EasyChair Preprint

№ 361

Towards the Semantics of QBF Clauses

Martin Suda

July 20, 2018

Towards the Semantics of QBF Clauses*

Martin Suda

TU Wien, Vienna, Austria

Extended Abstract

The ongoing interest in the problem of Quantified Boolean Formulas (QBF) has resulted in numerous solving techniques, e.g. [22, 19, 12, 23, 13], as well as various resolution-based, clausal calculi [21, 29, 3, 20, 7] which advance our understanding of the techniques and formalise the involved reasoning.

While a substantial progress in terms of understanding these calculi has already been made on the front of proof complexity [3, 20, 7–9, 5, 10, 15, 26, 18, 17], the question of semantics of the involved intermediate clauses has until now received comparatively less attention. In many cases, the semantics is left only implicit, determined by the way in which the clauses are allowed to interact via inferences. This is in stark contrast with propositional or first-order logic, in which a clause can always be identified with the set of its models.

In my talk, I would like to expand on why I find this situation unsatisfying, give examples of what I thought a uniform underlying semantics of QBF clauses *could* be, and, as a teaser for our talk at SAT, briefly explain what I and Bernhard Gleiss finally identified as a viable candidate [28].

The Mystery of QBF Tautologies. One hint that something is not quite right in the way we understand QBF clauses can be demonstrated on the treatment of tautologies. A tautology is a clause which contains both a literal and its complement. While in the setting of propositional and first-order logic tautologies are *harmless* (in the sense that they are always vacuously satisfied and thus can be safely added or discarded), in the study of resolution-based calculi for QBF we encounter tautologies which can be *harmful* (generation of tautologies is explicitly prohibited in Q-Res [21], because they would make the calculus unsound), but also *useful* (the long-distance resolution calculus LD-Q-Res [30, 1] gains exponential power over Q-Res by allowing generation of certain tautologies). How does one resolve this discrepancy? Shouldn't we give up on treating a QBF clause as a disjunction of its literals?

Semantics and Soundness. One of most important properties of a calculus is its soundness and one of the most common methods for showing soundness is relating the inferences of the calculus and the semantics of the manipulated clauses by a notion of logical *entailment*. We know how to show soundness of

* This work was supported by ERC Starting Grant 2014 SYMCAR 639270 and the Austrian research projects FWF S11403-N23 and S11409-N23.

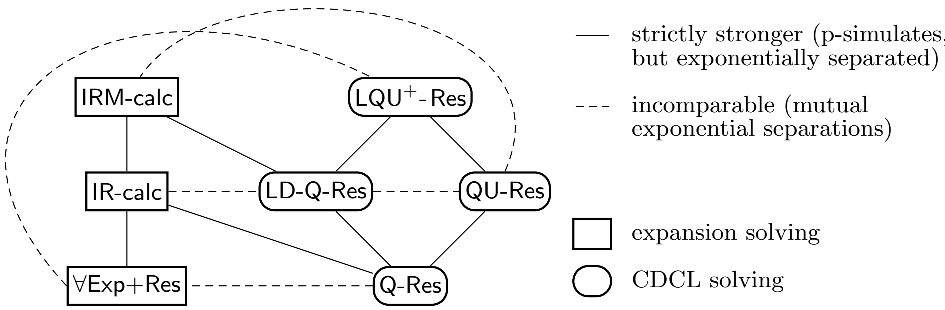

Fig. 1. QBF resolution calculi [8] and their simulation order.

Q-Res using semantical methods [24, 27] and I will argue that this technique is getting implicitly extended to LD-Q-Res via the notion of a *shadow clause* [4] introduced for the purpose of strategy extraction [2].

A different notion of semantics can be provided to the expansion-derived calculi ∀Exp+Res [20] and IR-calc [6] via a translation from QBF to first-order logic [25], and so soundness of these calculi can be established with the help of first-order model theory [16, 11]. Extending this approach to accommodate IRM-calc [6], a calculus which unifies the instantiation flavour inherent to the expansion-derived calculi with the essence of long-distance steps coming from LD-Q-Res (see Fig. 1), was one of the focal points behind this work. I will report on the challenges and lessons the most direct route in this direction provides.

