www.sciencemag.org/content/362/6412/308/suppl/DC1

Supplementary Materials for

Quantum advantage with shallow circuits

Sergey Bravyi, David Gosset, Robert König*

*Corresponding author. Email: robert.koenig@tum.de

Published 19 October 2018, *Science* **362**, 308 (2018)
DOI: 10.1126/science.aar3106

This PDF file includes:

Supplementary Text
Figs. S1 and S2

A The hidden linear function problem

In this section, we argue that the HLF problem is well-posed. Let $q : \{0,1\}^n \to \mathbb{Z}_4$ be a quadratic form as in Eq. (1). For brevity, we shall write $\mathcal{L}_q = \mathrm{Ker}(A)$ for the null-space defined by Eq. (2). Then the following holds.

Lemma 1. *The restriction of q to $\mathcal{L}_q$ is a linear function, that is, there exists a vector $z \in \{0,1\}^n$ such that $q(x) = 2z^T x \pmod 4$ for all $x \in \mathcal{L}_q$.*

Proof. Simple algebra shows that

$$q(x \oplus y) = q(x) + q(y) + 2y^T A x \pmod 4 \qquad \text{for all } x, y \in \{0,1\}^n.$$

Here $x \oplus y$ denotes addition of binary strings modulo two. By definition, $x \in \mathcal{L}_q$ implies $Ax = 0 \pmod 2$ and thus $2Ax = 0 \pmod 4$. Therefore,

$$q(x \oplus y) = q(x) + q(y) \pmod 4 \qquad \text{for all } x \in \mathcal{L}_q \text{ and for all } y \in \{0,1\}^n. \tag{S1}$$

In particular, $0 = q(0) = q(x \oplus x) = 2q(x) \pmod 4$ for any $x \in \mathcal{L}_q$, that is, $q(x) \in \{0,2\}$. Define a function $l : \mathcal{L}_q \to \{0,1\}$ by

$$l(x) = \begin{cases} 1 & \text{if} \quad q(x) = 2, \\ 0 & \text{if} \quad q(x) = 0. \end{cases}$$

From Eq. (S1) one infers that $l(x)$ is linear modulo two,

$$l(x \oplus y) = l(x) \oplus l(y) \qquad \text{for all } x, y \in \mathcal{L}_q.$$

It follows that $l(x) = z^T x \pmod 2$ for some $z \in \{0,1\}^n$. Thus $q(x) = 2z^T x$ for all $x \in \mathcal{L}_q$. □

The linear action of q on the subspace $\mathcal{L}_q$ can be thus be parameterized by a "hidden" bit string $z \in \{0,1\}^n$, which is a solution to the HLF specified by q. In contrast with the Bernstein-Vazirani problem, here z is not unique because the hidden linear function is only defined on a subspace of $\{0,1\}^n$. To see this, let $\mathcal{L}_q^\perp$ be the orthogonal complement of $\mathcal{L}_q$. Then for any solution z of the HLF, and any $y \in \mathcal{L}_q^\perp$, $z \oplus y$ is also a solution to the HLF (since $2(z \oplus y)^T x = 2z^T x + 2y^T x = 2z^T x$ for $x \in \mathcal{L}_q$).

We remark here that the non-uniqueness of the solution an HLF instance is no coincidence, but a necessary feature of any problem separating constant-depth quantum from constant-depth classical circuits. To see this, consider a problem which has a unique solution $z = (z_1, \ldots, z_n) = f(A) \in \{0,1\}^n$ for any input $A \in \{0,1\}^{m(n)}$, that is, the problem of function evaluation. If a constant-depth quantum circuit achieving this task is given, this implies that each output bit z_j only depends on a constant number of input bits of A, and can thus be computed by a constant-size classical circuit. Applying this to every output bit – i.e., parallelizing this computation – implies that z can be computed from A using a constant-depth classical circuit.

B Analysis of the quantum algorithm

Here we show that the proposed quantum algorithm produces solutions $z \in \{0,1\}^n$ of the HLF problem.

Let $p(z)$ be the distribution over outcomes $z \in \{0,1\}^n$ produced by the quantum algorithm. From Eq. (4) in the main text one gets

$$p(z) = 4^{-n} \left| \sum_{x \in \{0,1\}^n} i^{q(x)} (-1)^{z^T x} \right|^2 . \tag{S2}$$

Lemma 2. $p(z) > 0$ *if and only if* z *is a solution of the HLF problem. Furthermore,* $p(z)$ *is the uniform distribution on the set of all solutions* z*.*

Proof. For any linear subspace $\mathcal{L} \subseteq \{0,1\}^n$ and a vector $z \in \{0,1\}^n$ define a partial Fourier transform

$$\Gamma(\mathcal{L}, z) \equiv \sum_{x \in \mathcal{L}} (-1)^{z^T x} \cdot i^{q(x)}.$$

Then

$$p(z) = \frac{1}{4^n} \left| \Gamma(\{0,1\}^n, z) \right|^2 . \tag{S3}$$

Choose any linear subspace $\mathcal{K} \subseteq \{0,1\}^n$ such that

$$\{0,1\}^n = \mathcal{L}_q + \mathcal{K} \quad \text{and} \quad \mathcal{L}_q \cap \mathcal{K} = 0. \tag{S4}$$

From Eq. (S1) one infers that

$$\Gamma(\{0,1\}^n, z) = \Gamma(\mathcal{L}_q, z) \cdot \Gamma(\mathcal{K}, z). \tag{S5}$$

The statement of lemma 2 follows directly from Eqs. (S3,S5) and the following Claims 1,2. $\square$

Claim 1. *$\Gamma(\mathcal{L}_q, z) = |\mathcal{L}_q|$ if z is a solution of the HLF problem and $\Gamma(\mathcal{L}_q, z) = 0$ otherwise. The number of solutions to the HLF problem is $|\mathcal{L}_q^\perp|$.*

