Reasoning about Quantifiers in SMT: The QSMA algorithm

Maria Paola Bonacina
Università degli Studi di Verona
Verona, Italy
mariapaola.bonacina@univr.it

Abstract—Automated reasoning is a key enabling technology for formal methods. Automated theorem provers (ATP) for first-order and lately higher-order logic and solvers for satisfiability modulo theories (SMT) showcase impressive power and amazing sophistication. However, ATP systems reason well about formulas with arbitrary quantification and free symbols, while SMT solvers reason well about ground formulas with defined symbols. Since formulas from applications involve both quantifiers and defined symbols, a hiatus remains open. QSMA is a new algorithm for quantifiers in SMT [4]. QSMA stands for Quantified Satisfiability Modulo theory and Assignment. Currently, QSMA works for one theory with a unique intended model, so that models differ only in the assignment of values to variables. QSMA accepts arbitrary formulas, viewing all quantifiers as existential by double negation. Since QSMA operates a recursive descent over the tree structure of the formula, peeling off quantifiers and instantiating variables, each call works modulo an assignment. By building under- and over- approximations of the formula, QSMA zooms in on a model or finds that none exists. The implementation of QSMA in the YicesQS solver [6] built on top of the Yices 2 solver [5] exhibited excellent performances in linear rational arithmetic and nonlinear arithmetic [4]. Integrating QSMA in the CDSAT framework for conflict-driven satisfiability in a union of theories [1]–[3] is the next challenge.

REFERENCES

[1] Maria Paola Bonacina, Stéphane Graham-Lengrand, and Natarajan Shankar. Conflict-driven satisfiability for theory combination: transition system and completeness. *J. Autom. Reason.*, 64(3):579–609, March 2020.

[2] Maria Paola Bonacina, Stéphane Graham-Lengrand, and Natarajan Shankar. CDSAT for nondisjoint theories with shared predicates: arrays with abstract length. In Antti Hyvärinen and David Déharbe, editors, *Proc. SMT-20*, volume 3185 of *CEUR Proceedings*, pages 18–37. CEUR WS-org, August 2022.

[3] Maria Paola Bonacina, Stéphane Graham-Lengrand, and Natarajan Shankar. Conflict-driven satisfiability for theory combination: lemmas, modules, and proofs. *J. Autom. Reason.*, 66(1):43–91, February 2022.

[4] Maria Paola Bonacina, Stéphane Graham-Lengrand, and Christophe Vauthier. QSMA: a new algorithm for quantified satisfiability modulo theory and assignment. In Brigitte Pientka and Cesare Tinelli, editors, *Proceedings of the 29th International Conference on Automated Deduction (CADE)*, volume 14132 of *Lecture Notes in Artificial Intelligence*, pages 78–95. Springer, 2023.

[5] Bruno Dutertre. Yices 2.2. In Armin Biere and Roderick Bloem, editors, *Proceedings of the 26th International Conference on Computer Aided Verification (CAV)*, volume 8559 of *Lecture Notes in Computer Science*, pages 737–744. Springer, 2014.

[6] Stéphane Graham-Lengrand. The yicesQS solver web page. https://github.com/disteph/yicesQS, 2023. Last seen on September 14, 2023.