SMT-RAT 20.04

April 30, 2020

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://smtrat.github.io/. There will be two versions of SMT-RAT that employ different strategies that we call SMT-RAT, SMT-RAT-MCSAT and SMT-RAT-CDCAC.

SMT-RAT focuses on non-linear arithmetic. As core theory solving modules, it employs interval constraint propagation (ICP) as presented in [6], virtual substitution (VS) [1] and the cylindrical algebraic decomposition (CAD) [10]. For ICP, lifting splitting decisions and contraction lemmas to the SAT solving and aided by the other approaches for non-linear constraints in case it cannot determine whether a box contains a solution or not. For non-linear integer problems, we employ bit blasting up to some fixed number of bits [9] and use branch-and-bound [8] afterwards. The SAT solving takes place in an adaption of the SAT solver minisat [5] and we use it for SMT solving in a less-lazy fashion [12].

For linear inputs we use the Simplex method equipped with branch-and-bound and cutting-plane procedures as presented in [4]. 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 implementation of the MCSAT framework [3] that is still being worked on. It is equipped with multiple explanation backends based on the following: NLSAT-style CAD-based; Fourier-Motzkin variable elimination; Virtual substitution as in [14]; OneCell CAD as in [11]; Interval Constraint Propagation. The general MCSAT framework is integrated in our adapted minisat [5] solver, but is not particularly optimized yet. The latest addition has been making the variable ordering fully dynamic as suggested in [7].

SMT-RAT-CDCAC contains a straight-forward not-yet optimized implementation of a novel method based on cylindrical algebraic coverings as described in [13] for NRA solving. Except that the CAD module is replaced by the covering-based method, this solver is identical to SMT-RAT for solving non-linear real arithmetic.

Authors Erika Ábrahám[1], Gereon Kremer[3], Jasper Nalbach[1], Rebecca Haehn[1], Florian Corzilius[2], Sebastian Junges[4], Stefan Schupp[1].
[1] Theory of Hybrid Systems Group, RWTH Aachen University
[2] Former members of THS group
[3] Stanford University
[4] Learn and Verify Group, UC Berkeley

References

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

[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 *Proceedings of SAT 2015*, volume 9340 of *LNCS*, pages 360–368.

[3] Leonardo de Moura and Dejan Jovanović. A model-constructing satisfiability calculus. In *Proceedings of VMCAI 2013*, volume 7737 of *LNCS*, pages 1–12.

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

[5] Niklas Eén and Niklas Sörensson. An extensible sat-solver. In *Proceedings of SAT 2013*, volume 2919 of *LNCS*, pages 502–518.

[6] 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.

[7] Dejan Jovanović, Clark Barrett, and Leonardo de Moura. The design and implementation of the model constructing satisfiability calculus. In *Proceedings of FMCAD 2013*, pages 173–180.

[8] 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*, volume 9890 of *LNCS*, pages 315–335.

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

[10] 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*, 2013.

[11] Malte Neuß. Implementation of onecell cad for nonlinear explanations. Master's thesis, RWTH Aachen University, 2018.

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

[13] Erika Ábrahám, James Davenport, Matthew England, and Gereon Kremer. Deciding the Consistency of Non-Linear Real Arithmetic Constraints with a Conflict Driven Search Using Cylindrical Algebraic Coverings. *Journal of Logical and Algebraic Methods in Programming*.

[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*.