Electronic Colloquium on Computational Complexity, Report No. 127 (2024)

Anti-Concentration for the Unitary Haar Measure and Applications to Random Quantum Circuits

Bill Fefferman[*1], Soumik Ghosh[†1], and Wei Zhan[‡1]

[1]Department of Computer Science, The University of Chicago, Chicago, Illinois 60637, USA

Abstract

We prove a Carbery-Wright style anti-concentration inequality for the unitary Haar measure, by showing that the probability of a polynomial in the entries of a random unitary falling into an ε range is at most a polynomial in ε. Using it, we show that the scrambling speed of a random quantum circuit is lower bounded: Namely, every input qubit has an influence that is at least exponentially small in depth, on any output qubit touched by its lightcone.

We give three applications of this new scrambling speed lower bound that apply to random quantum circuits with Haar random gates:

- An optimal $\Omega(\log \varepsilon^{-1})$ depth lower bound for ε-approximate unitary designs;
- A polynomial-time quantum algorithm that computes the depth of a bounded–depth circuit, given oracle access to the circuit;
- A polynomial-time algorithm that learns log-depth circuits up to polynomially small diamond distance, given oracle access to the circuit.

The first depth lower bound works against any architecture. The latter two algorithms apply to architectures defined over any geometric dimension, and can be generalized to a wide class of architectures with good lightcone properties.

[*]wjf@uchicago.edu
[†]soumikghosh@uchicago.edu
[‡]weizhan@uchicago.edu

ISSN 1433-8092

1 Introduction

Random quantum circuits are one of the most popular paradigms of quantum computation in the near–term era. They are well–studied, both theoretically and experimentally, in the context of quantum advantage demonstrations: e.g., see [Boi+18; Bou+18; Aru+19; Bou+22; Mor+23; Mov23; Fef+23]. They also have numerous applications in areas like benchmarking, like in [Dan+09; Liu+22], in cryptography, as in e.g., [Bas+24; AH23; SHH24], and in the modeling of physical objects like black holes, as in e.g., [HP07; PSQ20; YE23].

One reason random quantum circuits are extensively studied is because they are rapid "scramblers" of information. Intuitively, this means that the output state it generates has non–trivial correlations across spatially separated qubits. The rate of scrambling depends on the depth—the deeper the circuit is, the better it is at scrambling. For a more thorough summary of scrambling and speed of scrambling, especially with respect to quantitative metrics like OTOCs and entanglement, see, e.g., [HL09; BF13; NVH18; Har+21; JBS22; Che+24a; Che+24b; HLT24; Met+24].

In this work, we give a lower bound on the speed with which random quantum circuits can scramble information. In particular, our main result gives a lower bound on the influence of an output qubit inside the lightcone of an input qubit and shows that it decays exponentially with depth. Intuitively, this means that the output state of random quantum circuits with logarithmic depth carries a signal pertaining to its input state that can be extracted from the output state using single qubit quantum state tomography. Our cornerstone theorem is a Carbery-Wright style anti-concentration inequality for the unitary Haar measure, which says that the values of any polynomial, defined on the entries of a Haar random unitary, are not too concentrated and in particular are typically not "too small."

As applications, we utilize the optimality of our metric to put a new lower bound on the depth required for approximate unitary k–designs using random quantum circuits. Additionally, given black box access to a randomly sampled circuit of bounded but unknown depth, we use our metric to compute the depth of that circuit. Finally, we use the metric to postulate a new learner for random quantum circuits. The time complexity of the learner scales exponentially with the depth of the circuit.

Informally, many of our applications—for instance, those pertaining to lower bounds on approximate designs and depth-testing—can be interpreted as a generalization of those arising out of simpler tests, like the swap test, which detect the amount of entanglement between two systems see, e.g., [Buh+01; JLS18; Aar+23]. However, in the context of random circuits, optimality results for the swap test have only been proven for specific architectures, like in 1D [Nah+17a]. Moreover, such tests do not have good typicality guarantees for bounded–depth circuits. Our results not only work for a wide variety of architectures over any geometric dimension, but they also have good typicality guarantees, which we prove using our Carbery-Wright style anti-concentration inequality.

