nature physics

ARTICLES

https://doi.org/10.1038/s41567-018-0318-2

On the complexity and verification of quantum random circuit sampling

Adam Bouland[1], Bill Fefferman[1,2*], Chinmay Nirkhe[1] and Umesh Vazirani[1]

A critical milestone on the path to useful quantum computers is the demonstration of a quantum computation that is prohibitively hard for classical computers—a task referred to as quantum supremacy. A leading near-term candidate is sampling from the probability distributions of randomly chosen quantum circuits, which we call random circuit sampling (RCS). RCS was defined with experimental realizations in mind, leaving its computational hardness unproven. Here we give strong complexity-theoretic evidence of 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, which is critical to establishing computational hardness in the presence of experimental noise. 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. Finally, we also give a natural condition under which an existing statistical measure, cross-entropy, verifies RCS, as well as describe a new verification measure that in some formal sense maximizes the information gained from experimental samples.

Establishing the exponential advantage of quantum computers over their classical counterparts was a crucial development in launching the field of quantum computation. The first evidence came in the form of complexity-theoretic proofs that certain computational problems (of no practical value) can be solved exponentially faster by quantum computers in the black box model[1,2], thus calling into question the extended Church–Turing thesis, a foundational principle of classical complexity theory. Soon thereafter, Shor's quantum factoring algorithm[3] provided a practically useful quantum speed-up while at the same time giving a different type of evidence for the power of quantum computers—integer factorization is arguably the most well-studied algorithmic problem—studied by number theorists going back to Fermat, and with particularly intense algorithmic efforts motivated by cryptography, including the RSA challenge.

With the recent progress in experimental realization of 'noisy intermediate-scale' quantum computers[4–7], the field is again at the threshold of a key milestone: quantum supremacy; that is, the experimental realization of a computational task that cannot be solved in a reasonable amount of time by any classical means. As in the earliest demonstrations of 'theoretical quantum supremacy', there is no requirement that the computational task be useful. The new challenge is that the computational task be experimentally realizable for near-term devices, thus ruling out standard computational tasks such as large-scale factoring that `noisy intermediate-scale' quantum devices will not be capable of performing. Instead, all proposals for quantum supremacy have focused on sampling problems (for example, refs [8,9]), since the raw output of a quantum computer is a sample from a probability distribution resulting from a measurement. This choice, however, has important ramifications for the challenge of establishing computational difficulty of the task for any classical computer—both in the types of complexity-theoretic technique available for proving hardness and the relative lack of experience with the algorithmic difficulty of specific sampling problems.

Broadly speaking, we can classify supremacy proposals into two categories—those seeking to provide very strong complexity-theoretic evidence of classical intractability while hoping to be physically realized in the near term, versus those with excellent prospects for physical realization in the short term while providing weaker evidence of classical intractability. Here we show that these categories intersect by providing strong complexity-theoretic evidence of classical intractability for the leading candidate from the latter category.

More specifically, the first category of quantum supremacy proposals had their origins in the desire to obtain strong complexity-theoretic evidence of the power of quantum computers. A key insight was that focusing on the probability distributions quantum devices can sample from, rather than more standard notions of computing or optimizing functions, opens up the possibility of strong evidence of classical intractability. This perspective led to proposals such as BosonSampling[8] and IQP[10], together with proofs that the probabilities of particular quantum outcomes correspond to quantities that are difficult to compute. This allowed them to connect the hardness of classical simulation of such systems to well-supported hardness assumptions stemming from complexity theory.

As an added bonus, Aaronson and Arkhipov realized that BosonSampling might be experimentally feasible in the near term, and helped jump-start the quest for quantum supremacy more than half a decade ago[11–14]. More recently, BosonSampling experiments have faced experimental difficulties with photon generation and detector efficiency, making it challenging to push these experiments to the scale required to achieve supremacy (~50 photons)[15,16]. It remains to be seen whether such experiments can be implemented in the near future.

The second category of supremacy results is directly inspired by the dramatic experimental progress in building high-quality superconducting qubits (for example, refs [4,9]). These groups defined the natural sampling task for their experimental context, which we call random circuit sampling (RCS). The task is to take an (efficient) quantum circuit of a specific form, in which each gate is chosen

[1]Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA. [2]Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland/NIST, College Park, MD, USA. *e-mail: wjf@umiacs.umd.edu

randomly, and generate samples from its output distribution. This proposal promises to be more readily scaled to larger system sizes in the near term. In particular, the group at Google/University of California Santa Barbara (UCSB) plans to conduct such an experiment on a two-dimensional array of 49 qubits in the very near term[17]. However, RCS lacks some of the complexity-theoretic evidence that made BosonSampling so theoretically compelling—essentially because the quantum system is of a generic form that does not directly connect with complexity. To put this another way, usually the difficulty of simulating quantum algorithms comes from carefully engineered constructive and destructive interference patterns. However, RCS by definition reproduces only 'generic' interference patterns, and there is thus far no evidence that these are difficult to reproduce classically.

Our main result gives strong complexity-theoretic support to this experimentally driven proposal. In particular, we rely on a characterization of the output distribution of quantum circuits using Feynman path integrals as a stepping stone to showing that computing output probabilities of random quantum circuits is computationally hard. These tools are directly relevant to the upcoming superconducting experiment of Google/UCSB but will be useful to understand the capabilities of many other near-term experiments. Taken in combination with recent results establishing a subsequent piece of evidence for hardness for such systems[18,19], our result puts RCS on par with the strongest theoretical proposals for supremacy including BosonSampling.

There is one more ingredient of a quantum supremacy proposal such as RCS, namely verifying that an experimental realization of RCS has performed RCS faithfully. The two leading proposals for verification, cross-entropy and heavy output generation (HOG), are known to work only under strong, and distinct assumptions. Cross-entropy verifies supremacy under a very strong assumption about the error model, and HOG verifies supremacy under a strong complexity assumption. Here we show how to greatly relax the assumptions under which cross-entropy verifies supremacy. In particular, we show that if the entropy of the device's output distribution is greater than the ideal entropy, then cross-entropy verifies supremacy, through our complexity arguments. This condition would follow assuming some natural local noise models.

