REPORT

QUANTUM COMPUTING

Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1]*, Robert König[2]†

Quantum effects can enhance information-processing capabilities and speed up the solution of certain computational problems. Whether a quantum advantage can be rigorously proven in some setting or demonstrated experimentally using near-term devices is the subject of active debate. We show that parallel quantum algorithms running in a constant time period are strictly more powerful than their classical counterparts; they are provably better at solving certain linear algebra problems associated with binary quadratic forms. Our work gives an unconditional proof of a computational quantum advantage and simultaneously pinpoints its origin: It is a consequence of quantum nonlocality. The proposed quantum algorithm is a suitable candidate for near-future experimental realizations, as it requires only constant-depth quantum circuits with nearest-neighbor gates on a two-dimensional grid of qubits (quantum bits).

Quantum nonlocality—the fact that measurements of multiple spatially separated quantum systems can yield certain classically nonlocal correlations—is a remarkable feature of quantum mechanics. Its understanding was revolutionized by Bell, who recognized that this phenomenon can be experimentally verified (*1*). His work also prompted a shift in our approach to quantum mechanical systems: Modern quantum information science seeks to exploit quantum phenomena such as nonlocality, entanglement, and the superposition principle to tackle information-processing tasks that are believed to be difficult or impossible to achieve by purely classical means.

The potential benefits resulting from the use of quantum resources in computation are challenging to quantify. A major difficulty is the fact that the computational hardness of a given task for a classical computing device is not easy to assess. The strongest evidence that quantum computers may be more powerful than classical computers is the existence of quantum algorithms, such as Shor's efficient factoring algorithm (*2*), that achieve better performance than the best currently known classical algorithms for certain tasks. The appeal of Shor's algorithm relies on the conjecture that factoring cannot be achieved in polynomial time on a classical computer. Other existing proposals for quantum speed-ups [see, e.g., (*3*)] similarly rely on complexity-theoretic conjectures and, as a result, the potential for quantum advantage disappears if these conjectures turn out to be false (*4*). To sidestep this issue, one can instead work within the framework of so-called query complexity, in which, in addition to a classical or quantum computer, we are also given black-box access to an "oracle" operation whose internal structure cannot be examined. The computational task is to determine some property of the oracle, using the smallest possible number of queries to the oracle. Notable examples of quantum speed-ups obtained in terms of query complexity include quantum algorithms for unstructured search (*5*), element distinctness (*6*), and formula evaluation (*7*). Unfortunately, a speed-up proved in the oracular setting might not translate into a real-world advantage because the internal structure of an oracle may help to solve the problem classically.

A more practical concern is the fact that most proposed quantum algorithms are beyond current experimental capabilities: Their implementation requires a fully functional quantum computer incorporating error correction. Although the overhead for encoding and manipulating quantum data fault-tolerantly is asymptotically small (*8*, *9*), it remains prohibitive for current technology. Accordingly, it is expected that near-term quantum computers will lack error correction capabilities (*10*–*12*). A quantum computation without error correction can perform only a constant number of operations before the qubits decohere and the entropy builds up. This is evidenced by the impossibility of realizing passive quantum memories (amounting to the identity gate) when qubits experience independent noise with constant decoherence rate (*13*). This leads to an interesting trade-off between the number of qubits n and the depth d of quantum circuits that can be implemented on near-term hardware. Because the total number of operations is proportional to nd, quantum circuits with a large number of qubits that can potentially be hard to simulate classically are limited to a small depth.

This motivates the study of quantum parallel algorithms running in a constant time. These take as input a classical bit string, apply a constant-depth quantum circuit, and output a random bit string obtained by measuring each qubit in the 0,1 basis. By definition, a quantum circuit of depth d consists of d layers of one- and two-qubit gates, where gates within each layer act on disjoint sets of qubits. We assume that such disjoint gates can be applied in parallel. Constant-depth quantum circuits can therefore be implemented in a constant time, which is independent of the problem size or the number of qubits n. For brevity, we refer to such parallel constant-time quantum computations as shallow quantum circuits (SQCs).

