Quantum Advantage with Shallow Circuits Under Arbitrary Corruption

Atsuya Hasegawa ✉
The University of Tokyo, Japan

François Le Gall ✉
Nagoya University, Japan

── **Abstract** ──

Recent works by Bravyi, Gosset and König (Science 2018), Bene Watts et al. (STOC 2019), Coudron, Stark and Vidick (QIP 2019) and Le Gall (CCC 2019) have shown unconditional separations between the computational powers of shallow (i.e., small-depth) quantum and classical circuits: quantum circuits can solve in constant depth computational problems that require logarithmic depth to solve with classical circuits. Using quantum error correction, Bravyi, Gosset, König and Tomamichel (Nature Physics 2020) further proved that a similar separation still persists even if quantum circuits are subject to local stochastic noise.

In this paper, we consider the case where *any* constant fraction of the qubits (for instance, huge blocks of qubits) may be arbitrarily corrupted at the end of the computation. We make a first step forward towards establishing a quantum advantage even in this extremely challenging setting: we show that there exists a computational problem that can be solved in constant depth by a quantum circuit but such that even solving *any* large subproblem of this problem requires logarithmic depth with bounded fan-in classical circuits. This gives another compelling evidence of the computational power of quantum shallow circuits.

In order to show our result, we consider the Graph State Sampling problem (which was also used in prior works) on expander graphs. We exploit the "robustness" of expander graphs against vertex corruption to show that a subproblem hard for small-depth classical circuits can still be extracted from the output of the corrupted quantum circuit.

1 Introduction

Background. Quantum computing was introduced in the early 1980s as a quantum mechanical model of the Turing machine that has a potential to simulate things that a classical computer could not [11, 25]. In 1994, Peter Shor developed a polynomial-time quantum algorithm for factoring integers [43], which gave an exponential speedup over the most efficient known classical algorithms for this task.

While initially realizing a physical quantum computer was thought to be extremely challenging, nowadays various types of high-fidelity processors capable of quantum algorithms have been developed [10, 24, 36, 38, 45]. These devices with noise and relatively small scale are called NISQ (Noisy Intermediate-Scale Quantum) devices [41]. For such devices, "quantum supremacy" [40] has been recently reported [6, 46].

32nd International Symposium on Algorithms and Computation (ISAAC 2021).
Editors: Hee-Kap Ahn and Kunihiko Sadakane; Article No. 74; pp. 74:1–74:16
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

While Shor's algorithm and such quantum supremacy results strongly suggest that quantum computation is more powerful than classical computation, they are not mathematical proofs. While the superiority of quantum computation has been formally shown in constrained models such as query complexity [4] and communication complexity [22, 34] and considering complexity classes relative to an oracle [12, 42], almost no definite answer is known in standard computational models such as Turing machines or general circuits. Since the complexity class BQP (the class of the problems that can be solved efficiently by a quantum computer) satisfies the inclusions P $\subseteq$ BPP $\subseteq$ BQP $\subseteq$ PSPACE, an unconditional separation between BPP and BQP would imply a separation between P and PSPACE, which would be a significant breakthrough. Therefore, unconditional separations between the computational powers of quantum computers and classical computers in a general setting are expected to be very hard to obtain.

However, with several assumptions from computational complexity such as non-collapse of the polynomial hierarchy or some conjectures on the hardness of the permanent, the superiority of quantum computation has been shown in the circuit model: even approximate or noisy probabilistic distributions of small depth quantum circuits are hard to simulate for classical computers [1, 2, 3, 13, 16, 17, 18, 44]. A recent breakthrough by Bravyi, Gosset and König [14] showed an *unconditional* separation between the computational powers of small-depth quantum and classical circuits: they constructed a computational problem that can be solved by quantum circuits of constant depth composed of one- and two-qubit gates acting locally on a grid and showed that any probabilistic classical circuit with bounded fan-in gates solving this problem on all inputs must have depth $\Omega(\log n)$, where n denotes the input size. The computational problem they use is a relation problem (i.e., for any input there are several possible outputs). Besides its theoretical importance, this separation is also important since shallow quantum circuits are likely to be easy to implement on physical devices experimentally due to their robustness to noise and decoherence.

There are several results related to this separation. Coudron, Stark and Vidick [21] and Le Gall [26] showed a similar separation in the average case setting, instead of the worst case setting considered in the original version of [14]: there exists a relation problem such that constant-depth quantum circuits can solve the relation on all inputs, but any $O(\log n)$ depth randomized bounded fan-in classical circuits cannot solve it on *most* inputs with high probability. Bene Watts et al. [9] showed that a similar separation holds against classical circuits using unbounded fan-in gates and, considering interactive tasks, Grier and Schaeffer [28] showed even stronger classical lower bounds.

Bravyi et al. [15] additionally proved, using quantum error-correction, that a similar separation holds even if quantum circuits are corrupted by local stochastic noise (see Definition 1 below). The computational problem used in [15] is a generalized version, defined on a 3D grid, of the magic square game [35, 39], which is a nonlocal game with two cooperating players Alice and Bob who cannot communicate. The noise model is as follows.

▶ **Definition 1** (Definition 9 in [15]). *Consider a random n-qubit Pauli error $E \in \{I, X, Y, Z\}^{\otimes n}$ and let $Supp(E) \subseteq [n]$ denote its support, i.e., the subset of qubits acted on by either X, Y, or Z. For any constant $p \in [0,1]$, E is called p-local stochastic noise if*

$$\Pr[F \subseteq Supp(E)] \leq p^{|F|} \quad \text{for all } F \subseteq [n].$$

In this model, an error is given as applying a gate which is X, Y or Z. This definition assumes that when picking an arbitrary subset of qubits, the probability of all qubits are corrupted is an exponentially small function of the size of the subset. This property, which implies that a subset of size $\Omega(\log n)$ contains with probability $1 - 1/\text{poly}(n)$ at least one qubit that

is not corrupted, is crucial in [15] to use quantum error correction. Note that, considering interactive tasks, Grier, Ju and Schaeffer [27] showed even stronger classical lower bounds in the same noise setting.

The Graph State Sampling problem. Before presenting our results, let us describe in more details the computational problem introduced in [14], which is called the 2D Hidden Linear Function problem and corresponds to an extension of the Bernstein-Vazirani problem [12].

We actually describe a slightly more general computational problem that we name the "Graph State Sampling problem" and denote $\rho(G)$. Here $G = (V, E)$ is a graph specifying the problem. For any graph G, the problem $\rho(G)$ is a relation $\rho(G) \subseteq \{0, 1\}^{|V|+|E|} \times \{0, 1\}^{|V|}$. Given an input $x \in \{0, 1\}^{|V|+|E|}$ for this relation problem, which we interpret as a pair $x = (y, H)$ with $y \in \{0, 1\}^{|V|}$ and H being a subgraph of G, we ask to output any bit string $z \in \{0, 1\}^{|V|}$ that may appear with nonzero probability when measuring the graph state corresponding to the subgraph H in a basis determined by the bit string y. We refer to Section 5.1 for details of the definition of the problem.