It turns out that, viewed from the correct perspective, cross-entropy and HOG are more similar than it appears at first sight. This perspective allows us to formulate a new verification measure—binned output generation (BOG), a common generalization of the two and has the property that it works if either does. In addition, it is the optimal verification measure in a certain formal sense.

Average-case hardness

Proposals for quantum supremacy have a common framework. The computational task is to sample from the output distribution D of some experimentally feasible quantum process or algorithm (on some given input). To establish quantum supremacy we must show hardness (that is, no efficient classical algorithm can sample from any distribution close to D) and verification (that is, an algorithm can check that the experimental device sampled from an output distribution close to D).This need for verifiability effectively imposes a robustness condition on the difficulty of sampling from D. For example, the ability to sample one particular output x of a quantum circuit with the correct probability $D(x)$ is known to be hard for classical computers, under standard complexity assumptions (for example, refs [10,20–23]). However, this is not a convincing proof of supremacy—for one, under any reasonable noise model, this single output probability $D(x)$ might not be preserved. Moreover, this single output x is exponentially unlikely to occur—and would therefore be extremely difficult to verify. Accordingly, any convincing proof of quantum supremacy must establish that D is actually uniformly difficult to sample from. That is, the computational difficulty must be embedded across the entire distribution, rather than concentrated in a single output.

The starting point for the BosonSampling proposal of Aaronson and Arkhipov consisted of three observations. First, in general, for sufficiently hard problems (think #P-hard), showing that a distribution D is uniformly difficult to sample from corresponds to showing that for most outputs x, it is hard to compute $D(x)$. In complexity theory, this is referred to as 'average-case' rather than 'worst-case' hardness. Second, the output probabilities of systems of non-interacting bosons can be expressed as permanents of certain $n\times n$ matrices. Third, by a celebrated result of Lipton[24], computing permanents of random matrices is #P-hard, or truly intractable in the complexity theory pantheon. Together, these gave convincing evidence of the hardness of sampling typical outputs of a suitable system of non-interacting bosons, which could be experimentally feasible in the near term.

Specifically, they proved that no classical computer can sample from any distribution within inverse-exponential total variation distance of the ideal BosonSampling output distribution. Formally extending these results to experimentally relevant noise models, such as constant total variation distance, seems to require approximation-robust average-case hardness that is beyond the reach of current methods. Nevertheless, their average-case hardness results are important as they establish a necessary foundation for noise-tolerant quantum supremacy of BosonSampling.

Permanents have a special structure enabling their average-case hardness—an ingredient that is thus far missing in other supremacy proposals. Technically, average-case hardness is established by creating a 'worst-to-average-case reduction'. We will show such a reduction for RCS. At a high level, such reductions are based on error-correcting codes, which are becoming more prominent across diverse areas of physics (see, for example, ref. [25]); just as an error-correcting code allows one to recover an encoded message under the corruption of some of its entries, a worst-to-average-case reduction allows one to recover a worst-case solution from an algorithm that works most of the time. More formally, such reductions involve showing that the value of a worst-case instance x can be efficiently inferred from the values of a few random instances $r_1, \ldots, r_m$. For this to be possible at all, while the r_k might be individually random, their correlations must depend on x (which we shall denote by r_0). Typically such reductions rely on a deep global structure of the problem, which makes it possible to write the value at r_k as a polynomial in k of degree at most m. For example, the average-case property of permanents is enabled by its algebraic structure—the permanent of an $n\times n$ matrix can be expressed as a low-degree polynomial in its entries. This allows the value at $r_0=x$ to be computed from the values at r_k by polynomial interpolation.

An astute reader may have noticed that randomizing the instance of permanent corresponds to starting with a random linear-optical network for the BosonSampling experiment, but still focusing on a fixed output. Our goal, however, was to show for a fixed experiment that it is hard to calculate the probability of a random output. These are equivalent by a technique called 'hiding'. By the same token, it suffices for RCS to show that it is hard to compute the probability of a fixed output, 0^n, for a random circuit C.

To show this average-case hardness for quantum circuits, we start with the observation that the probability with which a quantum circuit outputs a fixed outcome x can be expressed as a low-degree multivariate polynomial in the parameters describing the gates of the circuit, thanks to writing the acceptance probability as a Feynman path integral. Unfortunately, this polynomial representation of the output probability does not immediately yield a worst-to-average-case reduction. At its core, the difficulty is that we are not looking for structure in an individual instance—such as the polynomial description of the output probability for a particular circuit above. Rather, we would like to say that several instances

Table 1 | The leading quantum supremacy proposals

Proposal	Worst-case hardness	Exact average-case hardness	Approximate average-case hardness	Anti-concentration	Feasible experiment?
BosonSampling[a]	✓	✓			
FourierSampling[b]	✓	✓			
IQP[c]	✓			✓	
RCS[d]	✓	✓[e]		✓	✓

[a]Ref. [8]. [b]Ref. [26]. [c]Refs [10,27,29]. [d]Refs [9,19,33,35]. [e]This work.

of the problem are connected in some way, specifically by showing that the outputs of several different related circuits are described by a low-degree (univariate) polynomial. With permanents, this connection is established using the linear structure of matrices, but quantum circuits do not have a linear structure, that is if A and B are unitary matrices, then $A+B$ is not necessarily unitary. This limitation means that one cannot directly adapt the proof of average-case hardness for the permanent to make use of the Feynman path integral polynomial.

