Master Thesis Proposal

Certified Circuit Reconstruction for QBF

Student: Mihai-Alexandru Weng
Advisor: Dr. Friedrich Slivovsky

January 9, 2024

Contents

1 Motivation & Problem Statement

Given the success of SAT solvers, and its applications, we can go one step further and generalize the algorithms for the quantified version of boolean formulas, [2]. The problems' domain for the QBF version are founded in PSPACE class, whilst SAT problems are in NP class. QBFs can encode applications ranging from verification, model checking, to Artificial intelligence, games strategies, [8].

The current methods and tools used in certifying proofs revolve around usage of a trusted program (usually proved with formal methods). This program often introduce a custom proof format that facilitate the code running, [4], [3].

Translation of CNF to non-CNF format, [6], leaves room for improvement by trying to validate formally din transformation.

2 Aim of the Work

The objective of the thesis is to introduce an additional way of generating a QRAT proof for a given QBF in QDIMACS format, using its circuit translation.
In this way, we can achieve extra assurance for the circuit translation by checking the produce proof can also solve the input before translation. And also, utilize the favorable input for the QBF solver, based on empirical result [6], a circuit based format.

3 Methodological Approach

1. Better understanding of the tools involved in the process.
2. Devise test samples for checking various edge cases.
3. Automate the workflow.
4. Modify a QCIR QBF (QCDCL) solver to output the CNF encoding.
5. Implement conversion from Q-resolution proof to QRAT.
6. Implement a program for getting a (Q)RAT derivation of the CNF encoding using a SAT solver.
7. Verify against the test sample.
8. Using common benchmarks for testing.

4 Structure of the Work

1. Introduction
2. Preliminaries
   (a) Q-resolution proof
   (b) QRAT proof
   (c) QBF input formats (CNF / non-CNF)
3. Extension of circuit based solver
4. QRAT proof for QDIMACS from QCIR
5. Testing
6. Conclusion

5 State-of-the-Art

In [7], it is raised the problem that simple Tseitin translation can be harmful to the QBF, a CNF QBF solver could take exponential time for a trivial input before the translation. Thus, in the previous work, a tool for transforming a QDIMACS into circuit form is developed. Also, in [6] testing the circuit format, QCIR [1], is noted the direction of the ongoing research for non-CNF solvers in improving the translation and certification. In plus, we can see an interest in developing those solvers for circuits format for competition. This way, it can open the possibility for combining the best of both worlds solvers, CNF and non-CNF, [5].

6 Relevance to the Curricula of Logic and Computation

The topic of certifying proof, in development of validation tools for boolean formulas, touches many areas covered in the Logic and Computation syllabus. Those branches are: algorithms and data structures, logic, formal verification, complexity. Courses relevant to the thesis' content are:

- 186.814 Algorithmics
- 186.182 Seminar on Algorithms
- 184.090 SAT Solving
- 181.145 Computer Aided Verification
- 185.291 Formal Methods in Computer Science
- 185.A45 Logic and Computability
- 184.068 Artificial Intelligence Seminar

References

[1] QCIR-G14: A Non-Prenex Non-CNF Format for Quantified Boolean Formulas. *QBF Gallery 2014*.

[2] Olaf Beyersdorff, Mikoláš Janota, Florian Lonsing, and Martina Seidl. Chapter 31. Quantified Boolean Formulas. In Armin Biere, Marijn Heule, Hans Van Maaren, and Toby Walsh, editors, *Frontiers in Artificial Intelligence and Applications*. IOS Press, February 2021.

[3] Randal E Bryant, Wojciech Nawrocki, Jeremy Avigad, and Marijn J H Heule. Certified Knowledge Compilation with Application to Verified Model Counting. 2023.

[4] Luís Cruz-Filipe, Marijn J. H. Heule, Warren A. Hunt, Matt Kaufmann, and Peter Schneider-Kamp. Efficient Certified RAT Verification. In Leonardo De Moura, editor, *Automated Deduction – CADE 26*, volume 10395, pages 220–236. Springer International Publishing, Cham, 2017. Series Title: Lecture Notes in Computer Science.

[5] Mikoláš Janota. Circuit-Based Search Space Pruning in QBF. In Olaf Beyersdorff and Christoph M. Wintersteiger, editors, *Theory and Applications of Satisfiability Testing – SAT 2018*, volume 10929, pages 187–198. Springer International Publishing, Cham, 2018. Series Title: Lecture Notes in Computer Science.

[6] Charles Jordan, Will Klieber, and Martina Seidl. Non-CNF QBF Solving with QCIR.

[7] William Klieber. Formal Verification Using Quantified Boolean Formulas (QBF).

[8] Ankit Shukla, Armin Biere, Luca Pulina, and Martina Seidl. A Survey on Applications of Quantified Boolean Formulas. In *2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI)*, pages 78–84, Portland, OR, USA, November 2019. IEEE.