Proof. By Lemma 1 there exists a vector $y \in \{0,1\}^n$ such that $q(x) = 2y^T x$ for all $x \in \mathcal{L}_q$. Then $i^{q(x)} = (-1)^{y^T x}$ and thus

$$\Gamma(\mathcal{L}_q, z) = \sum_{x \in \mathcal{L}_q} (-1)^{x^T(y \oplus z)} = \begin{cases} |\mathcal{L}_q| & \text{if} \quad y \oplus z \in \mathcal{L}_q^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the first case, $y \oplus z \in \mathcal{L}_q^\perp$, occurs iff z is a solution of the HLF problem, since y and z have the same binary inner product with any vector from $\mathcal{L}_q$ iff $y \oplus z \in \mathcal{L}_q^\perp$. Therefore the number of solutions is $|\mathcal{L}_q^\perp|$. $\square$

Claim 2. *$|\Gamma(\mathcal{K}, z)|^2 = 2^n \cdot |\mathcal{L}_q|^{-1}$ for all $z \in \{0,1\}^n$.*

Proof. We claim that for any $z \in \{0,1\}^n$ there exists a vector $w \in \mathcal{K}$ such that

$$z^T x = w^T A x \quad \text{for all} \quad x \in \mathcal{K}. \tag{S6}$$

Indeed, note that $(\mathcal{X} \cap \mathcal{Y})^\perp = \mathcal{X}^\perp + \mathcal{Y}^\perp$ for any linear subspaces $\mathcal{X}, \mathcal{Y} \subseteq \{0,1\}^n$. Let $\mathrm{Im}(A) \equiv \mathrm{span}\{Ax \, : \, x \in \{0,1\}^n\}$. Using the identity

$$\mathrm{Ker}(A)^\perp = \mathrm{Im}(A^T) = \mathrm{Im}(A)$$

and taking the dual of $\mathcal{L}_q \cap \mathcal{K} = 0$, see Eq. (S4) gives

$$\mathrm{Im}(A) + \mathcal{K}^\perp = \{0,1\}^n \tag{S7}$$

Choose any vector $z \in \{0,1\}^n$ and write it as

$$z = u \oplus v, \quad \text{where} \quad u \in \mathrm{Im}(A) \quad \text{and} \quad v \in \mathcal{K}^\perp.$$

This is always possible due to Eq. (S7). Let $u = Au'$ for some $u' \in \{0,1\}^n$. From Eq. (S4) we infer that $u' = w \oplus w'$ for some $w \in \mathcal{K}$ and $w' \in \mathcal{L}_q$. Putting together the above facts we see that any vector $z \in \{0,1\}^n$ can be written as

$$z = Au' \oplus v = A(w \oplus w') \oplus v, \quad \text{where} \quad w \in \mathcal{K}, \quad w' \in \mathcal{L}_q, \quad v \in \mathcal{K}^\perp.$$

Note that $Aw' = 0$ since, by definition, $\mathcal{L}_q$ is the nullspace of A. Thus $z^T x = w^T A x$ for all $x \in \mathcal{K}$, as claimed in Eq. (S6). From Eqs. (S1,S6) one gets

$$(-1)^{z^T x} \cdot i^{q(x)} = (-1)^{w^T A x} \cdot i^{q(x)} = i^{q(w\oplus x) - q(w)} \qquad \text{for all } x \in \mathcal{K}.$$

Therefore

$$\Gamma(\mathcal{K}, z) = \sum_{x\in\mathcal{K}} (-1)^{z^T x} \cdot i^{q(x)} = i^{-q(w)} \cdot \sum_{x\in\mathcal{K}} i^{q(w\oplus x)} = i^{-q(w)} \cdot \sum_{x\in\mathcal{K}} i^{q(x)}.$$

This shows that the absolute value of $\Gamma(\mathcal{K}, z)$ does not depend on z. Let $C \equiv |\Gamma(\mathcal{K}, z)|^2$. Combining Eqs. (S3,S5) and Claim 1 one gets

$$1 = \sum_{z\in\{0,1\}^n} p(z) = \frac{|\mathcal{L}_q^\perp| \cdot |\mathcal{L}_q|^2 \cdot C}{4^n} = \frac{|\mathcal{L}_q| \cdot C}{2^n},$$

which proves the claim. □

C Non-locality thwarts constant-depth classical circuits

In this section we show that quantum nonlocality–even in states generated by constant-depth quantum circuits– thwarts simulation by classical circuits which are (I) geometrically local in one dimension, and finally (II) "constant-depth local" in the sense of Eq. (8). In more detail, in Section C.1, we show that geometrically local constant-depth classical circuits fail to solve the HLF associated with a cycle graph. In Section C.2, we then lift the assumption of geometric locality: we show that any constant-depth classical circuit fails to solve certain instances of the 2D HLF.

In the remaining sections it will be more convenient to describe an instance of the HLF problem by a pair (A, b) where A is a symmetric binary matrix with *zero diagonal* and $b \in \{0,1\}^n$ is a bit string such that

$$q(x) = x^T A x + b^T x \pmod 4.$$

This is equivalent to the definition given in the main text since $x_i^2 = x_i$ for binary x_i. Recall that the quantum algorithm solving the HLF problem can be converted to a sequence of single-qubit Pauli X and Y measurements performed on the graph state $|\Psi_{G(A)}\rangle$ defined in Eq. (7). Here $G(A)$ is a graph with n vertices and the adjacency matrix A. The i-th qubit is measured in the X basis if $b_i = 0$ and the Y basis if $b_i = 1$. Let $z_i \in \{0, 1\}$ be the measurement outcome. From Lemma 2 we infer that $z = (z_1, \ldots, z_n)$ is a random uniformly distributed solution of the corresponding HLF problem.

C.1 Geometric non-locality in the cycle graph and the HLF

Here we consider instances of the HLF associated with the M-cycle graph Γ with M even (as in Fig. 1). We briefly recall our notation: Let Δ be a binary matrix such that $\Gamma = G(\Delta)$, and let u, v, w be vertices of Γ such that all pairwise distances between them are even. We denote by

$$D = D(\{u, v, w\}) := \min\{\mathrm{dist}_\Gamma(u, v), \mathrm{dist}_\Gamma(v, w), \mathrm{dist}_\Gamma(u, w)\}\,. \tag{S8}$$

the minimum pairwise distance between two vertices in the set $\{u, v, w\}$.