Here is a more sophisticated attempt to connect up the outputs of different circuits with a polynomial: suppose we take a worst-case circuit $G=G_m \ldots G_1$, and multiply each gate G_j by a Haar-random matrix H_j. By the invariance of the Haar measure, this is another random circuit—it is now totally scrambled. Now we invoke a unique feature of quantum computation, which is that it is possible to implement a fraction of a quantum gate. This allows us to replace each gate H_j with $H_j e^{-i\theta h_j}$, where $h_j=-i\log H_j$ and θ is a small angle, resulting in a new circuit $G(\theta)$. If $\theta=1$ this gives us back the worst-case circuit $G(1)=G$, but if θ is very tiny the resulting circuit looks almost uniformly random. One might now hope to interpolate the value of $G(1)$ from the values of $G(\theta_k)$ for many small values of θ_k, thus effecting a worst-to-average-case reduction. Unfortunately, this does not work either. The problem is that $e^{-i\theta h_j}$ is not a low-degree polynomial in θ, and therefore neither is $G(\theta)$, so we have nothing to interpolate with.

The third attempt, which works, is to consider using a truncated Taylor series of $e^{-i\theta h_j}$ in place of $e^{-i\theta h_j}$ in the above construction. The values of the probabilities in this truncation will be very close to those of the proposal above—and yet by construction we have ensured our output probabilities are low-degree polynomials in θ. Therefore, if we could compute most output probabilities of these 'truncated Taylor' relaxations of random circuits, then we could compute a worst-case probability.

Theorem 1 (simplified): it is #P-hard to exactly compute $|\langle 0|C'|0\rangle|^2$ with probability $\frac{3}{4}+\frac{1}{\mathrm{poly}(n)}$ over the choice of C', where each gate of C' is drawn from any one of a family of discretizations of the Haar measure.

These truncated circuit probabilities are slightly different from the average-case circuit probabilities but are exponentially close to them (even in relative terms). However, they are essentially the same from the perspective of supremacy arguments because quantum supremacy requires that computing most output probabilities even approximately remains #P-hard, and our perturbations to the random circuits fall within this approximation window. Therefore, we have established a form of worst-to-average-case reduction that is necessary, but not sufficient, for the supremacy condition to remain true. This is directly analogous to the case of permanents, where we know that computing average-case permanents exactly is #P-hard, but we do not know this reduction is sufficiently robust to achieve quantum supremacy. For more details, see the Methods (Section 3.1).

RCS does satisfy an additional robustness property known as 'anti-concentration'. Anti-concentration states that the output distribution of a random quantum circuit is 'spread out'—that most output probabilities are reasonably large. Therefore, any approximation errors in estimating these probabilities are small relative to the size of the probability being computed. Once one has established a worst-to-average-case reduction, anti-concentration implies that there is some hope for making this reduction robust to noise—intuitively it says that the signal is large compared to the noise.

Of the numerous quantum supremacy proposals to date that are conjectured to be robust to noise[8,9,19,26–32], only two have known worst-to-average-case reductions: BosonSampling and FourierSampling[8,26]. However, it remains open whether these proposals also anti-concentrate. On the other hand, many supremacy proposals have known anti-concentration theorems (see, for example, refs [9,19,27,29–32]), but lack worst-to-average-case reductions. We note, however, that anti-concentration is arguably less important than worst-to-average-case reductions, as the latter are necessary for quantum supremacy arguments, while the former is not expected to be necessary. In the case of RCS, anti-concentration follows from previous work[18,19]. Therefore, our work shows that both can be achieved simultaneously. In Table 1 we list the leading quantum supremacy proposals and summarize their known complexity-theoretic properties.

Statistical verification of RCS

We now turn to verifying that an experimental realization of RCS has performed RCS faithfully. Verification turns out to be quite challenging. The first difficulty is that computing individual output probabilities of an ideal quantum circuit requires exponential classical time. However, current proposals leverage the fact that near-term devices with around $n=50$ qubits are small enough that it is feasible to perform this task on a classical supercomputer (inefficiently), but large enough that the quantum device solves an impressively difficult problem. While this might seem contradictory to the claim of quantum supremacy, note that the task that is (barely) feasible with an inefficient algorithm is to compute only individual probabilities. In contrast, naively simulating the sampling experiment would require far more—either computing all of the probabilities or computing a smaller number of conditional probabilities. The second difficulty is that one can take only a small number of samples from the experimental quantum device. This means that there is no hope of experimentally observing all 2^{50} outcomes, nor of estimating their probabilities empirically. The challenge is therefore to develop a statistical measure that respects these limitations, and nevertheless verifies quantum supremacy.

A leading statistical measure proposed for verification is the 'cross-entropy' measure[9,33,34], which, for a pair of distributions D and D', is defined as:

$$\mathrm{CE}(D,D')=\sum_{x\in\{0,1\}^n} D(x)\log\left(\frac{1}{D'(x)}\right)$$

For RCS it is being used as a measure of the distance between the output distribution of the experimental device tuned to perform the

unitary U, denoted p_{dev}, and the ideal output distribution of the random circuit under U, denoted p_U.

A useful feature of this measure is that it can be estimated by taking a few samples x_i from the device and computing the average value of $\log(1/p_U(x_i))$ using a classical supercomputer. By concentration of measure arguments this converges very quickly to the true value.

Ideally, we would like to connect the cross-entropy measure to the rigorous complexity-theoretic arguments in favour of quantum supremacy developed in the section entitled Average-case hardness, which require closeness in total variation distance to the ideal. Without any assumptions as to how the device operates, it is easy to see that cross-entropy cannot verify total variation distance directly, as the latter requires exponentially many samples to verify.

However, we show that there is a natural assumption under which the cross-entropy measure certifies closeness in total variation distance. Namely, if one assumes that the entropy of the experimental device is greater than the entropy of the ideal device, then scoring well in cross-entropy does certify closeness in total variation distance.