Our lower bound on scrambling speed can also be viewed as a converse of the Lieb-Robinson bounds in quantum information theory [LR72; CL21; WW22; CLY23] for random circuits. The Lieb-Robinson bounds put upper limits on how fast information is propagated in local quantum systems, while one can interpret our result as saying in a typical random

quantum circuit, information is indeed propagated with a speed lower bound, determined by the locality properties of the circuit.

1.1 Main Results and Applications

Here we state our main theorem as follows.

Theorem 1.1. *Let $\mathcal{C}$ be a random quantum circuit with a fixed architecture, where each gate is a k-qubit independent Haar random unitary. Let ρ and π be a pair of input and output qubits that are depth D apart. Arbitrarily fix the inputs to $\mathcal{C}$ except the qubit ρ, and let $\Phi_{\mathcal{C}}$ be the channel that maps ρ to π.*

Then for every $\gamma > 0$, with probability at least $1-\gamma$ over $\mathcal{C}$ the following holds: For every two single-qubit states ρ and ρ',

$$\left\|\Phi_{\mathcal{C}}(\rho) - \Phi_{\mathcal{C}}(\rho')\right\|_{\mathrm{F}} \geq \left\|\rho - \rho'\right\|_{\mathrm{F}} \cdot (2^{-D}\gamma)^{c_k}$$

where $c_k > 0$ is a constant that depends only on k.

In words, Theorem 1.1 means that the changes in the input qubit have influences on the output qubit that decays at most exponentially fast in depth. Moreover, the influences are uniformly bounded, such that the ratio $(2^{-D}\gamma)^{c_k}$ does not depend on how the input qubits are chosen or even the circuit architecture, which is important for some of our applications below.

We note that our bound in Theorem 1.1 is tight, in the sense that a matching upper bound $\left\|\Phi_{\mathcal{C}}(\rho) - \Phi_{\mathcal{C}}(\rho')\right\|_{\mathrm{F}} \leq \left\|\rho - \rho'\right\|_{\mathrm{F}} \cdot (2^{-D}\gamma)^{c'_k}$ can be shown for a different constant $c'_k < c_k$ when D is small. This is implied by the results in [HL09; BF13; Nah+17b] for various architectures, proved via analyzing the Markov chain of Pauli operators.

We present several applications of Theorem 1.1. To start off, we show that Theorem 1.1 directly implies a depth lower bound for random quantum circuits with any architecture being approximate unitary designs; see Section 5.1.

Theorem 1.2. *Let $\mathcal{C}$ be a random quantum circuit with a fixed architecture of minimum depth D, where each gate is a k-qubit independent Haar random unitary. If $\mathcal{C}$ is an ε-approximate 2-design, then $D \geq \Omega_k(\log \varepsilon^{-1})$.*

Here the minimum depth means that any path from input to output must go through D gates; see Definition 2.1. Note that a brickwork circuit of depth 1 is already an 1-design, while the lower bound for 2-design also holds for t-designs when $t > 2$. Combining Theorem 1.2 with the $\Omega(\log n)$ depth lower bound in [DHB22a; SHH24], it shows that the approximate t-design construction of depth $O(\log(n/\varepsilon) \cdot t \operatorname{polylog} t)$ from [SHH24] is optimal in both n and ε, assuming the gates are Haar random unitaries.

Our second application concerns testing the depth of a random circuit when the depth is at most logarithmic; see Section 5.2 and Theorem 5.2.

Theorem 1.3. *Let $\mathcal{C}$ be a brickwork random quantum circuit on n qubits of an unknown depth $D = O(\log n)$, where each gate is independently Haar random. Given oracle access to $\mathcal{C}$, there is a polynomial time algorithm that outputs D with probability $1 - 1/\mathrm{poly}(n)$.*

Although Theorem 1.3 is stated with brickwork circuits for simplicity, it is applicable to much more general architectures; see the remark at the end of Section 5.2. Note that our algorithm outputs the exact depth instead of obtaining an approximation, in contrast to the recently proposed depth test algorithm in [HG24].