For $b = b_u b_v b_w \in \{0, 1\}^3$ we 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. Finally, let us write $\mathsf{sol}(\Delta, 0^{M-3}b) \subset \{0, 1\}^n$ for the set of solutions to the instance $(\Delta, 0^{M-3}b)$ of the HLF problem. We then have the following statement:

Lemma 3. *Consider a classical randomness-assisted circuit $\mathcal{C}$ which takes as input a bit string $b = b_u b_v b_w \in \{0, 1\}^3$ and a random string $r \in \{0, 1\}^\ell$ (drawn from some distribution ρ) and outputs $z = z(b, r) \in \{0, 1\}^M$. Suppose*

$$\mathrm{Prob}\left[z(b, r) \in \mathsf{sol}(\Delta, 0^{M-3}b)\right] > \frac{7}{8} \qquad \textit{for all } b \in \{0, 1\}^3\,. \tag{S9}$$

Then the lightcone $L_{\mathcal{C}}(b_i)$ of one of the input bits $b_i \in \{b_u, b_v, b_w\}$ contains an output bit z_q such that $\mathrm{dist}_\Gamma(i, q) \geq D/2$.

Recall from Lemma 2 that $\mathsf{sol}(\Delta, 0^{M-3}b)$ is the set of possible measurement outcomes when measuring the 1D graph state (with measurement settings determined at $\{u, v, w\}$ determined by

b). To prove Lemma 3, we first show that these measurement outcomes satisfy an identity similar to Eq. (9), see Eq. (S10) below.

We shall say that a vertex j is even (resp. odd) if it has even distance (resp. odd distance) from u, v, w. Let L, R, B be the set of vertices for each of the three sides of the triangle Γ as shown in Fig. 1. The vertices u, v, w are not contained in any of these sets. Also define sets $R_{\mathrm{odd}}, R_{\mathrm{even}}$ of odd and even vertices respectively on side R of the triangle, and likewise $L_{\mathrm{odd}}, L_{\mathrm{even}}, B_{\mathrm{odd}}, B_{\mathrm{even}}$.

It will be convenient to work with ± 1-valued variables defined by $m_j = (-1)^{z_j}$ for $j \in \{1, 2, \ldots, M\}$. Define the following products:

$$m_L = \prod_{j \in L_{odd}} m_j \qquad m_R = \prod_{j \in R_{odd}} m_j \qquad m_B = \prod_{j \in B_{odd}} m_j \qquad m_E = \prod_{j \in R_{\mathrm{even}} \cup L_{\mathrm{even}} \cup B_{\mathrm{even}}} m_j. \tag{S10}$$

Claim 3. *Let* $b = b_u b_v b_w \in \{0,1\}^3$ *and suppose* $z \in \mathsf{sol}(\Delta, 0^{M-3}b)$. *Then* $m_R m_B m_L = 1$. *Moreover, if* $b_u \oplus b_v \oplus b_w = 0$ *then*

$$i^{b_u + b_v + b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = 1. \tag{S11}$$

Proof. Let $g_j = X_j \prod_{k:\{k,j\} \in E} Z_k$ be the stabilizer generator of the graph state $|\Phi_\Gamma\rangle$ associated with vertex j such that $g_j|\Phi_\Gamma\rangle = |\Phi_\Gamma\rangle$ for all j. For any subset $\mathcal{I} \subseteq [M]$ define operators

$$X(\mathcal{I}) = \prod_{j \in \mathcal{I}} X_j \quad \text{and} \quad g(\mathcal{I}) = \prod_{j \in \mathcal{I}} g_j$$

First note that the operator $X(R_{\mathrm{odd}} \cup L_{\mathrm{odd}} \cup B_{\mathrm{odd}})$ is in the stabilizer group of $|\Phi_\Gamma\rangle$. Indeed, we have

$$X(R_{\mathrm{odd}} \cup L_{\mathrm{odd}} \cup B_{\mathrm{odd}}) = g(R_{\mathrm{odd}} \cup L_{\mathrm{odd}} \cup B_{\mathrm{odd}}).$$

Accordingly, $|\Phi_\Gamma\rangle$ is in the $+1$ eigenspace of this operator. Therefore a measurement of each qubit in $R_{\mathrm{odd}} \cup L_{\mathrm{odd}} \cup B_{\mathrm{odd}}$ in the X basis will result in outcomes m_R, m_L, m_B satisfying $m_R m_B m_L = 1$

as claimed. The four cases of Eq. (S11) arise in the same way from the following elements of the stabilizer group of $|\Phi_\Gamma\rangle$:

$$
\begin{aligned}
&(b_u b_v b_w = 000) \qquad X_u X_v X_w \cdot X\big(R_{\text{even}} \cup L_{\text{even}} \cup B_{\text{even}}\big) = g(\{uvw\} \cup R_{\text{even}} \cup L_{\text{even}} \cup B_{\text{even}}) \\
&(b_u b_v b_w = 110) \qquad -Y_u Y_v X_w \cdot X\big(R \cup B \cup L_{\text{even}}\big) = g(\{uvw\} \cup R \cup B \cup L_{\text{even}}) \\
&(b_u b_v b_w = 101) \qquad -Y_u X_v Y_w \cdot X\big(R \cup L \cup B_{\text{even}}\big) = g(\{uvw\} \cup R \cup L \cup B_{\text{even}}) \\
&(b_u b_v b_w = 011) \qquad -X_u Y_v Y_w \cdot X\big(B \cup L \cup R_{\text{even}}\big) = g(\{uvw\} \cup B \cup L \cup R_{\text{even}}).
\end{aligned}
$$

□

Proof of Lemma 3. To reach a contradiction let us suppose that the hypotheses of the lemma are satisfied but the conclusion does not hold. That is, let $\mathcal{C}$ be a classical circuit satisfying Eq. (S9) and suppose that the lightcone $L_{\mathcal{C}}(b_u)$ only includes output bits z_j where $\mathrm{dist}_\Gamma(u, j) \leq D/2 - 1$ (and likewise for b_v and b_w). Therefore each output bit z_j only depends on the random string r as well as the nearest input bit b_u, b_v or b_w (if z_j is equidistant to two of them it depends on neither).