Claim 2: if $H(p_{\mathrm{dev}}) \geq H(p_U)$, then achieving a cross-entropy score that is ϵ-close to ideal (that is, $|\mathrm{CE}(p_{dev}, p_U) - H(p_U)| \leq \epsilon$) implies that $\|p_{dev} - p_U\| \leq \sqrt{\epsilon / 2}$.

The proof of this fact follows from Pinsker's inequality. A similar observation was recently independently obtained (F. Brandão, personal communication). This assumption would follow from a number of natural noise models—such as local depolarizing noise, but not others—such as forms of erasure. Therefore, to understand the utility of cross-entropy it is crucial to characterize the noise present in near-term devices. We also use this as intuition to construct distributions that score well on cross-entropy but are far in total variation distance—we start with the ideal distribution and lower entropy.

A concurrent proposal of Aaronson and Chen, known as HOG, studied a different avenue to supremacy. Aaronson and Chen conjectured that given a randomly chosen quantum circuit C, it is difficult to output strings that have 'above median' mass in C's output distribution. This proposal connects directly to a statistical test for verification, and the hardness of this task was connected to a non-standard complexity-theoretic conjecture known as QUATH.

To generalize these verification proposals, we describe a new statistical measure that we call BOG. BOG is a common ancestor to both cross-entropy and HOG and yet it is still easy to estimate from experimental data. In particular, this means that BOG verifies supremacy if either the entropy assumption or QUATH holds. Indeed, viewed from the right perspective, these measures are more similar than it appears at first sight. In some formal sense, BOG maximizes the amount of information one gains in the course of computing HOG or cross-entropy, and is therefore the optimal verification measure if one can take only polynomially many samples from the experimental device. For more details, see the Methods (Verification of RCS).

Online content

Any methods, additional references, Nature Research reporting summaries, source data, statements of data availability and associated accession codes are available at https://doi.org/10.1038/s41567-018-0318-2.

Received: 29 March 2018; Accepted: 14 September 2018;
Published online: 29 October 2018

References

1. Bernstein, E. & Vazirani, U. V. Quantum complexity theory. In *Proc. 25th Annual ACM Symposium on Theory of Computing* (eds Kosaraju, S. R. et al.) 11–20 (ACM, 1993).
2. Simon, D. R. On the power of quantum cryptography. In *Proc. 35th Annual Symposium on Foundations of Computer Science* 116–123 (IEEE Computer Society, 1994).
3. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**, 303–332 (1999).
4. Mohseni, M. et al. Commercialize quantum technologies in five years. *Nature* **543**, 171–174 (2017).
5. Kandala, A. et al. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* **549**, 242–246 (2017).
6. Zhang, J. et al. Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. *Nature* **551**, 601–604 (2017).
7. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
8. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. In *Proc. 43rd Annual ACM Symposium on Theory of Computing* (eds Fortnow, L. & Vadhan, S. P.) 333–342 (ACM, 2011).
9. Boixo, S. et al. Characterizing quantum supremacy in near-term devices. *Nat. Phys.* **14**, 595–600 (2018).
10. Bremner, M. J., Jozsa, R. & Shepherd, D. J. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proc. Royal Society of London A: Mathematical, Physical and Engineering Sciences* 459–472 (The Royal Society, 2010).
11. Spring, J. B. et al. Boson sampling on a photonic chip. *Science* **339**, 798–801 (2013).
12. Broome, M. A. et al. Photonic boson sampling in a tunable circuit. *Science* **339**, 794–798 (2013).
13. Tillmann, M. et al. Experimental boson sampling. *Nat. Photonics* **7**, 540–544 (2013).
14. Crespi, A. et al. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nat. Photonics* **7**, 545–549 (2013).
15. Neville, A. et al. No imminent quantum supremacy by boson sampling. *Nat. Phys.* **13**, 1153–1157 (2017).
16. Clifford, P. & Clifford, R. The classical complexity of boson sampling. In *Proc. 29th Annual ACM-SIAM Symposium on Discrete Algorithms*, (ed. Czumaj, A.) 146–155 (SIAM, 2018).
17. Martinis, J. The quantum space race (2018). Plenary talk at Quantum Information Processing (QIP) 2018. *TU Delft* https://collegerama.tudelft.nl/Mediasite/Showcase/qip2018/Channel/qip-day3 (2018)
18. Brandão, F. G. & Horodecki, M. Exponential quantum speed-ups are generic. *Quantum Inf. Comput.* **13**, 901–924 (2013).
19. Hangleiter, D., Bermejo-Vega, J., Schwarz, M. & Eisert, J. Anticoncentration theorems for schemes showing a quantum speedup. *Quantum* **2**, 65 (2018).
20. Terhal, B. M. & DiVincenzo, D. P. Adaptive quantum computation, constant depth quantum circuits and Arthur–Merlin games. *Quantum Inf. Comput.* **4**, 134–145 (2004).
21. Morimae, T., Fujii, K. & Fitzsimons, J. F. Hardness of classically simulating the one-clean-qubit model. *Phys. Rev. Lett.* **112**, 130502 (2014).
22. Farhi, E. & Harrow, A. W. Quantum supremacy through the quantum approximate optimization algorithm. Preprint at https://arxiv.org/abs/1602.07674 (2016).
23. Bouland, A, Mancinska, L. & Zhang, X. Complexity classification of two-qubit commuting Hamiltonians. In *Proc. 31st Conference on Computational Complexity (CCC 2016), vol. 50 of Leibniz International Proceedings in Informatics (LIPIcs)* (ed. Raz, R.) 28:1–28:33 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016).
24. Lipton, R. J. New directions in testing. In *Proc. Distributed Computing and Cryptography,* vol. 2 of DIMACS Series in Discrete Mathematics and Theoretical Computer Science (eds Feigenbaum, J. & Merritt, M.) 191–202 (DIMACS/AMS, 1991).
25. Pastawski, F., Yoshida, B., Harlow, D. & Preskill, J. Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence. *J. High Energy Phys.* **2015**, 149 (2015).
26. Fefferman, B. & Umans, C. On the power of quantum Fourier sampling. In *Proc. 11th Conference on the Theory of Quantum Computation, Communication and Cryptography,* vol. 61 of Leibniz International Proceedings in Informatics (LIPIcs) (ed. Broadbent, A.) 1:1–1:19 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016).
27. Bremner, M. J., Montanaro, A. & Shepherd, D. J. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.* **117**, 080501 (2016).
28. Aaronson, S. & Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. In *Proc. 32nd Computational Complexity Conference, vol. 79 of LIPIcs* (ed. O'Donnell, R.) 22:1–22:67 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017).
29. Bremner, M. J., Montanaro, A. & Shepherd, D. J. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum* **1**, 8 (2017).
30. Morimae, T. Hardness of classically sampling the one-clean-qubit model with constant total variation distance error. *Phys. Rev. A* **96**, 040302 (2017).