For our third application, we show that Theorem 1.1 allows us to learn brickwork random circuits of logarithmic depth. We start by showing that the first layer of gates can be learned given oracle access to the circuit.

Theorem 1.4. *Let $\mathcal{C}$ be a brickwork random quantum circuit on n qubits of known depth $D = O(\log n)$, where each gate is independently Haar random. Given oracle access to $\mathcal{C}$, there is a polynomial time algorithm that with high probability outputs each gate in the first layer with polynomially small error.*

Furthermore, in real life scenarios we can assume the distribution over the gates is a discrete approximation of the Haar measure (see Definition 5.7), and in this case we can actually learn the entire circuit:

Theorem 1.5. *Let $\mathcal{C}$ be a brickwork random quantum circuit on n qubits of known depth $D = O(\log n)$, where each gate is independently drawn from a discretized version of the Haar measure. Given oracle access to $\mathcal{C}$, there is a polynomial time algorithm that with high probability outputs $\mathcal{C}$ with polynomially small error.*

We will prove Theorem 1.4 and Theorem 1.5 in Section 5.3. Note that the learning algorithm in Theorem 1.4 is proper, that the outputted circuit has the exact same depth and architecture as the actual circuit $\mathcal{C}$. Furthermore, the $O(\log n)$ depth in Theorem 1.5 (and also Theorems 1.3 and 1.4) is optimal, if we assume that super-logarithmic-depth random circuits are pseudo-random unitaries.

Before this work, the state-of-art learning algorithm for brickwork quantum circuits is due to [Hua+24], which runs in polynomial time for circuits of k-dimensional geometry up to $O(\log^{1/(k+1)} n)$ depth. Our algorithm works for all geometric dimensions, and still has improved efficiency even for 1-dimensional brickwork circuits. The reason that we have to work with the discretized version instead of the Haar measure itself is due to a technical difficulty, and proving Theorem 1.5 for more general gate sets remains open.

1.2 Main Technical Tool: Anti-Concentration for Haar Measure

The intuition behind the proof of Theorem 1.1 is the following: We consider the path of $D+1$ qubits $\rho = \rho_0, \rho_1, \ldots, \rho_D = \Phi_{\mathcal{C}}(\rho)$ in the circuit $\mathcal{C}$, where gate G_i has ρ_i as an input and ρ_{i+1} as an output. Let ρ'_i be the corresponding qubits when the input is ρ', and we want to bound the ratios $\lambda_i = \left\|\rho_i - \rho'_i\right\|_{\mathrm{F}} / \left\|\rho_{i-1} - \rho'_{i-1}\right\|_{\mathrm{F}}$ and hence their product.

It turns out that we can prove the lower bound $\lambda_i \geq |F(G_i)|$, where F is a polynomial function over the entries of G_i in its matrix representation. Therefore, we only need to show that $|F(G_i)|$ is often not too small, when G_i is a Haar random unitary. In other words, we need to show that the polynomial does not concentrate around zero. Our main technical contribution is the following theorem which proves this anti-concentration phenomenon:

Theorem 1.6. *Let U be a Haar random $n \times n$ unitary matrix, and let $F : \mathbb{C}^{2n^2} \to \mathbb{C}$ be a degree-d polynomial on the entries of U and $U^\dagger$. Then for every $\varepsilon > 0$, it holds that*

$$\Pr\Big[\big|F(U,U^\dagger)\big|^2 \leq \varepsilon\, \mathbf{E}\big[|F(U,U^\dagger)|^2\big]\Big] \leq C'(n,d)\cdot \varepsilon^{C(n,d)}$$

where $C(n,d) > 0$ and $C'(n,d) > 0$ are constants that depend only on n and d.

The anti-concentration inequality of polynomials over Gaussian random variables was famously proved by Carbery and Wright [CW01], and their result actually applies to any log-concave distribution over $\mathbb{R}^n$. However, as the Haar measure does not even have a convex support, the proof techniques in [CW01] does not apply. We present a very different inductive proof in Section 3.

