360–368. Springer, 2015.

[3] 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.

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

[5] 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.

[6] D. Jovanović and L. de Moura. Solving non-linear arithmetic. In *Proc. of IJCAR'12*, volume 7364 of *LNAI*, pages 339–354. Springer, 2012.

[7] Gereon Kremer, Florian Corzilius, and Erika Ábrahám. A Generalised Branch-and-Bound Approach and Its Application in SAT Modulo Nonlinear Integer Arithmetic. In *Proc. of CASC'16*, pages 315–335. Springer, 2016.

[8] Andreas Krüger. Bitvectors in SMT-RAT and their application to integer arithmetics. Master's thesis, RWTH Aachen University, 2015.

[9] 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.

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