Write $z = F(b, r)$ for the function which is computed by the circuit $\mathcal{C}$. Below we show that for each r there exists a string $b \in \{0,1\}^3$ such that $F(b, r) \notin \mathsf{sol}(\Delta, 0^{M-3}b)$. This implies that when r is chosen at random from some distribution ρ we have

$$
\begin{aligned}
\frac{1}{8} \sum_{b \in \{0,1\}^3} \mathrm{Prob}_\rho \left[F(b,r) \in \mathsf{sol}(\Delta, 0^{M-3}b)\right] &= \frac{1}{8} \cdot \mathbb{E}_\rho \Big[\# \left\{b \in \{0,1\}^3 \;:\; F(b,r) \in \mathsf{sol}(\Delta, 0^{M-3}b)\right\}\Big] \\
&\leq \frac{7}{8}\,. \qquad \text{(S12)}
\end{aligned}
$$

This shows that $\mathrm{Prob}_\rho \left[F(b,r) \in \mathsf{sol}(\Delta, 0^{M-3}b)\right] \leq 7/8$ for some $b \in \{0,1\}^3$. Thus we arrive at a contradiction, which is sufficient to prove the Lemma.

It remains to show that for each r there exists a b such that $F(b,r) \notin \mathsf{sol}(\Delta, 0^{M-3}b)$. So let r be fixed and consider $z = F(b, r)$ as a function of b. Let $m_j = (-1)^{z_j}$ and consider the products defined in Eq. (S10) (as a function of b). Suppose first that $m_R m_B m_L = -1$ for some $b' \in \{0,1\}^3$. Then by Claim 3, $F(b', r) \notin \mathsf{sol}(\Delta, 0^{M-3}b')$ and we are done. Next suppose that $m_R m_B m_L = 1$ for all $b = b_u b_v b_w \in \{0,1\}^3$. Since each output bit z_j is a function only of the nearest input bit

b_u, b_v, b_w and we are considering products of values $(-1)^{z_j}$, there exist affine boolean functions $e, f, g, h : \{0,1\}^3 \to \{0,1\}$ such that

$$m_u m_v m_w m_E = (-1)^{e(b)} \qquad m_R = (-1)^{f(b)} \qquad m_B = (-1)^{g(b)} \qquad m_L = (-1)^{h(b)}$$

and such that $f(b)$ does not depend on b_u, $g(b)$ does not depend on b_v, $h(b)$ does not depend on b_w, and $f(b) \oplus g(b) \oplus h(b) = 0$. Note that

$$i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = i^{b_u+b_v+b_w}(-1)^{e(b)+f(b)b_u+g(b)b_v+h(b)b_w}. \tag{S13}$$

The following Claim 4 implies that there is a bit string $b \in \{0,1\}^3$ with even Hamming weight such that Eq. (S13) is not equal to $+1$. Applying Claim 3 we see that this implies that $F(b,r) \notin \mathsf{sol}(\Delta, 0^{M-3}b)$ for some (even Hamming weight) string $b \in \{0,1\}^3$, completing the proof. □

Claim 4. *Suppose* $e, f, g, h : \{0,1\}^3 \to \{0,1\}$ *are affine boolean functions. Write* $x = x_1x_2x_3 \in \{0,1\}^3$. *Suppose* $f(x)$ *does not depend on* x_1, $g(x)$ *does not depend on* x_2, $h(x)$ *does not depend on* x_3, *and that* $f(x) \oplus g(x) \oplus h(x)$ *is independent of* x. *Then*

$$\sum_{x_1 \oplus x_2 \oplus x_3 = 0} i^{x_1+x_2+x_3}(-1)^{e(x)+f(x)x_1+g(x)x_2+h(x)x_3} \leq 2.$$

Proof. Write

$$e(x) = e_0 \oplus e_1x_1 \oplus e_2x_2 \oplus e_3x_3 \qquad e_0, e_1, e_2, e_3 \in \{0,1\} \tag{S14}$$

$$f(x) = f_0 \oplus f_2x_2 \oplus f_3x_3 \qquad f_0, f_2, f_3 \in \{0,1\} \tag{S15}$$

$$g(x) = g_0 \oplus g_1x_1 \oplus g_3x_3 \qquad g_0, g_1, g_3 \in \{0,1\} \tag{S16}$$

$$h(x) = h_0 \oplus h_1x_1 \oplus h_2x_2. \qquad h_0, h_1, h_2 \in \{0,1\} \tag{S17}$$

Given this parametrization of the functions e, f, g, h, the claim could easily be verified by an exhaustive search. For convenience, however, we provide a proof which can be verified by hand. The fact that $f(x) \oplus g(x) \oplus h(x)$ is a constant function implies

$$f_2 \oplus h_2 = f_3 \oplus g_3 = g_1 \oplus h_1 = 0. \tag{S18}$$

We have

$$
\begin{aligned}
&f(x)x_1 + g(x)x_2 + h(x)x_3 \\
&\qquad = f_0x_1 + g_0x_2 + h_0x_3 + (f_2+g_1)x_1x_2 + (f_3+h_1)x_1x_3 + (g_3+h_2)x_2x_3. \qquad \text{(S19)}
\end{aligned}
$$

For all x satisfying $x_1 \oplus x_2 \oplus x_3 = 0$ we have $x_1x_3 = x_1x_2 \oplus x_1$ and $x_2x_3 = x_1x_2 \oplus x_2$. Using this fact and Eqs.(S19), (S18) we get

$$
(-1)^{f(x)x_1+g(x)x_2+h(x)x_3} = (-1)^{(f_0+f_3+h_1)x_1+(g_0+g_3+h_2)x_2+h_0x_3}
$$

whenever $x_1 \oplus x_2 \oplus x_3 = 0$. Noting that the exponent on the right hand side is an affine boolean function, and that $e(x)$ is also an affine boolean function we get

$$
\begin{aligned}
&\sum_{x_1\oplus x_2\oplus x_3=0} i^{x_1+x_2+x_3}(-1)^{e(x)+f(x)x_1+g(x)x_2+h(x)x_3} \\
&\qquad \le \max_{w\in\{0,1\}^4} \sum_{x_1\oplus x_2\oplus x_3=0} i^{x_1+x_2+x_3}(-1)^{w_0+w_1x_1+w_2x_2+w_3x_3} \qquad \text{(S20)} \\
&\qquad \le 2
\end{aligned}
$$

Since each summand in Eq. (S20) is ± 1, the last line is equivalent to the statement that the sum is strictly less than 4, which follows from the fact that the following system of equations over $\mathbb{F}_2$ has no solution:

$$
w_0 = 0 \qquad w_1 \oplus w_2 = 1 \qquad w_1 \oplus w_3 = 1 \qquad w_2 \oplus w_3 = 1. \qquad \text{(S21)}
$$