Note that if we consider $F(U,U^\dagger)$ as a complex random variable, and define the complex variance

$$\mathbf{Var}[F] = \mathbf{E}[|F|^2] - |\mathbf{E}[F]|^2 = \min_{z\in\mathbb{C}} \mathbf{E}[|F-z|^2],$$

then we obtain the form closer to the classical anti-concentration inequalities:

Corollary 1.7. *Let U be a Haar random $n \times n$ unitary matrix, and let F be a degree-d polynomial on the entries of U and $U^\dagger$. Then for every $\varepsilon > 0$ and every $z \in \mathbb{C}$, it holds that*

$$\Pr\big[|F-z|^2 \leq \varepsilon \mathbf{Var}[F]\big] \leq C'(n,d)\cdot \varepsilon^{C(n,d)}.$$

However in this work we will not use the form in Corollary 1.7, as Theorem 1.6 suffices for our applications.

Remark. Unlike the Carbery-Wright inequality which is dimension-free, meaning the right hand side is $C'(d)\cdot\varepsilon^{C(d)}$ and does not depend on n, we have $C(n,d) = (4n^2d)^{-1}$ and $C'(n,d) = O(n^3d)$ in our proof. In fact, using the concentration bounds it is not hard to show that $C'(n,d)$ must depends polynomially on n. However, we conjecture that $C(n,d)$ could be independent of n, in which case the result would be applicable to random quantum circuits with gates of higher locality.

1.3 Related Works

Concentration phenomenon on unitary Haar measures has been extensively studied, and the readers can refer to [Mec19] for a comprehensive review of the results. In comparison, much less has been shown for the reverse direction, namely the anti-concentration inequalities.

One common way to prove such inequalities is by calculating higher moments and apply the Paley-Zygmund inequality, which was indeed used for showing the anti-concentration property of *output distributions* of Haar random unitaries and random quantum circuits [AA11; Han+18; DHB22b]. However, the inequality proved this way is not strong enough for our applications, while calculating moments of a random quantum circuit is also non-trivial and depends highly on the architecture [Fis+23; Bra+24]. Instead, we resort to prove a general anti-concentration inequality for polynomials, whose theory has been well developed for Gaussian distributions [CW01] and product distributions (namely the Littlewood-Offord theory) and has found numerous applications in computational complexity theory [MZ13; MNV16; Kan17]. Our inductive proof of Theorem 1.6 also shares a similar spirit with the elementary proof of Carbery-Wright inequality in [Lov10].

Multiple notions of scrambling property of random quantum circuits has been previously studied. In particular, [BF13] showed that in a random circuit consists of $O(n \log^2 n)$ sequential applications of Haar random gates on a complete graph of n qubits, every subset of cn qubits is polynomially close to maximally mixed with high probability for some constant $c > 0$. Our Theorem 1.1 can be viewed as a result in the reverse direction which bounds the scrambling speed of such random circuits. Specifically, at least $\Omega(n \log n \log\log n)$ sequential gates are required, as otherwise with high probability a pair of input and output qubits are $o(\log n)$ depth apart due to a generalization of the coupon-collector problem [PR61]. It is also reasonable to believe that our method of proving Theorem 1.1, via the anti-concentration inequality, is applicable to obtain lower bounds for other measures of scrambling such as entanglement and out-of-time-ordered correlation (OTOC) [Nah+17b; NVH18; BP20; Har+21]. Upper bounds in the above-mentioned works are obtained by calculating moments and analyzing the averaged Markov chain on Pauli operators, which are not sufficient to prove lower bounds in the typical case.

We also review some previous works related to our applications and clarify the connections. For approximate unitary designs, many previous constructions, for example [HL09; BHH16; Haf22; HM23; Che+24c], employed Haar random unitary gates and achieved the optimal $O(\log \varepsilon^{-1})$ dependence on ε. The construction of depth $O(\log(n/\varepsilon) \cdot t \operatorname{polylog} t)$ in the recent work of [SHH24] also falls into this category. Meanwhile, they also proposed a construction of approximate 3-design with only $O(\log\log(n/\varepsilon))$ depth. This does not contradict our lower bound Theorem 1.2 as the construction uses random Clifford unitaries, which fails the anti-concentration property in Theorem 1.6. It is intriguing, however, to see if our argument can be extended to show a matching $\Omega(\log\log \varepsilon^{-1})$ depth lower bound.

