SMT-RAT 21.05

June 10, 2021

SMT-RAT [3] 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 non-linear 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://smtrat.github.io/. There will be two versions of SMT-RAT that employ different approaches that we call SMT-RAT and SMT-RAT-MCSAT.

SMT-RAT focuses on non-linear arithmetic.

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. For non-linear integer problems, we employ bit blasting up to some fixed number of bits [11] as preprocessing and use branch-and-bound [10] afterwards.

The SAT solving takes place in the SAT solver minisat [6] which we adapted for SMT solving in a less-lazy fashion [13].

For solving non-linear real arithmetic, as core theory solving modules, we employ several incomplete but efficient methods, namely subtropical satisfiability [7], interval constraint propagation (ICP) as presented in [8] and virtual substitution (VS) [2] which are called in this order before the computationally heavy cylindrical algebraic decomposition (CAD) [12] method is called. The ICP lifts splitting decisions and contraction lemmas to the SAT solver and relies on the methods called subsequently in case it cannot determine whether a box contains a solution or not.

For linear arithmetic, we do not employ the methods used for non-linear inputs, instead we use the Simplex method equipped with branch-and-bound and cutting-plane procedures as presented in [5].

SMT-RAT-MCSAT uses our implementation of the MCSAT framework [4]. As for less-lazy SMT solving, we employ incomplete methods to handle simpler problem classes more efficiently. Thus, our implementation is equipped with multiple explanation backends based on Fourier-Motzkin variable elimination, interval constraint propagation, virtual substitution as in [14], a novel level-wise variant (not published yet) of the one-cell CAD [1] and NLSAT-style model-based CAD projections [9], which are called in this order. The general MCSAT framework is integrated in our adapted minisat [6] solver, but is not particularly optimized yet.

Current authors Jasper Nalbach, Erika Ábrahám, Philippe Specht (Theory of Hybrid Systems Group, RWTH Aachen University).

Previous contributions by current and former group members Gereon Kremer (currently at Stanford University), Florian Corzilius, Rebecca Haehn, Sebastian Junges, Stefan Schupp (currently at TU Wien).

References

[1] Christopher W Brown and Marek Košta. Constructing a single cell in cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 70:14–48, 2015.

[2] Florian Corzilius and Erika Ábrahám. Virtual substitution for SMT solving. In *Proceedings of FCT 2011*, pages 360–371.

[3] 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 *Proceedings of SAT 2015*, pages 360–368.

[4] Leonardo de Moura and Dejan Jovanović. A model-constructing satisfiability calculus. In *Proceedings of VMCAI 2013*, pages 1–12.

[5] B. Dutertre and L. de Moura. A fast linear-arithmetic solver for DPLL(T). In *Proceedings of CAV 2006*, volume 4144, pages 81–94.

[6] Niklas Eén and Niklas Sörensson. An extensible SAT-solver. In *Proceedings of SAT 2013*, pages 502–518.

[7] Pascal Fontaine, Mizuhito Ogawa, Thomas Sturm, and Xuan Tung Vu. Subtropical satisfiability. In Clare Dixon and Marcelo Finger, editors, *Frontiers of Combining Systems*, pages 189–206, Cham, 2017. Springer International Publishing.

[8] 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 *Proceedings of FMCAD 2010*, pages 81–89.

[9] Dejan Jovanović and Leonardo De Moura. Solving non-linear arithmetic. In *International Joint Conference on Automated Reasoning*, pages 339–354. Springer, 2012.

[10] Gereon Kremer, Florian Corzilius, and Erika Ábrahám. A generalised branch-and-bound approach and its application in SAT modulo nonlinear integer arithmetic. In *Proceedings of CASC 2016*, pages 315–335.

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

[12] Ulrich Loup, Karsten Scheibler, Florian Corzilius, Erika Ábrahám, and Bernd Becker. A symbiosis of interval constraint propagation and cylindrical algebraic decomposition. *Automated Deduction – CADE-24*, pages 193–207, 2013.

[13] Roberto Sebastiani. Lazy satisfiability modulo theories. *Journal on Satisfiability, Boolean Modeling and Computation*, 3:141–224, 2007.

[14] Erika Ábrahám, Jasper Nalbach, and Gereon Kremer. Embedding the virtual substitution method in the model constructing satisfiability calculus framework. In *Proceedings of SC^2 2017 at ISSAC*, volume 1974 of *CEUR Workshop Proceedings*.