(Note that Eq. (S21) would be necessary for Eq. (S20) to be equal to 4, as can be seen by considering $x = x_1x_2x_3 \in \{000, 110, 101, 011\}$.) $\square$

C.2 Hardness of 2D HLF for constant-depth classical circuits

The following statement implies that there is no constant-depth classical circuit which solves all instances of the 2D HLF with certainty:

Theorem 1. *The following holds for all sufficiently large N. Let $\mathcal{C}_N$ be a classical probabilistic circuit with fan-in at most K which solves all size-N instances of the 2D Hidden Linear Function* *problem with probability greater than* $7/8$*. Then the depth of* $\mathcal{C}_N$ *is at least*

$$\frac{1}{8}\frac{\log(N)}{\log(K)}.$$

Proof. Let $\mathcal{C} \equiv \mathcal{C}_N$ be a classical probabilistic circuit of fan-in $\leq K$ which solves the 2D Hidden Linear Function problem with probability $> 7/8$ on all instances of size N. That is, the circuit $\mathcal{C}_N$ takes input A, b along with a random string r drawn from some (arbitrary) probability distribution and its output $z \in \{0,1\}^{N^2}$ must be a solution to the given instance with probability greater than $7/8$. We suppose that the depth d of $\mathcal{C}$ satisfies

$$d < \frac{1}{8}\frac{\log(N)}{\log(K)}. \tag{S22}$$

Below we prove that for all sufficiently large N (i.e., larger than some universal constant) this leads to a contradiction.

Suppose $q \in V$ is a vertex of the $N \times N$ grid $G = (V, E)$. Let $\mathrm{Box}(q) \subseteq V$ be a square box of size $\lfloor N^{1/2} \rfloor \times \lfloor N^{1/2} \rfloor$ centered at vertex q. Each box defines a subset of output variables z_j contained in this box. Choose square-shaped regions $\mathcal{U}, \mathcal{V}, \mathcal{W} \subseteq V$ as shown in Figure S1. Let $V_{\text{even}} \subset V$ denote the set of vertices on the even sublattice of the grid. In other words V_{even} contains all vertices with even horizontal and vertical coordinates.

Combining Eqs. (8,S22) we get

$$|L_{\mathcal{C}}(z_i)| \leq K^d < N^{\frac{1}{8}} \qquad i \in V. \tag{S23}$$

This shows that all output bits have "small" lightcones. Next we shall identify large sets of input bits which also have small lightcones.

For each region $\mathcal{R} \in \{\mathcal{U}, \mathcal{V}, \mathcal{W}\}$ define sets of good and bad vertices

$$\mathrm{Good}(\mathcal{R}) = \{v \in \mathcal{R} \cap V_{\text{even}} : |L_{\mathcal{C}}(b_v)| \leq N^{\frac{1}{4}}\} \tag{S24}$$

$$\mathrm{Bad}(\mathcal{R}) = (\mathcal{R} \cap V_{\text{even}}) \setminus \mathrm{Good}(\mathcal{R}). \tag{S25}$$

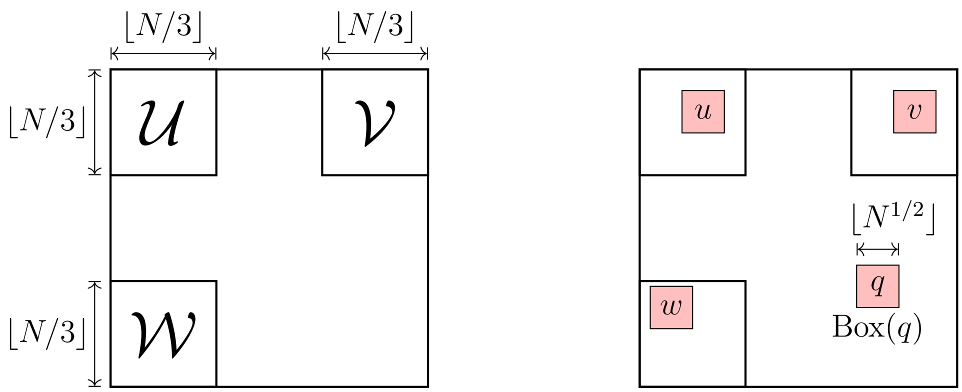

Figure S1: **Regions used in the proof.** Left: definition of the regions $\mathcal{U}, \mathcal{V}, \mathcal{W}$. Right: definition of $\mathrm{Box}(q)$ and a possible choice of vertices u, v, w.

Claim 5. *For* $\mathcal{R} \in \{\mathcal{U}, \mathcal{V}, \mathcal{W}\}$ *we have*

$$|\mathrm{Good}(\mathcal{R})| = \Omega(N^2) \qquad \textit{and} \qquad \frac{|\mathrm{Good}(\mathcal{R})|}{|\mathcal{R} \cap V_{even}|} \geq 1 - O(N^{-1/8}) \, . \tag{S26}$$

Proof. Define a bipartite graph with one side of the partition labeled by input bits b_v with $v \in \mathcal{R} \cap V_{\text{even}}$ and the other side labeled by outputs z_j with $j \in V$. An edge between z_j and b_v is present iff $b_v \in L_{\mathcal{C}}(z_j)$. The total number of edges J in this graph satisfies

$$|\mathrm{Bad}(\mathcal{R})| N^{\frac{1}{4}} \leq J \leq |V| \cdot \max_{i \in V} |L_{\mathcal{C}}(z_i)| \leq N^{\frac{17}{8}},$$

where we used $|V| = N^2$ and Eq. (S23). Rearranging gives $|\mathrm{Bad}(\mathcal{R})| \leq N^{\frac{15}{8}}$. Since $|\mathcal{R} \cap V_{\text{even}}| = \Theta(N^2)$ we get

$$|\mathrm{Good}(\mathcal{R})| = |\mathcal{R} \cap V_{\text{even}}| - |\mathrm{Bad}(\mathcal{R})| = \Omega(N^2)$$

as well as

$$\frac{|\mathrm{Good}(\mathcal{R})|}{|\mathcal{R} \cap V_{even}|} \geq 1 - \frac{|\mathrm{Bad}(\mathcal{R})|}{|\mathcal{R} \cap V_{even}|} \geq 1 - O(N^{-1/8}) \, .$$