The depth test algorithm in [HG24] is based on the entanglement dynamics of random circuits and implemented with their Bell sampling framework. For brickwork circuits, as there is a constant gap between the upper and lower bounds for the entanglement entropy in the typical case, their algorithm gives constant approximation of the depth. For general architectures, the algorithm in [HG24] also requires knowledge of the entanglement velocity, while our algorithm for Theorem 1.3 only relies on a specific property of the architecture that the lightcone strictly expands with depth.

The learning algorithm for shallow quantum circuits in [Hua+24] is based on the idea

of brute-force enumerating all possibilities in a light cone, and stitching the parts together. Therefore, their algorithm has complexity exponential in the lightcone size, which means that in order to have polynomial efficiency, the depth has to be $O(\log^{1/(k+1)} n)$ for k-dimensional geometrically local circuits and $O(\log \log n)$ for general architectures. Our algorithm does not work for general architectures, and also not for arbitrary gate sets. However, on brickwork and similar geometrically local circuits, where neighboring qubits can be distinguished by their lightcones, our algorithm Theorem 1.5 works up to logarithmic depth in polynomial time regardless of the dimension. Note that [Hua+24] also presented a polynomial time algorithm for log-depth circuits in 2D, with the catch that the learning algorithm is improper and will output circuits of polynomial depth.

We also mention that, there is a different learning task where instead given oracle access to the circuit $\mathcal{C}$, the learner is only given copies of the state $\mathcal{C}|0^n\rangle$, and needs to learn a circuit that prepares the same state with error in trace distance. Our algorithm relies on having different inputs and hence does not work in this case, whereas [Hua+24] gave a quasi-polynomial efficiency algorithm for 2D and the algorithm was extended to higher dimensions in [LL24].

2 Preliminaries

We start with some basic notations. We use $\mathbb{U}(d)$ to denote the unitary group of dimension d, and use $\mathcal{U}(d)$ to denote the Haar measure over $\mathbb{U}(d)$. We use Greek letters such as ρ, π, τ to denote density matrices of quantum states. We use $\|\cdot\|_1$ and $\|\cdot\|_{\mathrm{F}}$ for trace norm and Frobenius norm, and $d_\diamond(\cdot,\cdot)$ for diamond distance between unitary channels.

A circuit architecture determines the positions of gates in the circuit. We define the depth of an architecture as follows.

Definition 2.1. *In a circuit architecture, a path in space-time between two qubits ρ and ρ' is a sequence of qubits $\rho = \rho_0, \rho_1, \ldots, \rho_D = \rho'$ where for each i, there is a gate in the circuit that has ρ_i as an input and ρ_{i+1} as an output.*

We say ρ and ρ' are depth D apart if there exists a path of length D between ρ and ρ', and every other path between them also has length at least D. The architecture has minimum depth D if there exists a pair of input and output qubits that are depth D apart.

A specific architecture of interest is the (1-dimensional) brickwork architecture:

Definition 2.2. *A brickwork quantum circuit on n qubits of depth D consists of D layers of gates, where on layer j, there is a two-qubit gate $G_{i,j} = G_{i+1,j}$ acting on the i-th and $(i+1)$-th qubit if and only if i and j have the same oddity.*

The brickwork architecture could be generalized to higher dimensional geometry, and our results still hold for any constant dimension. However, for simplicity we stick with the 1-dimensional architecture in this paper.