Although SQCs constitute a highly restricted form of quantum computation, they are of central practical and theoretical importance. First, as discussed above, SQCs are among those forms of quantum computations most likely to be realized in the near future. Second, there are reasons to believe that SQCs may outperform classical circuits in certain tasks. The first evidence in this direction was provided in pioneering work (*14*) where it was argued that SQCs may be computationally hard to simulate classically. Quite recently, building on earlier studies of so-called instantaneous quantum polynomial-time circuits (*15*–*17*) and relying on complexity-theoretic assumptions, it was shown (*18*) that the output distribution of SQCs may be computationally hard to sample classically even if a constant statistical error is allowed [see also (*19*)]. Various models of computation closely related to SQCs have been studied (*20*–*26*).

Here, we compare the computational power of SQCs and their classical counterparts—that is, constant-depth classical (probabilistic) circuits. We present a simple linear algebra problem associated with binary quadratic forms that can be solved with certainty by a SQC composed of nearest-neighbor gates acting on a two-dimensional (2D) grid; this setup reflects near-term experimental abilities. At the same time,

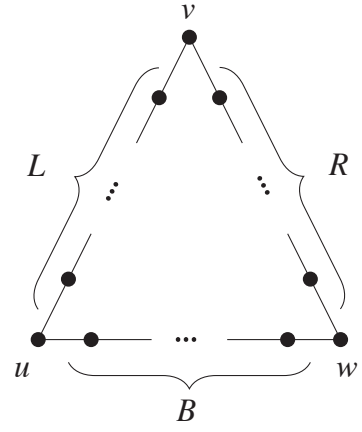

Fig. 1. Cycle graph Γ. Shown is a cycle Γ of even length M and three vertices u, v, w such that all pairwise distances are even. The sides L, R, B may have unequal lengths.

[1]IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA. [2]Technical University of Munich, 85748 Garching, Germany.
*Present address: Department of Combinatorics & Optimization and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.
†Corresponding author. Email: robert.koenig@tum.de

we prove that no constant-depth classical probabilistic circuit can solve the considered problem with a sufficiently small error probability for all instances. The classical circuit does not have to be geometrically local in any sense and may access random bits drawn from an arbitrary probability distribution that depends only on the input size. The only requirement is that all gates in the classical circuit must have bounded fan-in (i.e., each gate has a constant number of input wires). This result provides an unconditional separation between the power of constant-depth quantum and classical circuits.

The computational problem we use to establish the above separation can be viewed as a non-oracular variant of the well-known Bernstein-Vazirani problem (*27*). The latter involves a quantum oracle computing a linear function l: $\{0,1\}^n \to \{0,1\}$ such that $l(x) = \sum_{i=1}^{n} z_i x_i \pmod 2$ for some "hidden" bit string $z \in \{0,1\}^n$. The oracle is a unitary operator that can evaluate $l(x)$ on any superposition of inputs x. The task is to identify the hidden string z. As was shown in (*27*), the problem can be solved by a simple quantum algorithm making a single query to the oracle, whereas any classical algorithm with access to a classical oracle computing ℓ requires n queries to find z. To obtain a non-oracular variant of this problem, we ask: Where else—other than inside an oracle—can we hide a linear function?