The 2D Hidden Linear Function problem considered in [14] is essentially the problem $\rho(G)$ where G is the family of 2D grid graphs. Since the graph states of subgraphs of a 2D grid can be constructed by constant-depth quantum circuits whose gates act locally on the grid graphs, the problem $\rho(G)$ can be solved by a constant-depth quantum circuit. At the same time, Bravyi et al. [14] prove that no small-depth classical circuits can solve this problem using an argument based on the existence of quantum nonlocality in a triangle (first shown by Barrett et al. [7]). The main result in [14] can essentially be restated as follows.[1]

▶ **Theorem 2** ([14]). *There exist a constant $\alpha > 0$ such that the following holds for all sufficiently large 2D grid graphs G:*
   (i) *$\rho(G)$ can be solved on all inputs with certainty by a constant-depth quantum circuit on $\Theta(|G|)$ qubits composed of one- and two-qubit gates;*
   (ii) *no bounded-fanin classical probabilistic circuit whose depth is less than $\alpha \log(|G|)$ can solve with high probability $\rho(G)$ on all inputs.*

Description of our results. In this paper we show the following result.

▶ **Theorem 3.** *There exist constants $\alpha > 0$ and $\epsilon > 0$, and a family of graphs $(G_i)_{i \in \mathbb{N}}$ with $\lim_{i \to \infty} |G_i| = \infty$ such that the following holds for all sufficiently large i:*
   (i) *$\rho(G_i)$ can be solved on all inputs with certainty by a constant-depth quantum circuit on $\Theta(|G_i|)$ qubits composed of one- and two-qubit gates;*
   (ii) *for any induced subgraph S_i of G_i such that $|S_i| \geq (1-\epsilon)|G_i|$, no bounded-fanin classical probabilistic circuit whose depth is less than $\alpha \log(|S_i|)$ can solve with high probability $\rho(S_i)$ on all inputs.*

Item (ii) of Theorem 3, which is proved by considering the Graph State Sampling problem over expander graphs, gives a significantly stronger hardness guarantee than in Theorem 2 and thus provides us further compelling evidence of the computational power of quantum shallow circuits.

We stress that Theorem 3 does not claim a quantum advantage for noisy shallow quantum circuits: Theorem 3 simply shows that there exists a problem that can be computed by shallow quantum circuit but such that a shallow classical circuit cannot solve *any* (large)

---

[1] In this paper, for any graph G we use the notation $|G|$ to denote the size of the vertex set of G.

subproblem of it. We can nevertheless interpret Item (ii) as follows. A quantum circuit $\mathcal{C}$ solving the relation $\rho(G_i)$ has $|G_i|$ output qubits, which are measured at the end of the computation to give the output string $z \in \{0,1\}^{|G_i|}$ that is a solution for the relation. Assume that an adversary chooses up to $\epsilon|G_i|$ qubits among these $|G_i|$ qubits and corrupts them in an arbitrary way (or, essentially equivalently, corrupts the bits of the measurement outcomes corresponding to these positions). Let S_i denote the set of qubits that are not corrupted by the adversary. Since $\rho(S_i)$ corresponds to a subproblem[2] of $\rho(G_i)$, and since $\mathcal{C}$ before the corruption solved the problem $\rho(G_i)$ on all inputs, even after the corruption the part of the output of $\mathcal{C}$ corresponding to the qubits in S_i gives a correct solution to the problem $\rho(S_i)$. On the other hand, Item (ii) of Theorem 3 shows that no small-depth classical circuit can solve $\rho(S_i)$. (Note that in Item (ii) we even allow the classical circuit to depend on S_i.)

Let us compare this model of corruption of qubits with the model of noise considered in [15]. As already mentioned, in the error model of [15] (Definition 1 above), the probability that all qubits in a given set of size $\Theta(\log n)$, where n denotes the total number of qubits, are corrupted by the noise is polynomially small and thus can be neglected. In comparison, Theorem 3 deals with the case where any subset of qubits of size as large as $\Theta(n)$ can be corrupted, and shows that the quantum advantage is still preserved in this case. In this sense, our result gives a further compelling evidence of the computational power of quantum shallow circuits.

Brief overview of our techniques and organization of the paper. The family of graph $(G_i)_{i \in \mathbb{N}}$ used to prove Theorem 3 is a class of expander graphs of constant degree.[3] Item (i) of Theorem 3 essentially follows from the fact the graph state of a bounded-degree graph can be created by a constant-depth quantum circuit composed of one- and two-qubit gates. The proof of Item (ii) of Theorem 3 exploits the "robustness" of expander graphs against corruption of vertices. More precisely, we show that even after corrupting a constant fraction of vertices, an expander graph still has a large grid minor (see Lemma 8 in Section 3). Finally, exploiting the existence of a large grid minor, we can use arguments based on quantum nonlocality (very similarly to the arguments used in prior works [14, 26]) to conclude that any classical circuit solving the Graph State Sampling problem on the expander graph requires logarithmic depth.

After giving preliminaries in Section 2, in Section 3 we present graph-theoretical results about expander graphs. In particular, we prove Lemma 8 about the existence of large grid minors in corrupted expander graphs. In Section 4, we review the result about the nonlocality of a triangle quantum graph state used in prior works. In Section 5, we define our computational problem and prove Theorem 3.

2   Preliminaries

Graph theory. All graphs considered in this paper are undirected. We write a graph as $G = (V, E)$ where V is the vertex set and E is the edge set. $|G|$ means the number of vertex of graph G, i.e., $|V|$. The degree of a vertex is the number of edges that are incident to the vertex. We denote $deg(v)$ the degree of a vertex v. Given a graph $G = (V, E)$ and any vertex set $U \subseteq V$, we denote $N_G(U) = \{v \in V \setminus U : v \text{ has a neighbor in } U\}$ the external neighborhood of U in G.

---

[2] This property can immediately be derived from the formal definition of the computational problem given in Section 5.1

[3] For technical reasons, we actually consider a family of graphs of the form $G \times K_2$, where G is an expander graph of constant degree and K_2 is the graph consisting of a single edge.

Let us describe the definition of graph minors. Graph Γ is a graph minor of graph G if it is isomorphic to a graph obtained from G by deleting edges and vertices and by contracting edges. Note that if a graph Γ is a minor of a subgraph S of a graph G, Γ is also a minor of G. The definition is equivalent to the following definition, that if graph Γ is a minor of graph G, we can decompose G to connected subgraphs which connect to each other like Γ. We will use this definition later for explicit explanations.