31. Bouland, A, Fitzsimons, J. F. & Koh, D. E . Complexity classification of conjugated Clifford circuits. In *Proc. 33rd Computational Complexity Conference*, *vol. 102 of Leibniz International Proceedings in Informatics (LIPIcs)* (ed. Servedio, R. A.) 21:1–21:25 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik: 2018).
32. Mann, R. L. & Bremner, M. J. On the complexity of random quantum computations and the Jones polynomial. Preprint at https://arxiv.org/abs/1711.00686 (2017).
33. Neill, C. et al. A blueprint for demonstrating quantum supremacy with superconducting qubits. *Science* **360**, 195–199 (2018).
34. Boixo, S., Smelyanskiy, V. N. & Neven, H. Fourier analysis of sampling from noisy chaotic quantum circuits. Preprint at https://arxiv.org/abs/1708.01875 (2017).
35. Harrow, A. W. & Low, R. A. Random quantum circuits are approximate 2-designs. *Commun. Math. Phys.* **291**, 257–302 (2009).

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. 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.

Author contributions

All authors contributed equally to this work; author ordering is alphabetical.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41567-018-0318-2.

Reprints and permissions information is available at www.nature.com/reprints.

Correspondence and requests for materials should be addressed to B.F.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Methods

Worst-to-average-case reduction. Our first result gives evidence that approximating average-case output probabilities of random quantum circuits remains difficult. It is well known that computing output probabilities of worst-case quantum circuits is #P-hard. Our goal is, therefore, to establish that computing output probabilities of average-case random quantum circuits is just as difficult. We achieve this by giving a worst-to-average-case reduction for computing output probabilities of random quantum circuits. That is, we show that if one could compute average-case quantum circuit probabilities, then one could infer the value of worst-case quantum circuit probabilities. Therefore, computing average-case probabilities is also #P-hard.

Establishing average-case hardness is surprisingly subtle. It will be useful to first recall the worst-to-average-case reduction for the permanent of matrices over the finite field $\mathbb{F}_q$ (ref. [24]), where q is taken to be a sufficiently large polynomial in the input parameter. In the case of permanents, the structure that connects the values of random permanents is low-degree polynomials. The permanent of an $n\times n$ matrix,

$$\mathrm{perm}(A)=\sum_{\sigma\in S_n}\prod_{i=1}^{n}A_{i,\sigma(i)}$$

is a polynomial of degree n in the n^2 matrix entries. Let X be a random $n\times n$ matrix over $\mathbb{F}_q$, where $q\geq n+2$. Moreover, suppose our goal is compute the permanent of a worst-case matrix Y. We first consider the line $A(t)=Xt+Y$; note that for $t\neq 0$, $A(t)$ is uniformly distributed over $\mathbb{F}_q^{n\times n}$. If we are able to calculate $\mathrm{perm}(R)$ with probability $\geq 1-\frac{1}{3(n+1)}$ over $R\sim_U\mathbb{F}_q^{n\times n}$, then by the union bound, we could compute $A(t)$ correctly at $n+1$ different values of t with bounded error probability. This is possible because the union bound holds despite $A(t)$ being correlated with one another—it requires only that the marginal distribution on each one is uniform. Thus, standard polynomial interpolation techniques on $\{(t_j,\mathrm{perm}(A(t_j))\}_{j=1,\ldots,n+1}$ allow us to learn the function $\mathrm{perm}(A(t))$ and therefore, $\mathrm{perm}(Y)=\mathrm{perm}(A(0))$. With more rigorous analysis—but the same intuition—one can argue that we only need to calculate $\mathrm{perm}(R)$ with probability $3/4+1/\mathrm{poly}(n)$[36,37].

Therefore, polynomial interpolation allows us to compute permanents of every matrix $\in\mathbb{F}_q^{n\times n}$ if we can compute the permanent on most matrices. A 'random survey' of permanent values can be used to infer the value of all permanents. Combined with the fact that the permanent problem is worst-case #P-hard[38], this implies that computing permanents in $\mathbb{F}_q^{n\times n}$ on average is #P-hard. Formally, the following result was obtained.

Theorem 3 (average-case hardness for permanents[24,37]): the following is #P-hard: for sufficiently large q, given a uniformly random matrix $M\in\mathbb{F}_q^{n\times n}$, output $\mathrm{perm}(M)$ with probability $\geq\frac{3}{4}+\frac{1}{\mathrm{poly}(n)}$.

To establish worst-to-average-case reductions for random circuits, we need to find a similar structural relation between the circuit whose output probability we wish to compute, and average-case circuits in which each gate is chosen randomly. A first observation is that there is indeed a low-degree polynomial structure—stemming from the Feynman path-integral—which allows us to write the probability of any outcome as a low-degree polynomial in the gate entries. This polynomial is fixed once we fix both the outcome and the architecture of the circuit, and the degree is twice the number of gates in the circuit (where the factor of 2 accounts for the Born rule for output probabilities), which is a polynomial in the input parameter.