We now explain how to hide a linear Boolean function inside a quadratic form. We consider quadratic forms q: $\{0,1\}^n \to \mathbb{Z}_4 = \{0,1,2,3\}$ defined as

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \pmod 4 \qquad (1)$$

where $x = (x_1, \ldots, x_n)$ is a vector of n binary variables and A is a symmetric binary matrix; that is, $A_{i,j} = A_{j,i} \in \{0,1\}$. Evaluation of $q(x)$ modulo 4 ensures that $q(x)$ depends only on the value of input variables modulo 2. As a consequence, many properties of real-valued quadratic forms carry over to the binary case considered here. We are interested in the case when x lies in the binary null-space of A,

$$\mathrm{Ker}(A) = \{x \in \{0,1\}^n : Ax = 0 \pmod 2\} \qquad (2)$$

Here and below, we consider x as a column vector. We write x^T for the transposed row vector. If x is a real vector and $q(x) = x^T A x$ is a real-valued quadratic form, then the restriction of $q(x)$ onto the null-space of A is clearly zero because $Ax = 0$ implies $q(x) = 0$. In the binary case, this is no longer true. However, we will see that the restriction of $q(x)$ onto the binary null-space of A is always a linear function. In other words, for any quadratic form $q(x)$ as above, there exists a (generally not unique) vector $z \in \{0,1\}^n$ such that

$$q(x) = 2 \sum_{i=1}^{n} z_i x_i \pmod 4 \text{ for all } x \in \mathrm{Ker}(A) \qquad (3)$$

[See (*28*) for the proof of Eq. 3.] Thus, one can say that the quadratic form $q(x)$ hides a linear function $l(x) = 2z^T x \pmod 4$, which is analogous to the hidden linear function in the Bernstein-Vazirani problem. However, in our case the form $q(x)$ is explicitly specified by its matrix of coefficients A, so there is no need for the oracle.

We consider the following hidden linear function (HLF) problem: Given an $n \times n$ symmetric binary matrix A specifying a quadratic form $q(x) = x^T A x$, which is evaluated modulo 4, find a binary vector $z \in \{0,1\}^n$ such that $q(x) = 2z^T x$ for all x in the binary null-space of A. [We note that any instance of the HLF problem (*29*) can be solved classically with $O(n^3)$ binary arithmetic operations by computing a basis of $\mathrm{Ker}(A)$ and evaluating $q(x)$ on each basis vector $x \in \mathrm{Ker}(A)$.]

An instance of the HLF problem can be alternatively described by a graph $G(A)$ with n vertices $i = 1, \ldots, n$ such that the off-diagonal part of A is the adjacency matrix of $G(A)$ and the nonzero entries on the diagonal of A specify a subset of marked vertices. Thus, by definition, a pair of vertices $i \neq j$ is connected by an edge if $A_{i,j} = 1$. We consider special instances of the HLF, where $n = N^2$ for some integer N and $G(A)$ is a subgraph of the square grid with $N \times N$ vertices. In other words, $A_{i,j} = 0$ unless i and j are nearest-neighbor vertices of the grid or $i = j$. Such instances constitute what we call the 2D HLF problem. As far as we are aware, the best classical algorithm that solves the 2D HLF problem requires $O(n^2)$ arithmetic operations (*30*).

A quantum algorithm solving the 2D HLF problem is similar to the one considered by Bernstein and Vazirani (*27*). Suppose first that one has access to a quantum circuit U_q acting on the basis states $x \in \{0,1\}^n$ as $U_q|x\rangle = i^{q(x)}|x\rangle$. Consider a system of n qubits and a quantum state

$$|\Psi_q\rangle = H^{\otimes n} U_q H^{\otimes n} |0\rangle^{\otimes n} = 2^{-n} \sum_{x,z \in \{0,1\}^n} i^{q(x)} (-1)^{z^T x} |z\rangle \qquad (4)$$

where

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad (5)$$

is the Hadamard gate. It can be easily checked that destructive interference between different terms x in Eq. 4 results in a vanishing amplitude $\langle z|\Psi_q\rangle = 0$ on basis states z that are not solutions of the HLF problem. Conversely, all solutions z appear in the state $|\Psi_q\rangle$ with nonzero amplitudes (*28*). Therefore, measuring each qubit of $|\Psi_q\rangle$ in the standard basis produces a random bit string z that is a solution of the HLF problem. The circuit U_q can be decomposed into a product of controlled-Z gates CZ and phase-shift gates S defined as

$$S_j|x\rangle = i^{x_j}|x\rangle$$
$$CZ_{i,j}|x\rangle = (-1)^{x_i x_j}|x\rangle \qquad (6)$$

Here, the subscripts i, j indicate qubits acted upon by the gate. Indeed, applying a $CZ_{i,j}$ gate for each pair of qubits such that $A_{i,j} = 1$ and applying an S_i gate for each qubit such that $A_{i,i} = 1$ gives U_q.