▶ **Definition 4** (Minor, Definition 1 in [33]). *A graph Γ is a minor of a graph G if for every vertex $u \in \Gamma$ there is a connected subgraph G_u of G such that all subgraphs G_u are vertex disjoint, and G contains an edge between G_u and $G_{u'}$ whenever $\{u, u'\}$ is an edge of Γ.*

Next, we will define the product of graphs $G \times H$ of graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$. The vertex set of $G \times H$ is the Cartesian product $V_G \times V_H$ and an edge is spanned between (u_G, u_H) and (v_G, v_H) if and only if $u_G = v_G$ and $\{u_H, v_H\} \in E_H$, or $u_H = v_H$ and $\{u_G, v_G\} \in E_G$. There are several ways to define graph products but we will use the definition above. In this paper, we particularly use $G \times K_2$, which K_2 is the complete graph of two vertices. Given a graph $G = (V, E)$, the graph product $G \times K_2$ is with $2|V|$ vertices and $2|E| + |V|$ edges.

Lastly, we refer to the Vizing's theorem, which is about edge coloring. Edge coloring is to assign colors to edges so that the edges of the same color are not incident.

▶ **Lemma 5** (Vizing's theorem [23]). *Every simple undirected graph can be edge colored using a number of colors that is the maximum degree or the maximum degree+1.*

Quantum circuits. The textbook [37] is a good reference about notations of quantum computation in our paper. We will use the Pauli X, Y and Z gates, the Hadamard gate and the S and T gates as single qubit gates:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \ T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix},$$

where i denotes the imaginary unit of complex numbers. (Note the Phase gate S differs from the standard one in [37].) We also use the controlled Pauli Z gate (or $CZ = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes Z$) as two-qubit gate.

Let us explain about quantum circuits. An n-qubit quantum circuit is initialized to $|0^n\rangle$ and then arbitrary gates are applied to the state. We can apply gates at one time if each gate is applied to disjoint sets of qubits. The depth of a quantum circuit is d if the whole operation of circuits can be decomposed to $U_d...U_2U_1$ where each U_j is a tensor product of one- and two-qubit gates which act on disjoint sets of qubits.

Next, we describe measurements of quantum states. Mathematically, (projective) measurements are projections to some orthogonal bases. In this paper, We will use two kinds of measurements with the X basis and the Y basis. The orthogonal two states of X basis are $\{|+\rangle, |-\rangle\}$ and the ones of Y basis are $\{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\}$. Note that the measurements of X and Y basis are equivalent to the measurements of the computational basis if we apply H and HS gates before the measurements respectively.

Quantum graph states. Quantum graph states are a certain type of entangled states corresponding to graphs first introduced by [30]. Let $G = (V, E)$ be a finite simple graph. Define an associated $|V|$ qubit graph state $|\Phi_G\rangle$ by

$$|\Phi_G\rangle = \left(\prod_{e \in E} CZ_e \right) H^{\otimes |V|} |0^{|V|}\rangle. \tag{1}$$

The graph state $|\Phi_G\rangle$ is a stabilizer state with stabilizer group generated by the operators $g_v = X_v \left(\prod_{w:\{w,v\} \in E} Z_w \right)$ for all $v \in V$.

Classical circuits.   A classical circuit is specified by a directed acyclic graphs. Vertices with no incoming and outgoing edges are inputs and outputs respectively and all other vertices are called gates. We must specify a function of each gate $\{0,1\}^k \to \{0,1\}$ where k is the fan-in. We assume a classical probabilistic circuit receives an arbitrary binary x as an input and outputs a binary z and it also could input a random string r drawn from some arbitrary distribution. We say an input bit and an output bit are correlated iff the value of the output bit depends on the value of the input bit. For each input bit x_i, we denote the lightcone $L_C(x_i)$ the set of output bits correlated with x_i through a classical circuit C. Likewise, the lightcone $L_C(z_i)$ is the set of input bits correlated with an output bit z_i. In this paper, we are interested in small-depth classical circuits with bounded fan-in. We also say that a classical probabilistic circuit solves the relation R on all inputs if and only if the circuit takes any $x \in \{0,1\}^n$ and a random string r as input and outputs $z \in \{0,1\}^m$ such that xRz with high probability.

3   Expander graphs and their properties

Expander graphs are highly sparse but well connected graphs. Notable applications of the graphs have been found in mathematics and computer science [8, 19, 29]. Before giving the definition, we define the expansion ratio $h(G)$ of graph G. There are several ways to define the expansion ratio, for example edge expansion, vertex expansion and spectral expansion, but these are related to each other. The way we use is called vertex expansion.

▶ **Definition 6** (Expansion ratio). $h(G) = \min\left\{ \frac{|N_G(U)|}{|U|} \,\middle|\, U \subset V \text{ such that } 1 \leq |U| \leq \frac{1}{2}|V| \right\}$

The definition of expander graphs we use in this paper is as follows.

▶ **Definition 7** (Expander graphs, Definition 3.1.8 in [31]). *A family $(\Gamma_i)_{i\in\mathbb{N}}$ of finite non-empty connected graphs $\Gamma_i = (V_i, E_i)$ is an expander family, if there exist constants $d \geq 1$ and $h > 0$, independent of i, such that:*

(1) *The number of vertices $|V_i|$ "tends to infinity", in the sense that for any $N \geq 1$, there are only finitely many $i \in \mathbb{N}$ such that Γ_i has at most N vertices.*

(2) *For each $i \in \mathbb{N}$, we have $\max_{v \in V_i} deg(v) \leq d$, i.e., the maximum degree of the graphs is bounded independently of i.*

(3) *For each $i \in \mathbb{N}$, the expansion constant satisfies $h(\Gamma_i) \geq h > 0$, i.e., it is bounded away from 0 by a constant independent of i.*

h and d specify the family of expander graphs. The existence of expander graphs is by no means obvious, but it can be shown using probabilistic approaches or concrete constructions of such graphs [31]. In this paper, an expander graph denotes a graph with sufficiently large i of an expander family.

We want to prove the robustness of expander graphs to arbitrary vertex removals in terms of the size of grid minor, which is Lemma 8. We provide its proof in Appendix A.

▶ **Lemma 8.** *Let $G = (V, E)$ be a expander graph. If we take a sufficiently small constant $\epsilon > 0$, the graph has a connected component C which contains a $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ grid as a minor after up to an ϵ fraction of V are adversarially removed.*

4   Quantum nonlocality of a triangle graph state

In specific circumstances, local classical circuits cannot simulate measurement outcomes of entangled quantum states. This is called *quantum nonlocality*. In this section, we explain it occurs in a triangle graph state, as first shown in [7]. We will use this property to show the hardness of classical circuits to solve the relation problem in Section 5.
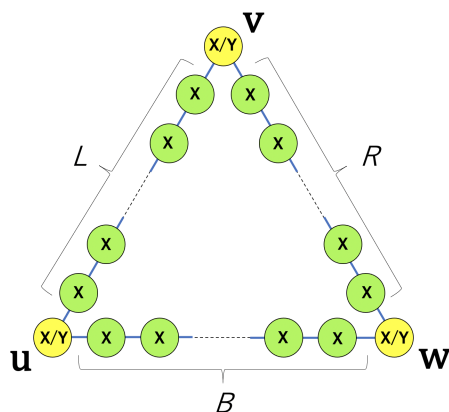
Figure 1 We consider an even cycle Γ and three vertices u, v, w such that all pairwise distances are even. L, R, B are the region between the three vertices. Each qubit of the corresponding graph state is measured by the X or Y basis.