We will need the following statements about quantum state tomography and quantum process tomography on single qubits for our algorithms (see e.g. [NC10])

Proposition 2.3. *Given access to copies of a single-qubit state ρ, one can output an estimation $\tilde{\rho}$ with $\|\rho - \tilde{\rho}\|_{\mathrm{F}} \leq \varepsilon$ in $\mathrm{poly}(1/\varepsilon)$ time.*

Proposition 2.4. *Given access to copies of a single-qubit unitary U, one can output an estimation $\tilde{U}$ with $d_\diamond(U, \tilde{U}) \leq \varepsilon$ in $\mathrm{poly}(1/\varepsilon)$ time.*

The following simple lemma is particularly useful, which bounds the difference between states through a channel:

Lemma 2.5. *Let Φ be a quantum channel that takes k qubits as the input. For every input states ρ and ρ', we have*

$$\big\|\Phi(\rho) - \Phi(\rho')\big\|_{\mathrm{F}} \leq 2^{k/2}\big\|\rho - \rho'\big\|_{\mathrm{F}}.$$

Proof. Since quantum channels do not increase trace distance, we have

$$\big\|\Phi(\rho) - \Phi(\rho')\big\|_{\mathrm{F}} \leq \big\|\Phi(\rho) - \Phi(\rho')\big\|_1 \leq \big\|\rho - \rho'\big\|_1 \leq 2^{k/2}\big\|\rho - \rho'\big\|_{\mathrm{F}}. \qquad \square$$

As we are frequently dealing with differences between quantum states, here we present some facts about the space of such differences. We start from the Bloch sphere presentation of a single-qubit state:

$$\rho = \frac{1}{2}(I + r_x X + r_y Y + r_z Z), \qquad r_x, r_y, r_z \in \mathbb{R}, \quad r_x^2 + r_y^2 + r_z^2 \leq 1 \tag{1}$$

where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2}$$

Then the difference $\rho - \rho'$ between two single-qubit states can be written in the Pauli basis

$$\rho - \rho' = r_x X + r_y Y + r_z Z, \quad r_x^2 + r_y^2 + r_z^2 = \frac{1}{2}\big\|\rho - \rho'\big\|_{\mathrm{F}}^2 \leq 1. \tag{3}$$

Therefore, if we view $\rho - \rho'$ under the coordinate system $\sqrt{2} \cdot (r_x, r_y, r_z)$, then the set Δ_1 of all possible single-qubit differences can be identified with a ball of radius $\sqrt{2}$ in $\mathbb{R}^3$. The Euclidean space $\mathbb{R}^3$ is equipped with the standard trace inner product $\langle A, B\rangle = \mathrm{Tr}[A^\dagger B]$, so that the norm coincides with the Frobenius norm.

More generally, let Δ_k be the set of all possible differences between two k-qubit states ρ and ρ'. The difference $\rho - \rho'$ can be written as a real linear combination over the Pauli basis

$$\{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$$

where the identity is removed as $\mathrm{Tr}[\rho - \rho'] = 0$. Since the Pauli basis are orthonormal, we can think of Δ_k as a subset of the Euclidean space $\mathbb{R}^{4^k - 1}$ (although the set is much more complicated than a ball for $k > 1$). The Euclidean space is also equipped with the standard trace inner product and the Frobenius norm. As a result, a quantum channel Φ with k-qubit input and n-qubit output induces a linear map from Δ_k to Δ_n:

$$\rho - \rho' \mapsto \Phi(\rho) - \Phi(\rho'),$$

which is also a real linear map from $\mathbb{R}^{4^k - 1}$ to $\mathbb{R}^{4^n - 1}$.

3 Anti-concentration Bound

In this section we prove Theorem 1.6. For simplicity, we introduce the notion of *semi-polynomials*: A function is a degree-d semi-polynomial in complex variables $z_1, \ldots, z_n$, if it is a polynomial in $z_1, \ldots, z_n, \overline{z_1}, \ldots, \overline{z_n}$ of degree at most d. Now Theorem 1.6 is implied by the following more general form:

Theorem 3.1. *Let $m \le n$, and $F : \mathbb{C}^{nm} \to \mathbb{C}$ be a degree-d semi-polynomial. Suppose that F takes as inputs the entries of the first m columns of an $n \times n$ unitary matrix, and that the value of F is always a non-negative real number over this domain. Then for $U \sim \mathcal{U}(n)$,*

$$\Pr\big[F(U_{1,1}, \ldots, U_{n,m}) \le \varepsilon\, \mathbf{E}[F]\big] \le C'(n,m,d) \cdot \varepsilon^{C(n,m,d)}$$

holds for every $\varepsilon > 0$, where $C(n,m,d) > 0$ and $C'(n,m,d) > 0$ are constants that depend only on n, m and d.