□

Claim 6. *For all large enough* N *one can choose a triple of vertices* u, v, w *such that* $u \in \mathrm{Good}(\mathcal{U})$*,* $v \in \mathrm{Good}(\mathcal{V})$*,* $w \in \mathrm{Good}(\mathcal{W})$ *and*

$$\mathrm{Box}(u) \subseteq \mathcal{U}, \quad \mathrm{Box}(v) \subseteq \mathcal{V}, \quad \mathrm{Box}(w) \subseteq \mathcal{W}, \tag{S27}$$

$$L_{\mathcal{C}}(b_u) \cap \mathrm{Box}(v) = \emptyset, \quad L_{\mathcal{C}}(b_u) \cap \mathrm{Box}(w) = \emptyset \tag{S28}$$

$$L_{\mathcal{C}}(b_v) \cap \mathrm{Box}(u) = \emptyset, \quad L_{\mathcal{C}}(b_v) \cap \mathrm{Box}(w) = \emptyset \tag{S29}$$

$$L_{\mathcal{C}}(b_w) \cap \mathrm{Box}(u) = \emptyset, \quad L_{\mathcal{C}}(b_w) \cap \mathrm{Box}(v) = \emptyset. \tag{S30}$$

Proof. Since each vertex in the grid belongs to at most N boxes, we infer that a given lightcone $L_{\mathcal{C}}(b_u)$ with $u \in \mathrm{Good}(\mathcal{U})$ can intersect with at most $N|L_{\mathcal{C}}(b_u)| \le N^{\frac{5}{4}}$ boxes. Here we used the fact that $|L_{\mathcal{C}}(b_u)| \le N^{\frac{1}{4}}$ for all $u \in \mathrm{Good}(\mathcal{U})$ by definition. The total number of vertices $v \in \mathrm{Good}(\mathcal{V})$ such that $\mathrm{Box}(v) \subseteq \mathcal{V}$ is $\Omega(N^2)$, which follows from Eq. (S26) (and since the number of vertices $q \in \mathcal{V}$ with $\mathrm{Box}(q) \not\subseteq \mathcal{V}$ is $o(N^2)$ as any such vertex q must lie near the boundary of region $\mathcal{V}$). Thus if u, v, w are picked uniformly at random from the sets $\mathrm{Good}(\mathcal{U})$, $\mathrm{Good}(\mathcal{V})$ and $\mathrm{Good}(\mathcal{W})$ respectively subject to Eq. (S27) then

$$\mathrm{Prob}[L_{\mathcal{C}}(b_u) \cap \mathrm{Box}(v) \neq \emptyset] \le O\left(\frac{N^{\frac{5}{4}}}{N^2}\right) = O(N^{-3/4}) < \frac{1}{6} \tag{S31}$$

for large enough N. A similar bound applies to the five other combinations of vertices that appear in Eqs. (S28,S29,S30). By the union bound, there exists at least one choice of u, v, w that satisfies all conditions Eqs. (S27,S28,S29,S30). □

Below we consider cycles Γ that are subgraphs of the grid G.

Claim 7. *The following holds for all sufficiently large N. Fix some triple of vertices $u \in \mathrm{Good}(\mathcal{U})$, $v \in \mathrm{Good}(\mathcal{V})$, $w \in \mathrm{Good}(\mathcal{W})$ satisfying Eqs. (S27,S28,S29,S30). Then there exists a cycle Γ containing u, v, w such that the lightcones $L_{\mathcal{C}}(b_u)$, $L_{\mathcal{C}}(b_v)$, $L_{\mathcal{C}}(b_w)$ contain no vertices of Γ lying outside of $\mathrm{Box}(u) \cup \mathrm{Box}(v) \cup \mathrm{Box}(w)$.*

Proof. Indeed, since each box has size $\lfloor N^{1/2} \rfloor \times \lfloor N^{1/2} \rfloor$, one can choose $\lfloor N^{1/2} \rfloor$ pairwise disjoint paths γ that connect any pair of boxes $\mathrm{Box}(u)$, $\mathrm{Box}(v)$, $\mathrm{Box}(w)$, see Figure S2. Let $\gamma(a, b)$ be a path connecting $\mathrm{Box}(a)$ and $\mathrm{Box}(b)$, where $a \neq b \in \{u, v, w\}$. Any triple of paths $\gamma(u, v)$, $\gamma(v, w)$, $\gamma(u, w)$ can be completed to a cycle Γ that contains u, v, w by adding the missing segments of the

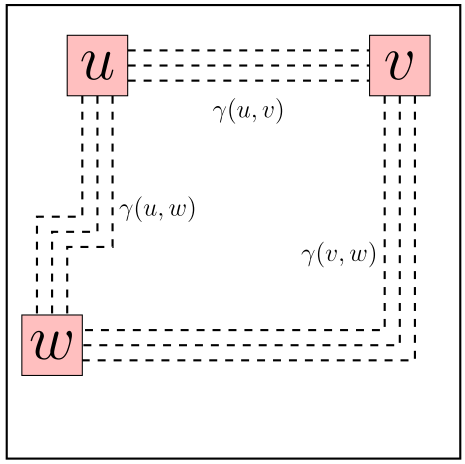

Figure S2: **Paths in the existence argument.** The figure shows pairwise disjoint paths γ connecting the boxes $\mathrm{Box}(u)$, $\mathrm{Box}(v)$, $\mathrm{Box}(w)$. The number of paths connecting each pair of boxes is $\lfloor N^{1/2} \rfloor$.