First, we note about properties of a graph state in a triangle shape. Let Γ be a triangle such that the distance between three vertices u, v, w are all even and $|\psi_\Gamma\rangle$ be a graph state for Γ as in Equation (1). We define L, R, B as the vertices between u and v, v and w, u and w, and M as a total number of vertices in Γ. Also define $L_{odd}, L_{even}, R_{odd}, R_{even}, B_{odd}, B_{even}$ as vertices of L, R, B which have odd and even distance from u, v, w respectively. The three bits $x = x_u x_v x_w$ decide the measurement basis of u, v, w (the X basis if $x_i = 0$ and the Y basis if $x_i = 1$) and the other vertices are measured in the X basis. We denote $\tau(x)$ possible measurement outcomes of all qubits of $|\psi_\Gamma\rangle$ for input x, i.e., $\tau(x) = \left\{ z \in \{0,1\}^M : \langle z| H^{\otimes M} S_u{}^{x_u} S_v{}^{x_v} S_w{}^{x_w} |\psi_\Gamma\rangle \neq 0 \right\}$. We consider a relationship between input x and output $z \in \tau(x)$. Define the following summations:

$$z_L = \bigoplus_{i \in L_{odd}} z_i \quad z_R = \bigoplus_{i \in R_{odd}} \quad z_B = \bigoplus_{i \in B_{odd}} z_i \quad z_E = \bigoplus_{i \in \{u,v,w\} \cup R_{even} \cup L_{even} \cup B_{even}} z_i.$$

▷ **Claim 9** (Claim 3 in [14]).   Let $x = x_u x_v x_w \in \{0,1\}^3$ and suppose $z \in \tau(x)$. Then $z_R \oplus z_B \oplus z_L = 0$. Moreover, if $x_u \oplus x_v \oplus x_w = 0$ then

$(x_u x_v x_w = 000) \quad z_E = 0, \qquad (x_u x_v x_w = 110) \quad z_E \oplus z_L = 1,$

$(x_u x_v x_w = 101) \quad z_E \oplus z_B = 1, \quad (x_u x_v x_w = 011) \quad z_E \oplus z_R = 1.$

The following lemma is about quantum nonlocality in graph states of triangles and similar to Lemma 3 in Section 4.1 of [14]. It shows that when we assume a classical circuit has a kind of locality, the classical circuit cannot satisfy the relation of Claim 9 as inputs and outputs.

▶ **Lemma 10** ([7, 14, 26]).   *Consider a classical circuit which takes as an input a bit string $x = x_u x_v x_w \in \{0,1\}^3$ and a random string r, and outputs $z \in \{0,1\}^M$ which are corresponding to vertices of Γ. Let us assume output bits in L depend on r and at most one geometrically near input bit, which is either x_u or x_v. Similarly, we assume output bits in R and B depend on r and at most one geometrically near input bit. Then, the classical circuit C cannot output $z \in \tau(x)$ with high probability.*

5   Proof of separation of depth between quantum and classical circuits to solve Graph State Sampling problem

In this section, we define Graph State Sampling problem and prove a separation of depth between quantum circuits and classical circuits. We consider an almost all induced subgraph S of a graph $G \times K_2$ such that G is an expander graph. Then, we prove $\rho(G \times K_2)$ can be solved on all inputs by a constant-depth quantum circuit on $\Theta(|G \times K_2|)$ qubits, but $\Omega(\log |S|)$ depth is required for any classical probabilistic circuits to solve $\rho(S)$ on all inputs.

5.1   Definition of Graph State Sampling problem $\rho(G)$

In this subsection, for any graph G, we define Graph State Sampling problem $\rho(G)$.

The relation is defined as a subset of $\{0,1\}^{|V|+|E|} \times \{0,1\}^{|V|}$ and thus consists of pairs (x,z), where $x \in \{0,1\}^{|V|+|E|}$ represents the input and $z \in \{0,1\}^{|V|}$ represents the output. Each bit of x corresponds to a vertex or a edge. The string x decides the quantum graph state and the measurement bases: a CZ gate corresponding to edge e is applied if $x_e = 1$, and the qubit corresponding to a vertex v is measured in the X basis if x_v is 0, or in the Y basis if x_v is 1. The quantum state $|\psi_x\rangle$ for each x before the measurement in the computational basis is thus:

$$|\psi_x\rangle = H^{\otimes |V|} \prod_{x_v=1} S_v \left(\prod_{x_e=1} CZ_e \right) H^{\otimes |V|} |0^{|V|}\rangle.$$

The output $z \in \{0,1\}^{|V|}$ of the relation is any possible outcome of the measurement of this quantum state (note that there are possibly several measurement outcomes z for each x). Since the probability of measurement results of each binary string z is $|\langle z|\psi_x\rangle|^2$, the definition of $\rho(G)$ is as follows.

▶ **Definition 11.** *Given a graph G,*

$$\rho(G) = \{(x,z)|x \in \{0,1\}^{|V|+|E|} \text{ and } z \in \{0,1\}^{|V|} \text{ such that } |\langle z|\psi_x\rangle|^2 > 0\}.$$
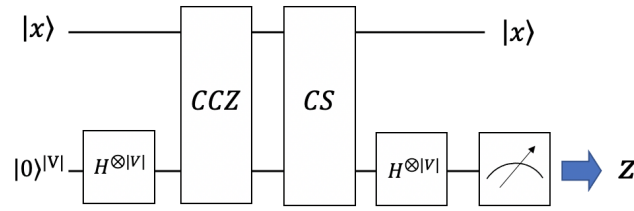
5.2   Constant-depth quantum circuits to solve Graph State Sampling problem

The following is easily shown by Lemma 5.

▶ **Lemma 12.** *When the maximum degree of graph $G = (V,E)$ is bounded by a constant, $\rho(G)$ on all inputs can be solved with certainty by a constant-depth quantum circuit on $\Theta(|G|)$ qubits composed of one- and two-qubit gates.*

Proof. The initial state $|x\rangle \otimes |0^{|V|}\rangle$ is prepared on $|E| + 2|V| = \Theta(|G|)$ qubits. We apply $H^{\otimes |V|}$ to the last $|V|$ qubits and then controlled-CZ (CCZ) gates and controlled-S (CS) gates that apply CZ_e if $x_e = 1$ and S_v if $x_v = 1$. Since G is edge colorable with a constant number from Lemma 5 and CCZ gates corresponding to edges assigned the same color can be applied simultaneously (since they act on disjoint sets of qubits), the total depth of CCZ gates can be bounded by a constant. CS gates can also be applied in constant depth. We finally apply $H^{\otimes |V|}$ to the last $|V|$ qubits and measure these qubits in the computational basis, which gives a string z such that $(x,z) \in \rho(G)$.

The total depth of this circuit can be bounded by a constant. (Note that each CCZ and CS gate can be implemented in constant depth using our elementary gates [5].) We refer to Figure 2 for an illustration.   ◀

Figure 2 Constant-depth quantum circuit to solve $\rho(G)$.