To see that Theorem 3.1 implies Theorem 1.6, it suffices to take $m = n$ and notice that $|F|^2 = F\overline{F}$ is a degree-$2d$ semi-polynomial that is always non-negative. We prove Theorem 3.1 via induction, and the proof is divided into four stages.

3.1 $m = 1, n = 1$

We start with the simplest case when $m = n = 1$. In this case $F : \mathbb{C} \to \mathbb{C}$ is a single-variable degree-d semi-polynomial over the unit circle $\{z : |z| = 1\}$. Since $\overline{z} = 1/z$ over this domain, assuming $F \neq 0$ we can write F as

$$F(z) = G(z)/z^d$$

where $G(z) = \alpha(z - z_1)\cdots(z - z_{2d})$ is a degree $2d$ polynomial in z. Without loss of generality we can assume that $|\alpha| = 1$, and therefore

$$F(z) = |F(z)| = |G(z)| = |z - z_1| \cdots |z - z_{2d}|. \tag{4}$$

Then we can bound the expectation of F as

$$\mathbf{E}[F] \le \sup_{|z|=1} \prod |z - z_i| \le \prod (1 + |z_i|). \tag{5}$$

On the other hand, if $|z - z_i| > \delta \ge 0$ for some $|z| \le 1$, it is easy to show that

$$\frac{|z - z_i|}{1 + |z_i|} > \frac{\delta}{\delta + 2}. \tag{6}$$

Thus if $|z - z_i| > \delta$ holds for all $i = 1, \ldots, 2d$, then

$$F(z) = \prod |z - z_i| > \left(\frac{\delta}{\delta + 2}\right)^{2d} \prod (1 + |z_i|) \ge \left(\frac{\delta}{\delta + 2}\right)^{2d} \mathbf{E}[F]. \tag{7}$$

That means, if we take $\varepsilon = \left(\frac{\delta}{\delta+2}\right)^{2d}$, then $F(z) \le \varepsilon\,\mathbf{E}[F]$ only happens when z falls into one of the δ-balls around some z_i. Each δ-ball intersect with the unit circle as an arc of angle at most 4δ, and thus has measure at most $2\delta/\pi$ under the Haar measure over the unit circle. Therefore we conclude that

$$\begin{aligned}\Pr_{|z|=1}[F(z) \le \varepsilon\,\mathbf{E}[F]] &\le \min\{4d\delta/\pi, 1\} \\ &= \min\left\{\frac{8d}{\pi}\cdot\frac{\varepsilon^{1/(2d)}}{1-\varepsilon^{1/(2d)}}, 1\right\} \le \left(\frac{8d}{\pi}+1\right)\varepsilon^{1/(2d)}, \end{aligned} \tag{8}$$

and we can take $C(1,1,d) = 1/(2d)$ and $C'(1,1,d) = 8d/\pi + 1$.

3.2 $m = 1, n = 1$, Alternative Distribution

For the sake of later use, we also need a version where $z = u_1$ follows the distribution of the first coordinate of a Haar-random unit vector $(u_1, \ldots, u_n) \in \mathbb{C}^n$, $n \ge 2$. In this case $\overline{z} = 1/z$ no longer holds, and we need an alternative method.

For every $r \in \mathbb{R}$, $0 \le r \le 1$ we define

$$P(r) = \mathop{\mathbf{E}}_{|u_1|=r}[F(u_1)]$$

where the expectation is over a Haar-random $z \in \mathbb{C}$ with $|z| = r$. Notice that a monomial $u_1^k\overline{u_1}^\ell$ in F has expectation 0 unless $k = \ell$, and when $k = \ell$ we have $u_1^k\overline{u_1}^\ell = r^k$. That means $P(r)$ is a degree-d polynomial in r^2.