Fact 4 (Feynman path integral): let $C=C_mC_{m-1}\ldots C_2C_1$ be a circuit formed by individual gates C_i acting on n qubits. Then

$$\langle y_m|\,C\,|y_0\rangle=\sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n}\prod_{j=1}^{m}\langle y_j|\,C_j\,|y_{j-1}\rangle$$

There are two subtleties we need to address. The first is that the value of this polynomial is the probability of a fixed output y_m. Our analysis will therefore focus on the hardness of estimating the

$$\mathrm{p}_0(C)\overset{\mathrm{def}}{=}|\langle 0^n|\,C\,|0^n\rangle|^2$$

probability for C drawn from $\mathcal{H}_\mathcal{A}$, rather than the hardness of approximating the probability of a random y_m. These can be proved to be equivalent using the 'hiding' property of the $\mathcal{H}_\mathcal{A}$ distribution: we can take a circuit drawn from this distribution, append Pauli X gates to a uniformly chosen subset of output qubits, and remain distributed via $\mathcal{H}_\mathcal{A}$. We discuss hiding in more detail in Supplementary Section 1.5.

The second subtlety is that this is a polynomial over the complex numbers, instead of $\mathbb{F}_q$. Bridging this gap requires considerable technical work. We note that Aaronson and Arkhipov have given a worst-to-average-case reduction for computing the permanent with complex Gaussian entries[8]. However, our reduction will be quite different, due to structural differences between quantum circuit amplitudes and permanents. Indeed, in proving the reduction for permanents of matrices over finite fields, we leveraged the fact that $A(t)=Xt+Y$ will be randomly distributed across $\mathbb{F}_q^{n\times n}$ since X is uniformly random and Y is fixed. To leverage a similar property for RCS, we need, given a (possibly worst-case) circuit C, a polynomial $C(t)$ over circuits such that $C(0)=C$ and $C(t)$ is distributed like a $\mathcal{H}_\mathcal{A}$. To be more precise, for a fixed architecture $\mathcal{A}$, we hope to say that the $p_0(C)$ probability for a circuit $C\sim\mathcal{H}_\mathcal{A}$ is hard to compute on average.

A naive approach to doing this is to copy the proof for the permanent. If we could perturb each gate in a random linear direction, then we could use polynomial interpolation to perform the worst-to-average-case reduction as above. That is, consider taking a worst-case circuit A and adding a random circuit B (gate by gate) to obtain $A+tB$. It is true that $\mathrm{p}_0(A+tB)$ is a low-degree polynomial in t, so one might hope to use interpolation to compute the worst-case value at $t=0$. Unfortunately, this idea does not work because quantum gates do not have a linear structure. In other words, if A and B are unitary matrices, then $A+tB$ is not necessarily unitary—and hence $A+tB$ are not necessarily valid quantum circuits. Thus, this naive interpolation strategy will not work.

We consider a different way of perturbing circuits, which makes use of the unique properties of quantum mechanics. Suppose that we take a (possibly worst-case) circuit $C=C_m,\ldots,C_1$, and multiply each gate C_j by an independent Haar-random matrix H_j. That is, we replace each gate C_j with C_jH_j. By the left-invariance of the Haar measure, this is equivalent to selecting each gate uniformly at random—that is, it is equivalent to $\mathcal{H}_\mathcal{A}$. We have now recovered our original distribution over circuits, but in some sense we have gone too far, as we have completely erased all of the information of our worst-case circuit C. To remedy this, we will make use of a uniquely quantum ability—namely, that it is possible to perform a fraction of a quantum gate. This has no classical analogue (indeed, what would it mean to perform 1/10 of a NAND gate?). That is, suppose we 'rotate back' by a tiny amount back towards C_j by some small angle θ. More specifically, replace each gate C_j of the circuit with $C_jH_je^{-ih_j\theta}$, where $h_j=-i\log H_j$. If $\theta=1$ this gives us back the circuit C, but if θ is very tiny then each gate looks almost Haar random. One might hope that by collecting the values of many probabilities at small angles θ, one could interpolate back to the point C of interest. Therefore, a second attempt would be to take the circuit C, scramble it by multiplying it gate-wise by a perturbed Haar distribution defined below, and then use some form of interpolation in θ to recover the probability for C at $\theta=1$.

Definition 5 (θ-perturbed Haar distribution): let $\mathcal{A}$ be an architecture over circuits, θ a constant $\in[0,1]$, and let $G_m,\ldots,G_1$ be the gate entries in the architecture. Define the distribution $\mathcal{H}_{\mathcal{A},\theta}$ over circuits in $\mathcal{A}$ by setting each gate $G_j=H_je^{-ih_j\theta}$, where H_j is an independent Haar random unitary and $h_j=-i\log H_j$.

Unfortunately, this trick is not sufficient to enable the reduction. The problem is that $e^{-i\theta h_j}$ is not a low-degree polynomial in θ, so we have no structure to apply polynomial interpolation onto. While there is structure, we cannot harness it for interpolation using currently known techniques. Although this does not work, this trick has allowed us to make some progress. A promising property of this method of scrambling is that it produces circuits that are close to randomly distributed—which we will later prove rigorously. This is analogous to the fact that $A+tB$ is randomly distributed in the permanent case, a key property used in that proof. We merely need to find some additional polynomial structure here to utilize this property.

We find this polynomial structure by considering Taylor approximations of $e^{-ih_j\theta}$ in place of $e^{-ih_j\theta}$ in the above construction. While these truncated circuits are slightly non-unitary, the values of the probabilities in this truncation will be very close to those of the proposal above—and yet by construction we have ensured our output probabilities are low-degree polynomials in θ. Formally, we define a new distribution over circuits with this property in the following.