Let us consider the quantum resources required to implement the circuit U_q. We place the ith qubit at the ith vertex of the graph $G(A)$ embedded into a 2D grid. Then U_q contains only nearest-neighbor CZ gates and single-qubit S gates.

One can decompose the CZ part of U_q into four layers of CZ gates such that each layer is a depth-one circuit composed of pairwise disjoint CZ gates. This shows that U_q is a constant-depth quantum circuit. The above algorithm can be easily converted into a SQC by adding ancillary qubits that store the input matrix A and replacing each gate of U_q by its controlled version. We envision each input bit $A_{i,j}$ as being provided at the edge $\{i, j\}$ and each bit $A_{i,i}$ at the vertex i of the 2D grid. Then each gate in the controlled version of U_q acts on at most three qubits located on the same edge or the same vertex of the grid. Hence, the 2D HLF can be solved with certainty by a SQC with geometrically local gates on a 2D grid.

The above algorithm can be alternatively described as a sequence of single-qubit Pauli measurements performed on the graph state (*31*, *32*) associated with the graph $G(A)$. The latter is a quantum state of n qubits defined as

$$|\Psi_{G(A)}\rangle = \prod_{1 \le i < j \le n} CZ_{i,j}^{A_{i,j}} \cdot H^{\otimes n} |0\rangle^{\otimes n} \qquad (7)$$

Here, a CZ gate is applied for every edge of the graph $G(A)$. We claim that a solution z of the HLF problem can be obtained by preparing the graph state $|\Psi_{G(A)}\rangle$ and measuring each qubit i in either the X basis (if $A_{i,i} = 0$) or the Y basis (if $A_{i,i} = 1$). Indeed, a comparison of Eqs. 4 and 7 reveals that $|\Psi_q\rangle$ can be obtained from $|\Psi_{G(A)}\rangle$ by applying a gate S_i to each qubit i with $A_{i,i} = 1$ and applying a layer of n Hadamard gates. Furthermore, because the states Ψ_q and $\Psi_q{}^*$ (the complex conjugate of Ψ_q) give rise to the same measurement statistics in the Z basis, one can replace all gates S_i by their complex conjugates $S_i{}^* = S_i{}^3$. The above claim then follows from the identities $ZH = HX$ and $Z(HS^3) = (HS^3)Y$.

To understand the difficulty of solving the 2D HLF problem using classical circuits, recall that such a circuit is specified by a directed acyclic graph in which each vertex is either an input (if it has in-degree 0), an output (if it has out-degree 0), or a gate. For each gate we must also specify a Boolean function $\{0,1\}^k \to \{0,1\}$ that is computed by the gate, where k is the in-degree or "fan-in" of the gate. The output bit computed by a gate is copied to all outgoing edges of this gate. The out-degree or "fan-out" of a gate is the number of times the output of the gate is used in the remainder of the circuit. The depth d of a classical circuit is the maximum number of gates along a path from an input (variable) to an output. We are interested in circuits $\mathcal{C}$ with constant depth $d = O(1)$ such that all gates have fan-in at most $K = O(1)$.