But why should we actually be so interested in semantic methods for showing soundness? The main reasons is that the corresponding argument can be structured *modularly*, treating each inferences rule in separation and concluding by trivial induction along the refutation: "Since every conclusion of a rule is entailed by its premises and since the empty clause cannot have a model, the input axioms cannot have a model either." In this sense, a semantic method enables the notion of a *sound inference*, an inference that can be added to a calculus without affecting its soundness. In contrast, the currently known proof of soundness of IRM-calc [6] is global, manipulating the whole refutation monolithically under an arguably complex inductive invariant. Should one want to add another rule to IRM-calc, the whole proof might need to be redone from scratch.

Semantics via Strategies. In our paper [28], we propose to use strategies, more specifically, the *partial strategies for the universal player*, as the central objects manipulated within a refutation. We show how strategies arise from the formula matrix and identify operations for obtaining new strategies by combining old ones. We then provide the missing meaning to the intermediate clauses of the existing calculi by seeing them as *abstractions* of these strategies. This way, we obtain soundness of all the calculi from Fig. 1 in a purely local, modular way.

Although primarily viewed as a model-theoretical concept in this context, the strategies also carry the obvious computational aspect. One can see the above mentioned abstraction as providing a specification for a strategy when understood as a program. This relates our approach to the Curry-Howard correspondence: We can treat the specification clause as a type and the derivation which lead to it and for which a strategy is the semantical denotation as the implementing program. The specification of the empty clause can then be read as "my strategy is total and, therefore, winning."

References

1. Balabanov, V., Jiang, J.R.: Unified QBF certification and its applications. Formal Methods in System Design 41(1), 45–65 (2012)
2. Balabanov, V., Jiang, J.R., Janota, M., Widl, M.: Efficient extraction of QBF (counter)models from long-distance resolution proofs. In: Bonet, B., Koenig, S. (eds.) Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA. pp. 3694–3701. AAAI Press (2015)
3. Balabanov, V., Widl, M., Jiang, J.H.R.: QBF resolution systems and their proof complexities. In: SAT. pp. 154–169 (2014)
4. Beyersdorff, O., Blinkhorn, J.: Dependency schemes in QBF calculi: Semantics and soundness. In: Rueher, M. (ed.) Principles and Practice of Constraint Programming - 22nd International Conference, CP 2016, Toulouse, France, September 5-9, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9892, pp. 96–112. Springer (2016)
5. Beyersdorff, O., Bonacina, I., Chew, L.: Lower bounds: From circuits to QBF proof systems. In: Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16). pp. 249–260. ACM (2016)
6. Beyersdorff, O., Chew, L., Janota, M.: On unification of QBF resolution-based calculi. In: Csuhaj-Varjú, E., Dietzfelbinger, M., Ésik, Z. (eds.) Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II. Lecture Notes in Computer Science, vol. 8635, pp. 81–93. Springer (2014)
7. Beyersdorff, O., Chew, L., Janota, M.: On unification of QBF resolution-based calculi. In: MFCS, II. pp. 81–93 (2014)
8. Beyersdorff, O., Chew, L., Janota, M.: Proof complexity of resolution-based QBF calculi. In: Proc. STACS. LIPIcs, vol. 30, pp. 76–89. Schloss Dagstuhl (2015)
9. Beyersdorff, O., Chew, L., Mahajan, M., Shukla, A.: Feasible interpolation for QBF resolution calculi. In: ICALP. Springer (2015)
10. Beyersdorff, O., Chew, L., Mahajan, M., Shukla, A.: Are short proofs narrow? QBF resolution is not simple. In: Proc. Symposium on Theoretical Aspects of Computer Science (STACS'16) (2016)
11. Beyersdorff, O., Chew, L., Schmidt, R.A., Suda, M.: Lifting QBF resolution calculi to DQBF. In: Creignou, N., Berre, D.L. (eds.) Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9710, pp. 490–499. Springer (2016)
12. Bjørner, N., Janota, M., Klieber, W.: On conflicts and strategies in QBF. In: Fehnker, A., McIver, A., Sutcliffe, G., Voronkov, A. (eds.) 20th International Conferences on Logic for Programming, Artificial Intelligence and