Definition 6 ((θ,K)-truncated perturbed Haar distribution): let $\mathcal{A}$ be an architecture over circuits, θ a constant $\in[0,1]$, K an integer, and let $G_m,\ldots,G_1$ be the gate entries in the architecture. Define the distribution $\mathcal{H}_{\mathcal{A},\theta,K}$ over circuits in $\mathcal{A}$ by setting each gate

$$G_j=H_j\left(\sum_{k=0}^{K}\frac{(-ih_j\theta)^k}{k!}\right)$$

where H_j is an independent Haar random unitary and $h_j=-i\log H_j$.

Now suppose we take our circuit C of interest and multiply it by $\mathcal{H}_{\mathcal{A},\theta,K}$ gate-by-gate to 'scramble' it. This is precisely how a classical computer would sample from $C\times\mathcal{H}_{\mathcal{A},\theta}$ (where the multiplication is performed gate-wise) as one cannot exactly represent a continuous quantity digitally. Suppose we could compute the probabilities of these circuits for many choices of θ with high probability. Now one can use similar polynomial interpolation ideas to show hardness of this task.

To state this formally, let us define some notation. For a circuit C and $\mathcal{D}$ a distribution over circuits of the same architecture, let $C\times\mathcal{D}$ be the distribution over circuits generated by sampling a circuit $C'\sim\mathcal{D}$ and outputting the circuit $C\times C'$ (where again, the multiplication is performed gate-wise). Explicitly, we show the following worst-to-average-case reduction.

Theorem 1: let $\mathcal{A}$ be an architecture so that computing $p_0(C)$ to within additive precision $2^{-\mathrm{poly}(n)}$, for any C over $\mathcal{A}$ is #P-hard in the worst case. Then it is #P-hard to exactly compute $\frac{3}{4}+\frac{1}{\mathrm{poly}(n)}$ of the probabilities $p_0(C')$ over the choice of C' from the distributions $\mathcal{D}'_C=C\times\mathcal{H}_{\mathcal{A},\theta,K}$, where $\theta=1/\mathrm{poly}(n)$, $K=\mathrm{poly}(n)$.

A formal proof of Theorem 1, as well as commentary on its relation to the hardness conjectures, needed to establish quantum supremacy, is provided in the Supplementary Information. For example, although we have changed the distribution over which average-case hardness is established, we show that hardness over the new distribution, Theorem 1, is necessary for the average-case conjecture relevant to the quantum supremacy of RCS to be true. For details, see Supplementary Section 1.2.

Verification of RCS. In this section, we discuss the verification of RCS experiments. Let us first recall the setting: we are given a description of a randomly generated quantum circuit (which we will refer to as the ideal circuit) as well as an experimental device that outputs samples.

We wish to verify that no efficient classical device could have produced this output. One difficulty that immediately arises is that one can take only a small (polynomial) number of samples from the device, and therefore one cannot characterize the entire output distribution of the device. Another basic difficulty is that the output of the ideal circuit is computationally hard to produce—so for large system sizes we do not even know what to compare the output of the experimental device to. Current verification schemes leverage the fact that intermediate size experiments, such as $n=50$ qubit systems, are small enough that it is feasible to calculate on a classical supercomputer the probability p_x that the ideal quantum circuit outputs a particular string x. The list of strings x output by the device, together with p_x, is summarized in a statistical score that can be efficiently estimated with few samples from the device. Our goal is to understand under what circumstances such a score verifies quantum supremacy.

In this section, if unspecified, a probability distribution will be over strings $x\in\{0,1\}^n$. The size of the domain will be denoted $N=2^n$. The phrase 'with high probability' will mean with probability $1-o(1)$.

The cross-entropy supremacy proposal. Cross-entropy is a leading proposal for verifying quantum supremacy[9,33,34]. Recall from the section entitled Statistical verification of RCS that the cross-entropy between distributions D and D' is defined as $\mathrm{CE}(D,D')=\sum_{x\in\{0,1\}^n} D(x)\,\log\left(\frac{1}{D'(x)}\right)$. For RCS, it is being used as a measure of the distance between the output distribution of the experimental device tuned to perform the unitary U, denoted p_{dev}, and the ideal output distribution of the random circuit under U, denoted p_U[9,33,34]. Estimating $\mathrm{CE}(p_{\mathrm{dev}}, p_U)$ requires taking merely $k\ll N$ samples, $x_1,\ldots,x_k$, from the experimental device, followed by the computation of the empirical estimate E of the cross-entropy

$$E=\frac{1}{k}\sum_{i=1\ldots k}\log\left(\frac{1}{p_U(x_i)}\right) \tag{1}$$

by using a supercomputer to calculate ideal probabilities $p_U(x_i)=|\langle x_i|\ U\ |0^n\rangle|^2$ for only the observed outcome strings x_i. By concentration of measure, for typical U, after polynomially many samples, E will converge to $\mathrm{CE}(p_{\mathrm{dev}}, p_U)$. This follows from the fact that with high probability over the choice of random unitary, the largest and smallest ideal outcome probability are of order $\log N/N$ and $1/N^2$, respectively. Hence, the logarithms of all $p_U(x_i)$ are within a constant factor of one another (on average), so by the Chernoff bound one can estimate this quantity to multiplicative error ϵ with merely $\log(1/\epsilon)$ samples.

The goal of their experiment is to score as close to the ideal expectation value as possible (on average over the choice of U). In fact, this measure has become incredibly important to the Google/UCSB group: it is being used to calibrate their candidate experimental device[17,33].

The relationship between cross-entropy and total variation distance. As before, let p_U be the ideal output distribution and p_{dev} be the output distribution of the experimental device. To motivate the cross-entropy score, the Google/UCSB paper assumes that p_{dev} is a convex combination of p_U with the uniform distribution[9]. Here we show that scoring well in cross-entropy certifies closeness in total-variation distance under a considerably weaker assumption.