5.3 Hardness to solve Graph State Sampling problem with shallow classical circuits

In this subsection, we prove Theorem 3, and especially the classical hardness. The impossibility argument in Section 4 assumed classical circuits had a kind of geometrical locality. The lower bounds in this section, however, do not require any geometrical locality of shallow classical circuits. The proofs are similar to the proofs of the results of Section 4.2 in [14], with the notable exception of Claim 16 and the discussion afterwards (in particular, the definition of boxes), which are specifically tailored for the expander graphs we consider.

5.3.1 Good and bad vertices

To begin with, we define "good" and "bad" vertices. In a shallow classical circuit, most input bits are not correlated with many output bits. We call a vertex "bad" if the corresponding input bit are correlated with many output bits. Here is the formal definition.

▶ **Definition 13.** *Given a graph $G = (V, E)$, we consider $\rho(G)$ and a classical probabilistic circuit C for it. Then, a vertex $v \in V$ is good if $L_C(x_v) = O(|V|^{\frac{1}{16}})$ and bad if v is not good.*

The following claim is similar to Claim 5 in [14].

▷ **Claim 14.** Let $G = (V, E)$ be a graph such that the maximum degree is bounded by a constant and C be a classical probabilistic circuit for $\rho(G)$. Suppose the fan-in is bounded by a constant K and the depth d is less than $\frac{\log|V|}{32\log K}$, the number of bad vertices is $o(|V|)$.

Proof. Since the number of correlated input bits increases by at most K times when the depth increases by 1,

$$|L_C(z_i)| \leq K^d < |V|^{\frac{1}{32}} \quad \text{for all } v \in V. \tag{2}$$

Let us consider a bipartite graph whose vertices are respective bits of x and z, and a edge is spanned if and only if x_i and z_j are correlated. Since the maximum degree of G is bounded by a constant, we have $|x| = |V| + |E| = \Theta(|V|)$. From Equation (2) and considering edges spanned from z, the total number of edges is limited by $|V| \cdot |V|^{\frac{1}{32}}$. Since bad vertices are correlated with $\Omega(|V|^{\frac{1}{16}})$ output bits, the total number of x_v such that v is bad is $O(|V|^{\frac{31}{32}})$ and this means the number of bad vertices is $o(|V|)$. ◁

5.3.2 Proof of Theorem 3

Before the proof, we rewrite Theorem 3 using the notations we defined. The reason we consider the graph product $G \times K_2$ is to take a cycle which has even length for using Lemma 10.

▶ **Theorem 15.** *There exist constants $\alpha > 0$ and $\epsilon > 0$ such that the following holds for all sufficiently large expander graphs G:*

(i) *$\rho(G \times K_2)$ can be solved on all inputs with certainty by a constant-depth quantum circuit on $\Theta(|G \times K_2|)$ qubits composed of one- and two-qubit gates;*

(ii) *for any induced subgraph S such that $|S| \geq (1 - \epsilon)|G \times K_2|$, no bounded-fanin classical probabilistic circuits whose depth is less than $\alpha \log(|S|)$ can solve $\rho(S)$ on all inputs.*

Proof of Theorem 15. We can take $|G| = |V|$ arbitrary large from the property of expander graphs. Then $|G \times K_2| = 2|G|$ and $|S| \geq (1 - \epsilon)|G \times K_2|$ are also sufficiently large. Let us introduce some convenient notations. Given a vertex $u \in G$, we denote u' and u'' the two corresponding vertices in $G \times K_2$ (with no special order). Given a vertex $v \in G \times K_2$, we denote $\bar{v}$ the other vertex in $G \times K_2$ associated to the same vertex in G.

First, we prove Theorem 15 (i). We consider the Graph State Sampling problem $\rho(G \times K_2)$. Since the maximum degree of G is bounded by a constant d, the maximum degree of $G \times K_2$ is bounded by $d + 1$. From Lemma 12, $\rho(G \times K_2)$ can be solved with a constant-depth quantum circuit.

Next, we will prove Theorem 15 (ii), the hardness to solve $\rho(S)$ on all inputs with shallow classical circuits. Let C be a classical probabilistic circuit to solve $\rho(S)$ on all inputs and K be the bounded fan-in of C. In order to reach a contradiction, we assume the depth of C is less than $\frac{\log |S|}{32 \log K}$. Then the number of bad vertices is small, which enables us to prove the following claim.

▷ Claim 16. S contains an induced subgraph $G' \times K_2$ such that all vertices are good and G' contains a $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ grid as a minor.

Proof. From Claim 14, we know that S contains $o(|S|)$ bad vertices. Let us remove all these bad vertices, and write S_{good} the remaining set. We further remove all vertices $u \in S_{good}$ such that $\bar{u} \notin S_{good}$. The remaining set of vertices induces a graph $H \times K_2$, for an induced subgraph H of G such that $|H| \geq (1 - 2\epsilon - o(1))|G|$. From Lemma 8, when ϵ is taken small enough, the graph $H \times K_2$ has a connected component $G' \times K_2$, where G' is contains a $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ grid as a minor.   ◁

Remember the definition of a graph minor (Definition 2 in Section 2.1). Each connected subgraph G_u in G' forming the grid (except connected subgraphs on the corners of the grid) is adjacent to the four connected subgraphs $G_{v_1}, G_{v_2}, G_{v_3}, G_{v_4}$ where $\{u, v_1\}$, $\{u, v_2\}$, $\{u, v_3\}$ and $\{u, v_4\}$ are edges of the grid. For each G_u, we arbitrarily select two of these four components. Assume for instance that we selected G_{v_1} and G_{v_2}. We choose arbitrarily one vertex v in G_u adjacent to a vertex of G_{v_1}, and one vertex w in G_u adjacent to a vertex of G_{v_2}. We then arbitrarily choose one path inside G_u that connects v and w (such a path necessarily exists). We refer to Figure 3 for an illustration.