Reasoning - Short Presentations, LPAR 2015, Suva, Fiji, November 24-28, 2015. EPiC Series in Computing, vol. 35, pp. 28–41. EasyChair (2015), http://www.easychair.org/publications/paper/255082
13. Bloem, R., Braud-Santoni, N., Hadzic, V.: QBF solving by counterexample-guided expansion. CoRR abs/1611.01553 (2016), http://arxiv.org/abs/1611.01553
14. Cimatti, A., Sebastiani, R. (eds.): Theory and Applications of Satisfiability Testing - SAT 2012 - 15th International Conference, Trento, Italy, June 17-20, 2012. Proceedings, vol. 7317. Springer (2012)
15. Egly, U.: On sequent systems and resolution for QBFs. In: Cimatti and Sebastiani [14], pp. 100–113
16. Egly, U.: On stronger calculi for qbfs. In: Creignou, N., Berre, D.L. (eds.) Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9710, pp. 419–434. Springer (2016)
17. Heule, M.J., Seidl, M., Biere, A.: Efficient extraction of skolem functions from qrat proofs. In: Formal Methods in Computer-Aided Design (FMCAD), 2014. pp. 107–114. IEEE (2014)
18. Heule, M.J., Seidl, M., Biere, A.: A unified proof system for qbf preprocessing. In: Automated Reasoning, pp. 91–106. Springer (2014)
19. Janota, M., Klieber, W., Marques-Silva, J., Clarke, E.M.: Solving QBF with counterexample guided refinement. In: Cimatti and Sebastiani [14], pp. 114–128
20. Janota, M., Marques-Silva, J.: Expansion-based QBF solving versus Q-resolution. Theor. Comput. Sci. 577, 25–42 (2015)
21. Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for quantified Boolean formulas. Inf. Comput. 117(1), 12–18 (1995)
22. Lonsing, F., Biere, A.: DepQBF: A dependency-aware QBF solver. JSAT 7(2-3), 71–76 (2010)
23. Rabe, M.N., Tentrup, L.: CAQE: A certifying QBF solver. In: Kaivola, R., Wahl, T. (eds.) Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, USA, September 27-30, 2015. pp. 136–143. IEEE (2015)
24. Samulowitz, H., Bacchus, F.: Binary clause reasoning in QBF. In: Biere, A., Gomes, C.P. (eds.) Theory and Applications of Satisfiability Testing - SAT 2006, 9th International Conference, Seattle, WA, USA, August 12-15, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4121, pp. 353–367. Springer (2006)
25. Seidl, M., Lonsing, F., Biere, A.: qbf2epr: A tool for generating EPR formulas from QBF. In: Proc. PAAR-2012. EPiC, vol. 21, pp. 139–148. EasyChair (2013)
26. Slivovsky, F., Szeider, S.: Variable dependencies and Q-resolution. In: Sinz, C., Egly, U. (eds.) Theory and Applications of Satisfiability Testing - SAT 2014 - 17th International Conference, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8561, pp. 269–284. Springer (2014)
27. Slivovsky, F., Szeider, S.: Soundness of q-resolution with dependency schemes. Theor. Comput. Sci. 612, 83–101 (2016), https://doi.org/10.1016/j.tcs.2015.10.020
28. Suda, M., Gleiss, B.: Local soundness for qbf calculi. In: SAT (2018), To appear.
29. Van Gelder, A.: Contributions to the theory of practical quantified Boolean formula solving. In: Milano, M. (ed.) CP. vol. 7514, pp. 647–663. Springer (2012)
30. Zhang, L., Malik, S.: Conflict driven learning in a quantified boolean satisfiability solver. In: Pileggi, L.T., Kuehlmann, A. (eds.) Proceedings of the 2002 IEEE/ACM International Conference on Computer-aided Design, ICCAD 2002, San Jose, California, USA, November 10-14, 2002. pp. 442–449. ACM / IEEE Computer Society (2002), http://doi.acm.org/10.1145/774572.774637