Size, Cost, and Capacity: A Semantic Technique for Hard Random QBFs*

Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hinde

School of Computing, University of Leeds, UK

Abstract

Recent decades have seen significant advances in the solution of computationally hard problems, in particular the decision problem for the NP-complete language SAT [5]. Quantified Boolean formulas (QBF) extend propositional logic with existential and universal quantification, forming the prototypical PSPACE-complete language [8]. Despite the higher complexity, QBF solvers are beginning to rival SAT solvers in certain application areas [6], and appear to be reaching the point of industrial applicability.

Alongside the development of solvers, there has been much interest in associated proof systems and their relative proof complexities [4]. A host of QBF proof systems have been proposed, many of which extend some propositional system P to handle universal quantification [2]. A natural way to do this is to add a universal reduction rule, yielding the system P+∀red [1].

We present a new technique for proving proof-size lower bounds in P+∀red. The technique relies only on two semantic measures: the *cost* of a QBF, and the *capacity* of a proof. Our central result, the *Size-Cost-Capacity Theorem*, states that proof-size in P+∀red is at least the ratio of cost to capacity. By examining the capacity of proofs in several concrete systems (the universal reduction extensions of Resoution, Cutting Planes and Polynomial Calculus) we obtain lower bounds based solely on cost. Our technique provides *genuine* lower bounds in the sense that they continue to hold if P+∀red is given access to an NP oracle [3].

As applications of the technique, we first prove exponential lower bounds for the *equality formulas*, a new QBF family based on a simple two-player game. The main application is in proving exponential lower bounds with high probability for a class of randomly generated QBFs, the first genuine results of this kind. Finally, we employ the technique to give a simple proof of hardness for the prominent formulas of Kleine Büning, Karpinski and Flögel [7].

References

1. Beyersdorff, O., Bonacina, I., Chew, L.: Lower bounds: From circuits to QBF proof systems. In: Sudan, M. (ed.) ACM Conference on Innovations in Theoretical Computer Science (ITCS). pp. 249–260. ACM (2016)

* An extended abstract for this work was published in the proceedings of ITCS 2018

2. Beyersdorff, O., Chew, L., Janota, M.: Proof complexity of resolution-based QBF calculi. In: Mayr, E.W., Ollinger, N. (eds.) International Symposium on Theoretical Aspects of Computer Science (STACS). Leibniz International Proceedings in Informatics (LIPIcs), vol. 30, pp. 76–89. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2015)
3. Beyersdorff, O., Hinde, L., Pich, J.: Reasons for hardness in QBF proof systems. In: Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS) (2017)
4. Buss, S.R.: Towards NP-P via proof complexity and search. Ann. Pure Appl. Logic 163(7), 906–917 (2012)
5. Cook, S.A.: The complexity of theorem-proving procedures. In: Harrison, M.A., Banerji, R.B., Ullman, J.D. (eds.) ACM Symposium on Theory of Computing (STOC). pp. 151–158. ACM (1971)
6. Faymonville, P., Finkbeiner, B., Rabe, M.N., Tentrup, L.: Encodings of bounded synthesis. In: Legay, A., Margaria, T. (eds.) International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). Lecture Notes in Computer Science, vol. 10205, pp. 354–370 (2017)
7. Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for quantified Boolean formulas. Information and Computation 117(1), 12–18 (1995)
8. Stockmeyer, L.J., Meyer, A.R.: Word problems requiring exponential time: Preliminary report. In: Aho, A.V., Borodin, A., Constable, R.L., Floyd, R.W., Harrison, M.A., Karp, R.M., Strong, H.R. (eds.) ACM Symposium on Theory of Computing (STOC). pp. 1–9. ACM (1973)