We denote T the length of one side of the grid (T $= \Omega(|V|^{\frac{1}{4}})$). From each connected subgraph forming the $T \times T$ grid of G', we choose one vertex such that it is on a path selected in the way above (this condition of the vertices is required when adding missing segments inside boxes for Claim 18). For such a vertex j, we define $\text{Box}(j) \subseteq G' \times K_2$ as a 2D grid of connected subgraphs of size $\lfloor |V|^{\frac{1}{8}} \rfloor \times \lfloor |V|^{\frac{1}{8}} \rfloor$ centered at the connected subgraph which j' and j'' belong to. We choose grid-shaped regions $P, Q, R \subseteq G' \times K_2$ as shown in Figure 4. P is a upper-left region of the graph product of K_2 and a $\lfloor T/3 \rfloor \times \lfloor T/3 \rfloor$ grid of connected subgraphs cut from $G' \times K_2$. Q is a upper-right region and R is a bottom-left region. The following claim is similar to Claim 6 in [14].
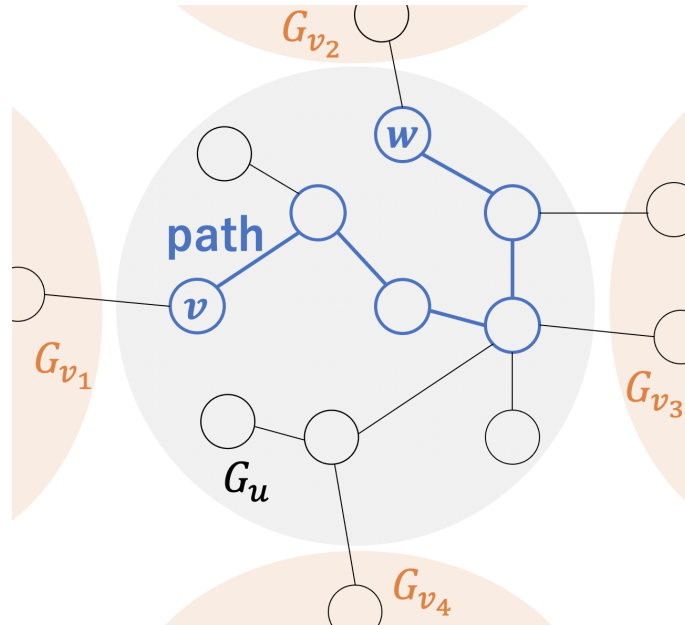
Figure 3 The path in G_u described with blue line connects G_{v_1} and G_{v_2}.
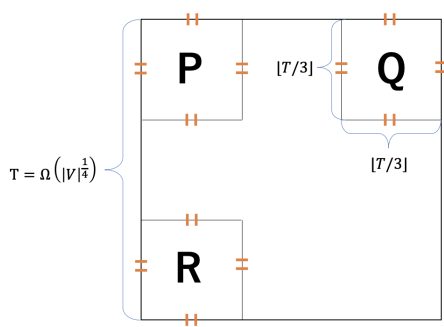
Figure 4 Definition of the regions P, Q, R of $G' \times K_2$.
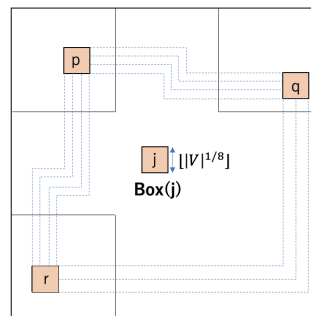
Figure 5 Definition of $\text{Box}(j)$ and a possible choice of p, q, r.

▷ **Claim 17.** For all large enough $|V|$, we can choose a triple of vertices $p, q, r \in V$ such that $p', p'' \in P$, $q', q'' \in Q$, $r', r'' \in R$ and

$$\mathrm{Box}(p) \subseteq P, \ \mathrm{Box}(q) \subseteq Q, \ \mathrm{Box}(r) \subseteq R, \tag{3}$$

$$L_C(x_{p'} \cup x_{p''}) \cap \mathrm{Box}(q) = \emptyset, \ L_C(x_{p'} \cup x_{p''}) \cap \mathrm{Box}(r) = \emptyset, \tag{4}$$

$$L_C(x_{q'} \cup x_{q''}) \cap \mathrm{Box}(p) = \emptyset, \ L_C(x_{q'} \cup x_{q''}) \cap \mathrm{Box}(r) = \emptyset, \tag{5}$$

$$L_C(x_{r'} \cup x_{r''}) \cap \mathrm{Box}(p) = \emptyset, \ L_C(x_{r'} \cup x_{r''}) \cap \mathrm{Box}(q) = \emptyset. \tag{6}$$

Proof. One connected subgraph in the grid minor can belong to at most $|V|^{\frac{1}{8}} \times |V|^{\frac{1}{8}} = |V|^{\frac{1}{4}}$ boxes. Since the vertices in $G' \times K_2$ are good, a given lightcone $L_C(x_{u'} \cup x_{u''})$ can intersect with at most $|V|^{\frac{1}{4}} \times |L_C(x_{u'} \cup x_{u''})| = |V|^{\frac{1}{4}} \times O(|S|^{\frac{1}{16}}) = O(|V|^{\frac{5}{16}})$ boxes. The number of possibilites to choose a box in Q is $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}}) = \Omega(|V|^{\frac{1}{2}})$. Thus if we pick boxes uniformly at random then

$$\Pr[L_C(x_{p'} \cup x_{p''}) \cap \mathrm{Box}(q) = \emptyset] \leq O\left(\frac{|V|^{\frac{5}{16}}}{|V|^{\frac{1}{2}}}\right) < \frac{1}{6} \tag{7}$$

for large enough $|V|$. A similar bound applies to the five others that appear in the three equations (4, 5, 6). By the union bound, there exists at least one choice of p, q, r that satisfies all the four equations (3, 4, 5, 6). ◁

Below we consider a cycle Γ that is a subgraph of $G' \times K_2$. The following claim is similar to Claim 7 in [14].

▷ **Claim 18.** The following holds for all sufficiently large $|V|$. Fix some triple of vertices p, q, r satisfying the four equations (3, 4, 5, 6). Then there exists an even length cycle Γ containing $p', p'', q', q'', r', r''$ such that the lightcones $L_C(x_{p'} \cup x_{p''})$, $L_C(x_{q'} \cup x_{q''})$, $L_C(x_{r'} \cup x_{r''})$ contain no vertices of Γ lying outside of $\mathrm{Box}(p) \cup \mathrm{Box}(q) \cup \mathrm{Box}(r)$.

Proof. Since the size of connected subgraphs of each box is $\lfloor |V|^{\frac{1}{8}} \rfloor \times \lfloor |V|^{\frac{1}{8}} \rfloor$, we can choose $\lfloor |V|^{\frac{1}{8}} \rfloor$ pairwise vertex disjoint paths γ that connect any pair of boxes $\mathrm{Box}(p), \mathrm{Box}(q), \mathrm{Box}(r)$ (in each connected subgraph, we can always find a path which connects adjacent connected subgraphs). We refer to Figure 5 for an illustration. Let $\gamma(a, b)$ be a path connecting $\mathrm{Box}(a)$ and $\mathrm{Box}(b)$, where $a \neq b \in \{p, q, r\}$. Any triple of paths $\gamma(p, q), \gamma(q, r), \gamma(p, r)$ can be completed to a cycle Γ by adding the missing segments of the cycle inside the boxes $\mathrm{Box}(p)$, $\mathrm{Box}(q)$, $\mathrm{Box}(r)$ because p, q, r are defined to take such a path inside each box. Since all vertices are good in $G' \times K_2$ and each connected subgraph belongs to at most one path γ, we infer that $L_C(x_{p'} \cup x_{p''})$ intersects with at most $2 \cdot O(|S|^{\frac{1}{16}}) = O(|V|^{\frac{1}{16}})$ paths γ. Thus if we pick the path $\gamma(p, q)$ uniformly at random among all $\lfloor |V|^{\frac{1}{8}} \rfloor$ possible choices then