The structure of such a circuit $\mathcal{C}$ imposes severe restrictions on the form of correlations present between the input (*33*) $x \in \{0,1\}^m$ and outputs $z = F(x) \in \{0,1\}^n$, where F is the function computed by $\mathcal{C}$. Let us say that the input bit (variable) x_j is correlated with the output bit (variable) z_k if and only if there is some $y \in \{0,1\}^m$ such that flipping the jth bit of y flips the kth bit of $F(y)$. Then the function F computed by $\mathcal{C}$ is local in the sense that each output bit can only be correlated with a constant number of input bits. Indeed, defining the ("backward") lightcone of the output bit z_k as the set $L_{\mathcal{C}}(z_k)$ of input variables x_j correlated with z_k, we have the obvious inequality

$$|L_{\mathcal{C}}(z_k)| \leq K^d \quad \text{for all output bits } z_k \qquad (8)$$

Similarly, we can argue [see claim 5 in (*28*)] that a constant fraction of input bits x_j have a small ("forward") lightcone $L_{\mathcal{C}}(x_j)$. The latter is the set of output variables z_k correlated with x_j. We will see that locality restrictions of this kind ultimately prevent solution of the 2D HLF by constant-depth classical circuits.

To understand why, recall that correlations present in the measurement statistics of entangled quantum states exhibit quantum nonlocality. A famous illustration (*34*, *35*) of this phenomenon is based on the three-qubit GHZ state $|\mathrm{GHZ}\rangle = (1/\sqrt{2})(|000\rangle + |111\rangle)$. Let $b \in \{0,1\}^3$ and consider the measurement outcomes $z \in \{0,1\}^3$ obtained by measuring each qubit j of $|\mathrm{GHZ}\rangle$ in either the X basis (if $b_j = 0$) or the Y basis (if $b_j = 1$). Then the measurement statistics satisfy

$$i^{b_1+b_2+b_3}(-1)^{z_1+z_2+z_3} = 1 \quad \text{whenever} \quad b_1 \oplus b_2 \oplus b_3 = 0. \qquad (9)$$

In contrast, it is well known (*35*) that Eq. 9 cannot be satisfied by a local hidden-variable model in which every output bit z_j is a function only of the local measurement setting b_j and some shared random string r, that is, $z_j = z_j(b_j, r)$. A local hidden-variable model can equivalently be viewed as a strictly local classical circuit in which every output bit depends only on one input bit (as well as the shared random string). Thus, rephrasing the GHZ example in terms of circuits, we conclude that a strictly local, possibly randomness-assisted classical circuit cannot solve the relational problem of producing a string $z \in \{0,1\}^3$ satisfying Eq. 9 for any input $b \in \{0,1\}^3$.

Our main technical contribution is a proof that this type of quantum nonlocality provides a relational problem that cannot be solved by general constant-depth classical circuits in the case when the GHZ state is replaced by the graph state defined in Eq. 7. To arrive at this result, we first consider 1D instances of the HLF problem and show that a constant-depth classical circuit with geometrically local gates cannot solve all such instances. We then use this result to show that a classical circuit that is "constant-depth local" (in the sense of having constant-size backward lightcones) cannot solve all instances of the 2D HLF problem.

Our starting point is an extension of the GHZ example described in (*36*). It shows that the statistics of single-qubit X and Y measurements performed on the graph state $|\Psi_\Gamma\rangle$ corresponding to a cycle graph Γ possess geometrically nonlocal correlations. In other words, certain measurement outcomes are correlated with measurement settings (i.e., choice of single-qubit measurement bases) that are far away with respect to the shortest path on the cycle. As a consequence, low-depth classical circuits that are geometrically local in one dimension cannot reproduce these statistics. Because the considered Pauli measurements are identical to those required to solve instances of the HLF problem on the cycle graph, we conclude that these instances cannot be solved by geometrically local constant-depth classical circuits.