Assumption 7: $H[p_{\mathrm{dev}}]\geq H[p_U]$. Claim 8: if Assumption 7 holds, then achieving a cross-entropy score that is ϵ-close to ideal (that is, $|\mathrm{CE}(p_{\mathrm{dev}},p_U)-H(p_U)|\leq\epsilon$) implies that $\|p_{dev}-p_U\|\leq\sqrt{\epsilon/2}$. Proof: the claim follows from a straightforward application of Pinkser's inequality:

$$\|p_{\mathrm{dev}}-p_U\|\leq\sqrt{\frac{\|p_{\mathrm{dev}}-p_U\|_{KL}}{2}} \tag{2}$$

$$=\sqrt{\frac{\mathrm{CE}(p_{\mathrm{dev}},p_U)-H(p_{\mathrm{dev}})}{2}} \tag{3}$$

$$\leq\sqrt{\frac{\mathrm{CE}(p_{\mathrm{dev}},p_U)-H(p_U)}{2}}\leq\sqrt{\frac{\epsilon}{2}} \tag{4}$$

where equation (2) is Pinsker's inequality, equation (3) follows from the definition of KL divergence $\|D,D'\|_{KL}=\mathrm{CE}(D,D')-H(D)$ and equation (4) follows from Assumption 7.

It might appear at first sight that Assumption 7 follows from the very reasonable physical assumption that the experimental device is any noisy version of the ideal device. While this is not true in general, it does hold for some standard noise models such as local depolarizing noise. Thus, one approach to verification is to verify the noise model and show that it is consistent with Assumption 7. We note that, of course, verifying Assumption 7 directly would require exponentially many samples from the device.

Following this connection further, one can easily construct examples of distributions that score well on cross-entropy but are far from ideal in total variation distance. In particular, one can achieve this by taking the ideal distribution and reducing its entropy.

Theorem 9: for every unitary U, there exists a distribution D_U such that, with probability $1-o(1)$ over the choice of U from the Haar measure, $|D_U-p_U|\geq 0.99$, and yet $\mathrm{CE}(D_U, p_U)$ is $O(1/N^{\Theta(1)})$-close to ideal.

We provide a proof of Theorem 9 in the Supplementary Information.

BOG is a common ancestor to cross-entropy and HOG. Recall that the goal of these statistical measures is to verify RCS with very few samples from the experimental device, but allowing for exponential classical post-processing time (see Statistical verification of RCS). These tests are all performed by taking $k=\mathrm{poly}(n)$ samples from the device $x_1\ldots x_k$ and then computing statistics on the ideal output probabilities $p_U(x_i)$ of the observed strings. It is natural to try to maximize the amount of information obtained from the computed values of $p_U(x_i)$, so as to eliminate the largest number of imposter distributions. In this section, we describe a statistical measure that performs this task. It simultaneously generalizes both HOG and cross-entropy difference—that is, passing this test implies that one has scored well on both cross-entropy and HOG. Furthermore, this test eliminates more imposter distributions than naively combining cross-entropy and HOG. As discussed previously, cross-entropy and HOG certify supremacy under two very different assumptions—one relating to the noise present in the device, and another to a non-standard complexity conjecture. Therefore, this new measure verifies quantum supremacy if either assumption holds. We call this measure BOG, which we define below.

Consider dividing the interval [0, 1] into $\mathrm{poly}(n)$ bins, such that for each bin $[a/N, b/N]$, we have $\int_a^b q\mathrm{e}^{-q}=\Theta(1/\mathrm{poly}(n))$. In other words, when sampling from a Porter–Thomas distribution, one would expect to see roughly an equal number of counts of $p_U(x_i)$ in each bin. Now suppose that one takes $k=\mathrm{poly}(n)$ samples from an experimental device (with a randomly chosen U) to obtain strings $x_1\ldots x_k$. We say that the test passes if one has approximately the correct frequency of counts of $p_U(x_i)$ in each bin (up to small constant multiplicative error). By concentration of measure, the ideal distribution will pass the test with high probability.

BOG can be seen as a simple refinement of HOG, where we divide the output probabilities into $\mathrm{poly}(n)$ bins instead of two (below median and above median). Therefore, this measure both verifies HOG and additionally ensures that the more fine-grained 'shape' of the distribution is present as well. Furthermore, one can show that for a suitable choice of parameters, passing BOG implies that one has achieved nearly the ideal cross-entropy as well—as the ideal cross-entropy is $O(n)$, an $(1\pm 1/\mathrm{poly}(n))$ multiplicative approximation to the cross-entropy suffices to verify $o(1)$ closeness to the ideal cross-entropy difference. BOG extracts the maximum amount of information out of the computation of the $p_U(x_i)$, as long as one ignores the higher-order bits of the results. Differences between these higher-order bits are not observable with merely $\mathrm{poly}(n)$ samples from the device. For instance, if one passes BOG, then one has certified the expectation value of any Lipschitz function of the ideal probabilities to error $O(1/\mathrm{poly})$. In this particular sense, BOG is information theoretically optimal. We therefore propose BOG as a measure for verification, as it uses the same data as HOG and cross-entropy to obtain more information about the output distribution.

Data availability

The data that support the plots within this paper and other findings of this study are available from the corresponding author upon reasonable request.

References

36. Welch, L. & Berlekamp, E. Error correction for algebraic block codes. US patent 4,633,470 (1986).
37. Gemmell, P., Lipton, R., Rubinfeld, R., Sudan, M. & Wigderson, A. Self-testing/correcting for polynomials and for approximate functions. In *Proc. 23rd Annual ACM Symposium on Theory of Computing* (eds Koutsougeras, C. & Vitter, J. S.) 33–42 (ACM, 1991).
38. Valiant, L. The complexity of computing the permanent. *Theor. Comput. Sci.* **8**, 189–201 (1979).