$$\Pr[L_C(x_{p'} \cup x_{p''}) \cap \gamma(p, q) \neq \emptyset] \leq O\left(\frac{|V|^{\frac{1}{16}}}{|V|^{\frac{1}{8}}}\right) < \frac{1}{9} \tag{8}$$

for enough large $|V|$. The same bound applies to eight remaining combinations of lightcones $L_C(x_{p'} \cup x_{p''}), L_C(x_{q'} \cup x_{q''}), L_C(x_{r'} \cup x_{r''})$ and paths $\gamma(p, q)$, $\gamma(p, r)$, and $\gamma(q, r)$. By the union bound, there exists at least one triple of paths $\gamma(p, q), \gamma(q, r), \gamma(p, r)$ that do not intersect with $L_C(x_{p'} \cup x_{p''}), L_C(x_{q'} \cup x_{q''}), L_C(x_{r'} \cup x_{r''})$. When we choose v' and v'' consecutively, any cycle in $G' \times K_2$ has an even length. Since we can take the cycle in the way above, the cycle has a even length and is the desired cycle Γ. ◁

Let p, q, r and Γ be chosen as described in Claim 18. Let M be the even number of vertices of Γ. When we choose $p', p'', q', q'', r', r''$ properly, the distances between p', q', r' are all even. Consider the subset of instances where

$$x_e = \begin{cases} 1 & \text{if } e \text{ is an edge of } \Gamma \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad x_v = 0 \text{ if } (v \in V \setminus \{p', q', r'\})$$

There are $2^3 = 8$ such instances corresponding to choices of input bits $x_{p'}, x_{q'}, x_{r'} \in \{0, 1\}$. Let us fix inputs x of the circuit C except $\{x_{p'}, x_{q'}, x_{r'}\}$ and consider only output bits z_j with $j \in \Gamma$. By the way of fixing, we obtain a classical circuit D which takes a three-bit string $x_{p'} x_{q'} x_{r'} \in \{0, 1\}^3$ and a random string r as input and output $z_\Gamma \in \{0, 1\}^M$. For any input bit $x_i \in \{x_{p'}, x_{q'}, x_{r'}\}$ we have $L_D(x_i) \subseteq L_C(x_i)$ since any pair of input and output variables which are correlated in D are also correlated in C, by definition. Our assumption that C can solve $\rho(S)$ on all inputs implies that D can output $z_\Gamma \in \tau(x_{p'} x_{q'} x_{r'})$. From Lemma 10, at least one output bit z_j such that $j \in \Gamma$ and $j \notin \{p', q', r'\}$ depends on the two geometrically near inputs from $x_{p'}, x_{q'}, x_{r'}$. By $L_D(x_i) \subseteq L_C(x_i)$, the same is true for the input-output dependency of C. From Claim 9, for each x_i, $L_C(x_i)$ only intersects with z_j such that $j \in \text{Box}(i)$ and there is a contradiction. Therefore, the depth of any classical probabilistic circuit that has bounded fan-in K and solves $\rho(S)$ on all inputs is not less than $\frac{\log |S|}{32 \log K}$. This concludes the proof of Theorem 3.   ◄

───── **References** ─────

1   Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the 43rd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2011)*, pages 333–342, 2011.

2   Scott Aaronson and Alex Arkhipov. Bosonsampling is far from uniform. *Quantum Information & Computation*, 14(15–16):1383–1423, 2014.

3   Scott Aaronson and Lijie Chen. Complexity-Theoretic Foundations of Quantum Supremacy Experiments. In *Proceedings of 32nd Computational Complexity Conference (CCC 2017)*, volume 79 of *LIPIcs*, pages 22:1–22:67, 2017.

4   Andris Ambainis. Understanding quantum algorithm via query complexity. In *Proceedings of the International Congress of Mathematicians (ICM 2018)*, pages 3265–3285, 2019.

5   Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 32(6):818–830, 2013.

6   Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

7   Jonathan Barrett, Carlton M. Caves, Bryan Eastin, Matthew B. Elliott, and Stefano Pironio. Modeling pauli measurements on graph states with nearest-neighbor classical communication. *Physical Review A*, 75(1):012103, 2007.

8   Ya. M. Barzdin. On the realization of networks in three-dimensional space. In *Selected Works of A. N. Kolmogorov: Volume III: Information Theory and the Theory of Algorithms*, pages 194–202. Springer, 1993.

9   Adam Bene Watts, Robin Kothari, Luke Schaeffer, and Avishay Tal. Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019)*, pages 515–526, 2019.

10 Jan Benhelm, Gerhard Kirchmair, Christian F. Roos, and Rainer Blatt. Towards fault-tolerant quantum computing with trapped ions. *Nature Physics*, 4(6):463–466, 2008.

11 Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

12 Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

13 Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. "Quantum Supremacy" and the Complexity of Random Circuit Sampling. In *Proceedings of 10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *LIPIcs*, pages 15:1–15:2, 2019.

14 Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

15 Sergey Bravyi, David Gosset, Robert König, and Marco Tomamichel. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16(10):1040–1045, 2020.

16 Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011.

17 Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical Review Letters*, 117(8):080501, 2016.

18 Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1:8, 2017.

19 Michael Capalbo, Omer Reingold, Salil Vadhan, and Avi Wigderson. Randomness conductors and constant-degree lossless expanders. In *Proceedings of the 34th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2002)*, pages 659–668, 2002.

20 Julia Chuzhoy and Rachit Nimavat. Large minors in expanders. *arXiv*, 2019. `arXiv:1901.09349`.

21 Matthew Coudron, Jalex Stark, and Thomas Vidick. Trading locality for time: certifiable randomness from low-depth circuits. *Communications in Mathematical Physics*, 382(1):49–86, 2021. Also presented at QIP 2019.

22 Ronald De Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002.

23 Reinhard Diestel. *Graph theory*, volume 173 of *Graduate texts in mathematics*. Springer, 2000.

24 Andreas Wallraff et al. Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics. *Nature*, 431(7005):162–167, 2004.

25 Richard P Feynman. Simulating physics with computers. *Int. J. Theor. Phys*, 21(6/7):467–488, 1982.

26 François Le Gall. Average-Case Quantum Advantage with Shallow Circuits. In *Proceedings of 34th Computational Complexity Conference (CCC 2019)*, volume 137 of *LIPIcs*, pages 21:1–21:20, 2019.

27 Daniel Grier, Nathan Ju, and Luke Schaeffer. Interactive quantum advantage with noisy, shallow clifford circuits. *arXiv*, 2021. `arXiv:2102.06833`.

28 Daniel Grier and Luke Schaeffer. Interactive shallow clifford circuits: quantum advantage against NC^1 and beyond. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2020)*, pages 875–888, 2020.

29 Misha Gromov and Larry Guth. Generalizations of the kolmogorov–barzdin embedding estimates. *Duke Mathematical Journal*, 161(13):2549–2603, 2012.