In more detail, let Γ be a cycle graph of even length M and let Δ be the adjacency matrix of Γ. Suppose u, v, w are vertices of Γ such that all pairwise distances between them are even (Fig. 1). We define the distance $\mathrm{dist}_\Gamma(j, k)$ between any two vertices j, k to be the number of edges in the shortest path between them in Γ. Given a string $b = b_u b_v b_w \in \{0,1\}^3$, we can write $0^{M-3}b \in \{0,1\}^M$ for the string that associates the bits b_u, b_v, b_w to the vertices u, v, w and the value 0 to all other vertices. Let Δ_b be a matrix obtained from Δ by placing the string $0^{M-3}b$ on the main diagonal. This defines eight instances of the HLF problem on the cycle graph Γ with $A = \Delta_b$ and $b \in \{0,1\}^3$. Each instance has M output bits $z_1, \ldots, z_M$. In (*28*) we show that any classical randomness-assisted circuit $\mathcal{C}$ that solves all eight instances Δ_b with probability of at least ⅞ is geometrically nonlocal: The lightcone $L_{\mathcal{C}}(b_i)$ of at least one of the input bits $b_i \in \{b_u, b_v, b_w\}$ contains an output bit z_q such that $\mathrm{dist}_\Gamma(i,q) \geq \frac{1}{2}D_\Gamma(\{u, v, w\})$, where $D_\Gamma(\{u, v, w\})$ is the minimum pairwise distance between two vertices in the set $\{u, v, w\}$. The proof of this intermediate result proceeds by establishing a relation analogous to Eq. 9 for the graph state $|\Psi_\Gamma\rangle$ [similar to (*36*); see (*28*)].

Now consider the more general family of constant-depth classical circuits, which may not be geometrically local. Here, the HLF associated with the cycle graph Γ is not suitable for establishing our desired separation. Classical constant-depth circuits can communicate values b_u, b_v, b_w of input bits to distant locations in the cycle Γ and solve the HLF in this case essentially by simulating geometric nonlocality. We thus turn to the 2D HLF problem: We establish that the correlations between the input A and the solutions z in the 2D HLF problem have a strong form of nonlocality that cannot be reproduced by constant-depth randomness-assisted classical circuits of bounded fan-in. The key difference relative to the cycle graph setting is that the underlying graph $G(A)$ in the problem is also varied. Our main technical result is the following lower bound, which is valid for all sufficiently large N: If a classical circuit $\mathcal{C}_N$ with fan-in at most K solves all $N \times N$ instances of the 2D HLF problem with probability greater than ⅞, then the depth of $\mathcal{C}_N$ is at least $[1/(8 \log K)] \log N$.

Thus, no constant-depth circuit with bounded fan-in can solve all instances of the 2D HLF problem with high probability. The full proof of this result is given in (*28*). It proceeds by contradiction. Suppose a small-depth circuit $\mathcal{C}_N$ with bounded fan-in solves all size-N instances of the 2D HLF. To conform with the previous notations, we write $b_i \equiv A_{i,i}$ for the diagonal elements of A. We restrict our attention to instances A where $G(A)$ is a subgraph Γ of the 2D grid chosen in a particular way (depending on $\mathcal{C}_N$) such that

1) Γ is an even length cycle of length proportional to N,

2) There are vertices u, v, w on Γ, with even pairwise distances at least proportional to N, and

3) Any output bit z_q lying on the cycle Γ and correlated with one of the input bits b_u, b_v, b_w must be located in a small neighborhood of this input bit (of size proportional to $N^{1/2}$).

We establish the existence of such a cycle Γ by a probabilistic argument. Informally, restricting $\mathcal{C}_N$ to the instances of the HLF defined above gives rise to a certain geometrically local structure, as described by condition 3. However, such a geometrically local structure can be ruled out using the example of the HLF on the cycle graph. Indeed, in the latter case we have already shown that the lightcone of at least one input bit $b_i \in \{b_u, b_v, b_w\}$ must contain an output bit z_q located far from b_i, such that $\mathrm{dist}_\Gamma(i,q) \geq \frac{1}{2}D_\Gamma(\{u, v, w\})$. This contradicts condition 3 because $D_\Gamma(\{u, v, w\})$ is proportional to N. Thus, we obtain the desired lower bound on the depth of $\mathcal{C}_N$. This lower bound can be viewed as a worst-case hardness result, as we assume that the classical circuit solves all instances of the problem. In (*28*), we provide an analogous average-case hardness result that assumes only that the classical circuit solves a constant fraction of instances from a suitable random ensemble.

