"Quantum Supremacy" and the Complexity of Random Circuit Sampling

Adam Bouland

Electrical Engineering and Computer Sciences, University of California, Berkeley, 387 Soda Hall
Berkeley, CA 94720, U.S.A.
abouland@berkeley.edu
https://orcid.org/0000-0002-8556-8337

Bill Fefferman

Electrical Engineering and Computer Sciences, University of California, Berkeley, 387 Soda Hall
Berkeley, CA 94720, U.S.A.
Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland/NIST, Bldg 224 Stadium Dr Room 3100, College Park, MD 20742, U.S.A.
wjf@umiacs.umd.edu
https://orcid.org/0000-0002-9627-0210

Chinmay Nirkhe

Electrical Engineering and Computer Sciences, University of California, Berkeley, 387 Soda Hall
Berkeley, CA 94720, U.S.A.
nirkhe@cs.berkeley.edu
https://orcid.org/0000-0002-5808-4994

Umesh Vazirani

Electrical Engineering and Computer Sciences, University of California, Berkeley, 387 Soda Hall
Berkeley, CA 94720, U.S.A.
vazirani@cs.berkeley.edu

Abstract

A critical goal for the field of quantum computation is quantum supremacy – a demonstration of any quantum computation that is prohibitively hard for classical computers. It is both a necessary milestone on the path to useful quantum computers as well as a test of quantum theory in the realm of high complexity. A leading near-term candidate, put forth by the Google/UCSB team, is sampling from the probability distributions of randomly chosen quantum circuits, called Random Circuit Sampling (RCS).

While RCS was defined with experimental realization in mind, we give strong complexity-theoretic evidence for the classical hardness of RCS, placing it on par with the best theoretical proposals for supremacy. Specifically, we show that RCS satisfies an average-case hardness condition – computing output probabilities of typical quantum circuits is as hard as computing them in the worst-case, and therefore #P-hard. Our reduction exploits the polynomial structure in the output amplitudes of random quantum circuits, enabled by the Feynman path integral. In addition, it follows from known results that RCS also satisfies an anti-concentration property, namely that errors in estimating output probabilities are small with respect to the probabilities themselves. This makes RCS the first proposal for quantum supremacy with both of these properties. We also give a natural condition under which an existing statistical measure, cross-entropy, verifies RCS, as well as describe a new verification measure which in some formal sense maximizes the information gained from experimental samples.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases quantum supremacy, average-case hardness, verification

Digital Object Identifier 10.4230/LIPIcs.ITCS.2019.15

10th Innovations in Theoretical Computer Science (ITCS 2019).
Editor: Avrim Blum; Article No. 15; pp. 15:1–15:2
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Related Version A full version of this paper, including all proofs, is available at [1], `https://doi.org/10.1038/s41567-018-0318-2`.

Funding A.B., B.F., C.N. and U.V. were supported by ARO grant W911NF-12-1-0541 and NSF grant CCF-1410022 and a Vannevar Bush faculty fellowship. B.F. is supported in part by an Air Force Office of Scientific Research Young Investigator Program award number FA9550-18-1-0148. Parts of this work were done at the Kavli Institute for Theoretical Physics. Portions of this paper are a contribution of NIST, an agency of the US government, and are not subject to US copyright.

Acknowledgements We thank S. Aaronson, D. Aharonov, F. Brandão, M. Coudron, A. Deshpande, T. Gur, Z. Landau, N. Spooner and H. Yuen for helpful discussions.

References

1 Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 2018. `doi:10.1038/s41567-018-0318-2`.