cycle inside the boxes $\mathrm{Box}(u)$, $\mathrm{Box}(v)$, $\mathrm{Box}(w)$. Since $L_{\mathcal{C}}(b_u)$ has size at most $N^{\frac{1}{4}}$ (recall that u is a good vertex) and each vertex $q \in V$ belongs to at most one path γ, we infer that $L_{\mathcal{C}}(b_u)$ intersects with at most $N^{\frac{1}{4}}$ paths γ. Thus if we pick the path $\gamma(u,v)$ uniformly at random among all $\lfloor N^{1/2} \rfloor$ possible choices then

$$\mathrm{Prob}[L_{\mathcal{C}}(b_u) \cap \gamma(u,v) \neq \emptyset] \leq \frac{N^{\frac{1}{4}}}{\lfloor N^{1/2} \rfloor} = O(N^{-1/4}) < \frac{1}{9} \tag{S32}$$

for large enough N. The same bound applies to the eight remaining combinations of a lightcone $L_{\mathcal{C}}(b_u)$, $L_{\mathcal{C}}(b_v)$, $L_{\mathcal{C}}(b_w)$ and a path γ. By the union bound, there exists at least one triple of paths $\gamma(u,v)$, $\gamma(v,w)$, $\gamma(u,w)$ that do not intersect with $L_{\mathcal{C}}(b_u)$, $L_{\mathcal{C}}(b_v)$, $L_{\mathcal{C}}(b_w)$. This gives the desired cycle Γ. □

Let u, v, w and Γ be chosen as described in Claim 7. Recall that $u, v, w \in V_{\mathrm{even}}$ and therefore all pairwise distances between them along Γ are even. In particular, properties (i)–(iii) mentioned in the main text are satisfied. Let M be the number of vertices in Γ. Consider the subset of instances (A, b) of the 2D Hidden Linear Function problem where

$$A_e = \begin{cases} 1 & \text{if } e \text{ is an edge of } \Gamma \\ 0 & \text{otherwise.} \end{cases} \qquad \text{and} \qquad b_j = 0 \quad \text{if} \quad j \in V \setminus \{u, v, w\}. \tag{S33}$$

There are 8 such instances corresponding to choices of input bits $b_u, b_v, b_w \in \{0, 1\}$. By fixing inputs to the circuit $\mathcal{C}$ in this way and looking only at output bits z_j with $j \in \Gamma$ we obtain a classical circuit $\mathcal{D}$ which takes a three-bit string $b_u b_v b_w \in \{0,1\}^3$ and a random string r as input and outputs $z_\Gamma \in \{0,1\}^M$. For any input bit $b_i \in \{b_u, b_v, b_w\}$ we have

$$L_{\mathcal{D}}(b_i) \subseteq L_{\mathcal{C}}(b_i) \tag{S34}$$

since any pair of input/output variables which are correlated in $\mathcal{D}$ are by definition also correlated in $\mathcal{C}$. Our assumption that $\mathcal{C}$ solves the 2D Hidden Linear Function problem with probability greater than $7/8$ implies that the output $z_\Gamma(b,r)$ of the circuit $\mathcal{D}$ satisfies

$$\mathrm{Prob}\left[z_\Gamma(b,r) \in \mathsf{sol}(\Delta, 0^{M-3}b)\right] > \frac{7}{8} \qquad \text{for all } b \in \{0,1\}^3\,, \tag{S35}$$

where Δ is the adjacency matrix of Γ. Using Eq. (S35) and applying Lemma 3 with the cycle Γ constructed above we infer that the lightcone $L_{\mathcal{D}}(b_i)$ of one of the input bits $b_i \in \{b_u, b_v, b_w\}$ contains at least one output bit z_q such that $q \in \Gamma$ and the distance between i and q along the cycle Γ is $\Omega(N)$. By Eq. (S34) the same is true for the lightcone $L_{\mathcal{C}}(b_i)$. For all sufficiently large N this contradicts Claims 6,7. Indeed, by Claim 7, the vertex $q \in L_C(b_i) \cap \Gamma$ must lie in one of $\mathrm{Box}(u), \mathrm{Box}(v)$ or $\mathrm{Box}(w)$, and since $L_{\mathcal{C}}(b_i)$ has no intersection with $\mathrm{Box}(j)$ ($i \neq j$) by Claim 6, this implies that $q \in \mathrm{Box}(i)$. But the distance from i to any vertex inside $\mathrm{Box}(i)$ is $\leq N^{1/2}$. We conclude that Eq. (S22) is false for all sufficiently large N. □

C.3 An average-case hardness result for the 2D HLF problem

Our proof of Theorem 1 actually gives a stronger result that can be interpreted as an average-case hardness of the 2D HLF problem for shallow classical circuits (as opposed to the worst-case hardness stated in the theorem which we have prioritized here because of its simplicity). To state this stronger result let us introduce additional notation. Let $\mathcal{S}_N$ be the set of all size-N instances of the 2D HLF problem and $\mathcal{S}_N^{\times 4}$ be the set of 4-tuples of such instances. We shall say that a classical probabilistic circuit $\mathcal{C}_N$ solves a tuple of instances $(I_1, I_2, I_3, I_4) \in \mathcal{S}_N^{\times 4}$ with probability p if $\mathcal{C}_N$ solves *each* instance I_1, I_2, I_3, I_4 with probability at least p. We then have the following statement:

Lemma 4. *For all large enough N there exists a subset $\mathcal{T}_N \subset \mathcal{S}_N^{\times 4}$ with the following property. Suppose $\mathcal{C}_N$ is a classical circuit with fan-in at most K which solves at least one half of tuples in $\mathcal{T}_N$ with probability greater than $7/8$. Then the depth of $\mathcal{C}_N$ is at least*

$$\frac{1}{8}\frac{\log(N)}{\log(K)}.$$

Furthermore, the set $\mathcal{T}_N$ has size $poly(N)$ and can be efficiently computed.

The lemma has an important practical implication: in order to demonstrate a separation between constant depth quantum and classical circuits it is sufficient to test whether the constant-depth quantum circuit $\mathcal{Q}_N$ described in the main text solves a small subset of size-N instances rather than testing that it solves *all* size-N instances (the latter task is clearly impractical since the total number of size-N instances is exponentially large). More precisely, let $d = \frac{1}{8}\frac{\log(N)}{\log(K)}$ be the lower bound from Lemma 4. Suppose one picks 100 random 4-tuples from the uniform distribution on $\mathcal{T}_N$. This results in a set of size-N instances $I_1, I_2, \ldots, I_{400} \in \mathcal{S}_N$. One can test whether the quantum circuit $\mathcal{Q}_N$ solves each instance $I_1, I_2, \ldots, I_{400}$ with probability greater than $7/8$. If this is the case, one can infer from Lemma 4 that the chance of $\mathcal{Q}_N$ having a classical simulator described by a depth-d circuit with fan-in $\le K$ is less than 2^{-100}. This number can be viewed as zero for all practical purposes. Thus, in principle, one can rule out the possibility of $\mathcal{Q}_N$ having a constant-depth classical simulator by testing its behavior on a set of $O(1)$ instances (for sufficiently large N).