Our result constitutes a provable separation between analogously defined classical and quantum computational models that uses quantum nonlocality in answering a complexity-theoretic question. Our quantum circuit for the 2D HLF problem, which uses only classically controlled Clifford gates in a 2D geometry, is a promising target for future experimental demonstration of a quantum algorithm with provably better scaling (in terms of circuit depth) than any classical algorithm. Future theoretical work may address the question of minimizing resource requirements for practical demonstrations of such a quantum advantage, and may incorporate methods of fault tolerance tailored to hardware architectures of interest.

REFERENCES AND NOTES

1. J. S. Bell, *Physics* **1**, 195–200 (1964).
2. P. W. Shor, *SIAM Rev.* **41**, 303–332 (1999).
3. A. Montanaro, *NPJ Quantum Inf.* **2**, 15023 (2016).
4. Separations between quantum and classical information processing have been established in the area of communication complexity (*37*, *38*), but computational restrictions of communicating nodes are typically not considered in that field.
5. L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (ACM, 1996), pp. 212–219.
6. A. Ambainis, *SIAM J. Comput.* **37**, 210–239 (2007).

7. B. W. Reichardt, R. Spalek, in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing* (ACM, 2008), pp. 103–112.
8. D. Gottesman, *Quantum Inf. Comput.* **14**, 1338–1371 (2014).
9. H. Bombín, *New J. Phys.* **17**, 083002 (2015).
10. K. Temme, S. Bravyi, J. M. Gambetta, *Phys. Rev. Lett.* **119**, 180509 (2017).
11. Y. Li, S. C. Benjamin, *Phys. Rev. X* **7**, 021050 (2017).
12. S. Boixo *et al.*, *Nat. Phys.* **14**, 595–600 (2018).
13. F. Pastawski, A. Kay, N. Schuch, I. Cirac, *Phys. Rev. Lett.* **103**, 080501 (2009).
14. B. M. Terhal, D. P. DiVincenzo, *Quantum Inf. Comput.* **4**, 134–145 (2004).
15. M. J. Bremner, A. Montanaro, D. J. Shepherd, *Phys. Rev. Lett.* **117**, 080501 (2016).
16. M. J. Bremner, A. Montanaro, D. J. Shepherd, *Quantum* **1**, 8 (2017).
17. E. Farhi, A. W. Harrow, arXiv:1602.07674 [quant-ph] (24 February 2016).
18. J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, J. Eisert, *Phys. Rev. X* **8**, 021010 (2018).
19. X. Gao, S.-T. Wang, L.-M. Duan, *Phys. Rev. Lett.* **118**, 040502 (2017).
20. C. Moore, M. Nilsson, *SIAM J. Comput.* **31**, 799–815 (2001).
21. R. Cleve, J. Watrous, in *Proceedings, 41st Annual Symposium on Foundations of Computer Science* (IEEE, 2000), pp. 526–536.
22. P. Høyer, R. Špalek, *Theory Comput.* **1**, 83–101 (2005).
23. D. Browne, E. Kashefi, S. Perdrix, in *Conference on Quantum Computation, Communication, and Cryptography* (Springer, 2010), pp. 35–46.
24. L. Eldar, A. W. Harrow, in *58th Annual Symposium on Foundations of Computer Science* (IEEE, 2017), pp. 427–438.
25. S. Aaronson, *Proc. R. Soc. London Ser. A* **461**, 3473–3482 (2005).
26. S. Aaronson, L. Chen, in *Proceedings of the 32nd Computational Complexity Conference* (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2017), pp. 22:1–22:67.
27. E. Bernstein, U. Vazirani, *SIAM J. Comput.* **26**, 1411–1473 (1997).
28. See supplementary materials.
29. Our analysis [see Lemma 2 in (*28*)] also shows that the HLF problem can be regarded as a non-oracular variant of the "Fourier Fishing problem" introduced in (*39*), where the task is to find a nonzero Fourier coefficient of a function. In our case, the function of interest is $x \rightarrow i^{q(x)}$.