30 Marc Hein, Jens Eisert, and Hans J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6):062311, 2004.

31 Emmanuel Kowalski. *An introduction to expander graphs*. Société Mathématique de France, 2019.

32 Michael Krivelevich. Expanders – how to find them, and what to find in them. *Surveys in Combinatorics*, pages 115–142, 2019.

33 Michael Krivelevich and Benjamin Sudakov. Minors in expanding graphs. *Geometric and Functional Analysis*, 19(1):294–331, 2009.

34 Hoi-Kwong Lo. Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity. *Physical Review A*, 62(1):012313, 2000.

35 N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838, 1990.

36 Yasunobu Nakamura, Chii Dong Chen, and Jaw Shen Tsai. Spectroscopy of energy-level splitting between two macroscopic quantum states of charge coherently superposed by josephson coupling. *Physical Review Letters*, 79(12):2328, 1997.

37 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

38 Jeremy L O'Brien. Optical quantum computing. *Science*, 318(5856):1567–1570, 2007.

39 Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.

40 John Preskill. Quantum computing and the entanglement frontier. *Bulletin of the American Physical Society*, 58, 2013.

41 John Preskill. Quantum computing in the NISQ era and beyond. *Quantum*, 2:79, 2018.

42 Ran Raz and Avishay Tal. Oracle separation of BQP and PH. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019)*, pages 13–23, 2019.

43 Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

44 Barbara M. Terhal and David P. DiVincenzo. Adptive quantum computation, constant depth quantum circuits and arthur-merlin games. *Quantum Information & Computation*, 4(2):134–145, 2004.

45 Jian-Qiang You and Franco Nori. Atomic physics and quantum optics using superconducting circuits. *Nature*, 474(7353):589–597, 2011.

46 Han-Sen Zhong et al. Quantum computational advantage using photons. *Science*, 370:1460–1463, 2020.

A   Proof of Lemma 8

First, we introduce a notation. The range in Definition 6, $1 \leq |U| \leq \frac{1}{2}|V|$, may be a little arbitrary. In terms of the range where the expansion ratio is considered, we define more general expander graphs as follows.

▶ **Definition 19** (Definition 2.2 in [32])**.** *Let $G = (V, E)$ be a graph, let I be a set of positive integers. The graph G is an I-expander if a positive constant h exists such that $N_G(U) \geq h|U|$ for every vertex subset $U \subset V$ satisfying $|U| \in I$.*

Note that this definition does not limit the maximum degree of graphs. When the graph G is an expander graph (as defined as Definition 7), G is also a $\left[1, \frac{|V|}{2}\right]$-expander with bounded degree.

Then, the following claim shows an expander graph still has a large connected component and it can be described using the notation of Definition 19 when a small fraction of vertices are adversarially removed.

▷ **Claim 20.** Let $G = (V, E)$ be an expander graph. If we take a sufficiently small constant $\epsilon > 0$, the graph has a connected component C which has more than $\frac{|V|}{2}$ vertices and is a $\left[\frac{|C|}{3}, \frac{2|C|}{3}\right]$-expander after up to an ϵ fraction of the vertices are adversarially removed.

Proof. Let h be the expansion ratio and d be the maximum degree of the graph G. Let $V' \subset V$ be an arbitrary subset of vertices such that $|V'| \leq \epsilon|V|$. Let $C_1, ..., C_m$ be the connected components of the left graph after $|V'|$ vertices are adversarially removed.

To reach a contradiction, we assume every connected component is equal to or smaller than half of $|V|$, i.e., for all i, $|C_i| \leq \frac{|V|}{2}$. From $|V \setminus V'| + |V'| = |V|$, $|V \setminus V'| = |V| - |V'| \geq (1-\epsilon)|V|$. Each connected component C_i has its neighbor $N_G(C_i)$ such that $|N_G(C_i)| \geq h|C_i|$ since $|C_i| \leq \frac{|V|}{2}$. A vertex can be a neighbor of at most d connected components at the same time. Therefore, by the summation of neighbors of all connected components C_i,

$$|N_G(V \setminus V')| \geq \frac{h|V \setminus V'|}{d} \geq \frac{h}{d}(1 - \epsilon)|V|.$$

In terms of the total number of vertices, $|V \setminus V'| + |N_G(V \setminus V')| \leq |V|$. Then,

$$\epsilon|V| \geq |V'| = |V| - |V \setminus V'| \geq |N_G(V \setminus V')| \geq \frac{h}{d}(1 - \epsilon)|V|.$$

Thus, $\epsilon \geq \frac{\frac{h}{d}}{1+\frac{h}{d}}$ and this contradicts ϵ is sufficiently small. Therefore we can pick a connected component C such that $|C| > \frac{|V|}{2}$ from $C_1, ..., C_m$.

In the graph C, we consider an arbitrary subset of vertices W, which satisfies $\frac{|C|}{3} \leq W \leq \frac{2|C|}{3}$. From the expander property of G, $|N_G(W)| \geq \frac{h|C|}{3} > \frac{h|V|}{6}$. Since the number of removed vertices is up to $\epsilon|V|$, $|N_C(W)| > \left(\frac{h}{6} - \epsilon\right)|V|$. If we take ϵ smaller than $\frac{h}{6}$, C is a $\left[\frac{|C|}{3}, \frac{2|C|}{3}\right]$-expander. $\triangleleft$

The next claim is to show there is a relation between I-expanders of Definition 5.

$\triangleright$ **Claim 21** (Lemma 2.4 in [32]). Let graph $G = (V, E)$ be a $\left[\frac{|V|}{3}, \frac{2|V|}{3}\right]$-expander. Then there is a vertex subset $Z \subset V$ such that $|Z| < \frac{|V|}{3}$ and the graph $G' = G[V \setminus Z]$ is a $\left[1, \frac{|G'|}{2}\right]$-expander.

The most significant result of minors of expander graphs is Claim 22 below. It is known that this bound ($O(\frac{|V|}{\log(|V|)})$) is tight especially in terms of the size of grid minors.

$\triangleright$ **Claim 22** (Corollary 8.3 in [32] and Theorem 1.1 in [20]). Let graph $G = (V, E)$ be a $\left[1, \frac{|V|}{2}\right]$-expander. For any graph H with $O(\frac{|V|}{\log(|V|)})$ vertices and edges, G contains H as a minor.

Finally, using the above claims, we can prove Lemma 8.

Proof of Lemma 8. From Claim 20, after the removal, the left graph has a connected component C which is a $\left[\frac{|C|}{3}, \frac{2|C|}{3}\right]$-expander. Using Claim 21, C contains an induced subgraph C' such that C' is a $\left[1, \frac{|C'|}{2}\right]$-expander and $|C'| > \frac{2|C|}{3} > \frac{|V|}{3}$. When n is sufficiently large, $\frac{n}{\log(n)} \gg n^{\frac{1}{2}}$. Therefore, from Claim 22, C contains a $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ grid as a minor since the maximum degree of grid graphs is 4, which is a constant, and the number of vertices and edges of a $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ grid is $\Omega(|V|^{\frac{1}{2}})$. $\blacktriangleleft$