In the rest of this section we explain how the proof of Theorem 1 has to be modified to obtain Lemma 4. Below we use the notations introduced in the proof of Theorem 1. Let $\mathcal{U}, \mathcal{V}, \mathcal{W} \subseteq V$ be the square-shaped regions shown in Figure S1. For any pair of vertices $i, j \in V$ such that $\mathrm{Box}(i)$ and $\mathrm{Box}(j)$ are contained in distinct regions $\mathcal{U}, \mathcal{V}, \mathcal{W}$ fix a family $\Gamma(i,j)$ of $N^{1/2}$ pairwise disjoint paths connecting the boundary of $\mathrm{Box}(i)$ with the boundary of $\mathrm{Box}(j)$. We illustrate the construction of such paths on Fig. S2. Consider the following algorithm that generates 4-tuples of instances with a specified size N.

function GENERATETUPLE(N)

1. Pick vertices $u, v, w \in V_{\text{even}}$ such that $\text{Box}(u) \subseteq \mathcal{U}$, $\text{Box}(v) \subseteq \mathcal{V}$, and $\text{Box}(w) \subseteq \mathcal{W}$.
2. Pick paths $\gamma(u,v) \in \Gamma(u,v)$, $\gamma(v,w) \in \Gamma(v,w)$, and $\gamma(w,u) \in \Gamma(w,u)$.
3. Complete the paths $\gamma(u,v)$, $\gamma(v,w)$, $\gamma(w,u)$ to a cycle Γ that contains the vertices u, v, w by adding the missing segments of the cycle inside $\text{Box}(u)$, $\text{Box}(v)$, $\text{Box}(w)$.
4. Set $A_{i,j} = 1$ for $(i,j) \in \Gamma$ and $A_{i,j} = 0$ otherwise.
5. Set $b_i = 0$ for $i \notin \{u, v, w\}$.
6. Consider all possible assignments $b_u, b_v, b_w \in \{0,1\}$ such that $b_u \oplus b_v \oplus b_w = 0$. Each of the four assignments results in a size-N instance $I = (A, b)$ of the 2D HLF problem. Return the corresponding 4-tuple of instances.

end function

This definition leaves some freedom in choosing the missing segments of the cycle at Step 3. Let us agree that for each choice of the paths $\gamma(u,v)$, $\gamma(v,w)$, $\gamma(w,u)$ at Step 2 one fixes some (arbitrary) completion of these paths to a cycle Γ.

Let $\mathcal{T}_N$ be the set of 4-tuples of instances that can be produced by this algorithm. Then clearly $\mathcal{T}_N$ has size $poly(N)$ and can be efficiently computed.

To prove Lemma 4, we need the following strengthenings of Claim 6 and Claim 7.

Claim 6′. *Pick a random triple of vertices $u, v, w \in V_{even}$ such that*

$$\text{Box}(u) \subseteq \mathcal{U}, \quad \text{Box}(v) \subseteq \mathcal{V}, \quad \text{Box}(w) \subseteq \mathcal{W}. \tag{S36}$$

Each vertex is drawn from the uniform distribution subject to the constraints Eq. (S36). Then with probability $1 - O(N^{-1/8})$, all conditions (S28), (S29) and (S30) are satisfied and

$$u \in \text{Good}(\mathcal{U}), \quad v \in \text{Good}(\mathcal{V}), \quad w \in \text{Good}(\mathcal{W})\ . \tag{S37}$$

Proof. Indeed, condition (S37) holds with probability $1 - O(N^{-1/8})$ as follows from (S26) and the union bound. The claim then follows from (S31) and the union bound. □

Claim 7′. *Fix a triple of vertices $u \in \mathcal{U}$, $v \in \mathcal{V}$, and $w \in \mathcal{W}$ satisfying Eqs. (S36,S37). Let $\Gamma \subseteq E$ be a random cycle passing through u, v, w constructed at Steps 2,3 of the tuple generating algorithm. The lightcones $L_{\mathcal{C}}(b_u)$, $L_{\mathcal{C}}(b_v)$, $L_{\mathcal{C}}(b_w)$ contain no vertices of Γ lying outside of $\text{Box}(u) \cup \text{Box}(v) \cup \text{Box}(w)$ with probability $1 - O(N^{-1/4})$.*

Proof. This follows similarly from (S32) and the union bound. $\square$

With these statements, Lemma 4 can be shown along the same lines as the proof of Theorem 1.

Proof. Assume that $\mathcal{C}$ is a circuit of small depth, i.e., depth satisfying (S22), which solves at least one half of tuples in $\mathcal{T}_N$ with probability greater than $7/8$. Let u, v, w and Γ be chosen as described in Steps 1,2,3 of the algorithm generating $\mathcal{T}_N$. Using Eq. (S35) and applying Lemma 3 with the cycle Γ constructed above we infer that for at least half these tuples, the lightcone $L_{\mathcal{C}}(b_i)$ of one of the input bits $b_i \in \{b_u, b_v, b_w\}$ contains at least one output bit z_q such that $q \in \Gamma$ and the distance between i and q along the cycle Γ is $\Omega(N)$. On the other hand, Claims 6′,7′ imply that a fraction $1-O(N^{-1/4})$ of all tuples in $\mathcal{T}_N$ obey Eqs. (S28,S29,S30) and have the property that the lightcones $L_{\mathcal{C}}(b_u)$, $L_{\mathcal{C}}(b_v)$, $L_{\mathcal{C}}(b_w)$ contain no vertices of Γ lying outside of $\mathrm{Box}(u)\cup\mathrm{Box}(v)\cup\mathrm{Box}(w)$. None of these tuples can have a vertex $q \in L_C(b_i) \cap \Gamma$ such that the distance between i and q along the cycle Γ is $\Omega(N)$. Therefore, if $\mathcal{C}$ solves a fraction $\Omega(N^{-1/4})$ of all tuples in $\mathcal{T}_N$ with probability greater than $7/8$, then Eq. (S22) is false. $\square$