Q3B in SMT Competition 2023

Martin Jonáš
Masaryk University
Czechia

Jan Strejček
Masaryk University
Czechia

Jakub Szymsza
Masaryk University
Czechia

1 Solver Description

Q3B is an SMT solver developed at Masaryk University by M. Jonáš. The solver is focused on quantified formulas in the theory of fixed-size bit-vectors and follows a BDD-based approach to SMT introduced in the paper Solving Quantified Bit-Vector Formulas Using Binary Decision Diagrams [4].

Besides the direct translation of the input formula to the corresponding BDD, the approach consists of three additional techniques that make it efficient: (1) aggressive formula preprocessing, including simplifications of quantified formulas that contain unconstrained variables [2], (2) formula approximations that allow representing some of the variables by fewer bits than their full bit-width, and (3) abstractions [1] that allow computing only several bits of the results of expensive bit-vector operations such as multiplication.

The current version of Q3B is written in C++17, uses a parser generated by ANTLR to parse the input formula from the SMT-LIB format, and uses the API of the SMT solver Z3 [5] for an internal formula representation and to perform some of the preprocessing steps. However, Q3B does not classify as a wrapper solver, as it does not use any actual SAT or SMT-solving capabilities of Z3. The operations on BDDs are implemented using the library CUDD [7] and the library by P. Navrátil [6] that implements bit-vector operations on top of CUDD. This library has been extended by the authors of this paper to support abstractions of bit-vector operations. The solving approach used by Q3B and its architecture is described in detail in the corresponding tool paper [3].

2 Changes Since SMT-COMP 2022

Q3B has not been actively developed since 2019. Therefore, the current submission implements no new solving techniques or other algorithmic improvements or heuristics. The only difference with respect to the SMT-COMP 2022 submission is that several bugs have been fixed, BDD reordering heuristics have been tweaked, and the code has been updated to work with current versions of ANTLR and Z3.

3 Availability

The solver is open-source, available under MIT license, and can be downloaded from GitHub: `https://github.com/martinjonas/Q3B/`

References

[1] Martin Jonáš and Jan Strejček. "Abstraction of Bit-Vector Operations for BDD-Based SMT Solvers". In: *Theoretical Aspects of Computing - ICTAC 2018 - 15th International Colloquium, Stellenbosch, South Africa, October 16-19, 2018, Proceedings.* 2018, pp. 273–291. DOI: 10.1007/978-3-030-02508-3_15. URL: https://doi.org/10.1007/978-3-030-02508-3_15.

[2] Martin Jonáš and Jan Strejček. "On Simplification of Formulas with Unconstrained Variables and Quantifiers". In: *Theory and Applications of Satisfiability Testing - SAT 2017 - 20th International Conference, Melbourne, VIC, Australia, August 28 - September 1, 2017, Proceedings.* 2017, pp. 364–379. DOI: 10.1007/978-3-319-66263-3_23. URL: https://doi.org/10.1007/978-3-319-66263-3_23.

[3] Martin Jonáš and Jan Strejček. "Q3B: An Efficient BDD-based SMT Solver for Quantified Bit-Vectors". In: *Computer Aided Verification - 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part II.* 2019, pp. 64–73. DOI: 10.1007/978-3-030-25543-5_4. URL: https://doi.org/10.1007/978-3-030-25543-5_4.

[4] Martin Jonáš and Jan Strejček. "Solving Quantified Bit-Vector Formulas Using Binary Decision Diagrams". In: *Theory and Applications of Satisfiability Testing – SAT 2016 – 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings.* 2016, pp. 267–283. DOI: 10.1007/978-3-319-40970-2_17. URL: https://doi.org/10.1007/978-3-319-40970-2_17.

[5] Leonardo Mendonça de Moura and Nikolaj S. Bjørner. "Z3: An Efficient SMT Solver". In: *Tools and Algorithms for the Construction and Analysis of Systems, 14th International Conference, TACAS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008. Proceedings.* Ed. by C. R. Ramakrishnan and Jakob Rehof. Vol. 4963. Lecture Notes in Computer Science. Springer, 2008, pp. 337–340. DOI: 10.1007/978-3-540-78800-3_24. URL: https://doi.org/10.1007/978-3-540-78800-3%5C_24.

[6] Peter Navrátil. *Adding Support for Bit-Vectors to BDD Libraries CUDD and Sylvan.* Bachelor Thesis. 2018. URL: https://is.muni.cz/th/lij5a/.

[7] Fabio Somenzi. "CUDD: CU decision diagram package release 3.0.0". In: *University of Colorado at Boulder* (2015).