30. Because our quantum algorithm for the 2D HLF problem only involves classically controlled Clifford gates applied to an initial stabilizer state, it can be simulated classically using the Gottesman-Knill theorem (*40*, *41*). Imagine an "active window" W of width $O(1)$ that sweeps through the $N \times N$ lattice from left to right. At each step of the simulation, we measure qubits in the leftmost column of W in the appropriate basis (X or Y), shift W one column to the right, and then apply CZ gates near the right boundary of W to incorporate a newly arrived column of qubits into the graph state. Note that all qubits outside of W are unentangled: Qubits on the left have been already measured, and qubits on the right have not yet been incorporated into the graph state. Thus, the Gottesman-Knill simulator only needs to keep track of $O(N)$ qubits located in W, leading to a classical algorithm using $O(N^4) = O(n^2)$ arithmetic operations.
31. R. Raussendorf, D. E. Browne, H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
32. M. Hein, J. Eisert, H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
33. Our results also hold for probabilistic circuits in which a subset of input bits may be chosen at random; that is, $x = x'r$, where $r \in \{0,1\}^{\ell}$ is a random string drawn from some (arbitrary) distribution $\rho(r)$ and $x' \in \{0,1\}^{m-\ell}$.
34. D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger, *Am. J. Phys.* **58**, 1131–1143 (1990).
35. N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838–1840 (1990).
36. J. Barrett, C. M. Caves, B. Eastin, M. B. Elliott, S. Pironio, *Phys. Rev. A* **75**, 012103 (2007).
37. G. Brassard, *Found. Phys.* **33**, 1593–1616 (2003).
38. R. de Wolf, *Theor. Comput. Sci.* **287**, 337–353 (2002).
39. S. Aaronson, in *Proceedings of the 42nd ACM Symposium on Theory of Computing* (ACM, 2010), pp. 141–150.
40. D. Gottesman, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics* (International Press, 1999), pp. 32–43.
41. S. Aaronson, D. Gottesman, *Phys. Rev. A* **70**, 052328 (2004).

ACKNOWLEDGMENTS

We thank the anonymous referees for their comments. **Funding:** Supported by the IBM Research Frontiers Institute (S.B. and D.G.) and by the Technical University of Munich–Institute for Advanced Study, funded by the German Excellence Initiative and the European Union Seventh Framework Programme under grant agreement 291763 (R.K.). **Author contributions:** S.B., D.G., and R.K. contributed equally to this work. **Competing interests:** None.

SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/362/6412/308/suppl/DC1
Supplementary Text
Figs. S1 and S2

24 October 2017; accepted 30 August 2018
10.1126/science.aar3106

Science

Quantum advantage with shallow circuits

Sergey Bravyi, David Gosset and Robert König

Science **362** (6412), 308-311.
DOI: 10.1126/science.aar3106

Quantum outperforms classical

Quantum computers are expected to be better at solving certain computational problems than classical computers. This expectation is based on (well-founded) conjectures in computational complexity theory, but rigorous comparisons between the capabilities of quantum and classical algorithms are difficult to perform. Bravyi *et al.* proved theoretically that whereas the number of "steps" needed by parallel quantum circuits to solve certain linear algebra problems was independent of the problem size, this number grew logarithmically with size for analogous classical circuits (see the Perspective by Montanaro). This so-called quantum advantage stems from the quantum correlations present in quantum circuits that cannot be reproduced in analogous classical circuits.

Science, this issue p. 308; see also p. 289