Notice that r^2 follows the Beta distribution $\mathrm{Beta}(1, n-1)$, with the density function

$$f(r; 1, n-1) = (n-1)(1-r)^{n-2},$$

and $\mathbf{E}[P(r)]$ under this distribution coincides with $\mathbf{E}[F]$.

With the analysis in the previous section which also works on $P(r)$, we can show that if we take $\varepsilon = \left(\frac{\delta}{\delta+2}\right)^{d}$, then $P(r) \le \varepsilon\,\mathbf{E}[P(r)] = \varepsilon\,\mathbf{E}[F]$ only happens when r^2 falls into one of the δ-balls around d complex roots of P, which are intervals of length at most 2δ on the real line. Since the density function of r^2 has a maximum of $n-1$, we have

$$\Pr[P(r) \le \varepsilon\,\mathbf{E}[F]] \le \min\{2d(n-1)\delta, 1\} \le 4dn\varepsilon^{1/d}. \tag{9}$$

On the other hand, applying (8) from the previous section on $F(rz)$ for every fixed r directly provides

$$\Pr_{|z|=r}[F(z) \le \varepsilon P(r)] \le \left(\frac{8d}{\pi}+1\right)\varepsilon^{1/(2d)}. \tag{10}$$

Thus by a union bound we have

$$\begin{aligned}\Pr[F(u_1) \le \varepsilon\,\mathbf{E}[F]] &\le \Pr\left[P(r) \le \sqrt{\varepsilon}\,\mathbf{E}[F]\right] + \Pr_{|z|=r}\left[F(z) \le \sqrt{\varepsilon}P(r)\right] \\ &\le 4dn\varepsilon^{1/(2d)} + \left(\frac{8d}{\pi}+1\right)\varepsilon^{1/(4d)} \\ &\le 4d(n+1)\varepsilon^{1/(4d)}. \end{aligned} \tag{11}$$

We note that not only this result will be used in the next stage, the technique itself will also be reapplied multiple times in the later proofs.

3.3 $m = 1, n > 1$

In this stage we consider $m = 1$ with general n, and thus the inputs to F is a Haar-random unit vector $(u_1, \ldots, u_n) \in \mathbb{C}^n$. The strategy is to use induction on n, and show that with high probability over the choice of u_1,

$$P(u_1) = \mathop{\mathbf{E}}_{u_2,\ldots,u_n}[F(u_1, \ldots, u_n)]$$

is not too small conditioned on the fixed u_1. To handle this, we need the following lemma.

Lemma 3.2. *If $F : \mathbb{C}^n \to \mathbb{C}$ is a degree-d semi-polynomial, and $(u_1, \ldots, u_n) \in \mathbb{C}^n$ is a Haar-random unit vector, then $P(u_1) = \mathbf{E}_{u_2,\ldots,u_n}[F(u_1, \ldots, u_n)]$ is a degree-d semi-polynomial on u_1.*

Proof. Consider each monomial in F, and let G be the part of monomial over $u_2, \ldots, u_n$ and their conjugates. Since $(u_2, \ldots, u_n) = r \cdot u'$, where $r = (1 - |u_1|^2)^{1/2}$ and u' follows the Haar measure over the unit sphere in $\mathbb{C}^{n-1}$, we have:

- If G has an odd degree then $\mathbf{E}[G] = 0$, by the symmetry $u' \to -u'$;
- And if G has an even degree $2\ell \le d$ then

$$\mathbf{E}[G] = r^{2\ell}\,\mathbf{E}[G(u')] = (1 - u_1\overline{u_1})^{\ell}\,\mathbf{E}[G(u')], \tag{12}$$

  where $\mathbf{E}[G(u')]$ is a constant irrelevant to the choice of u_1.

Either way $\mathbf{E}[G]$ is a degree-d semi-polynomial in u_1, and thus so is $P(u_1)$. □

Since P is an expectation over F, it is also always non-negative and has the same expectation as $\mathbf{E}[F]$. Thus (11) from the previous section gives

$$\Pr[P(u_1) \le \varepsilon\,\mathbf{E}[F]] \le 4d(n+1)\varepsilon^{1/(4d)}. \tag{13}$$

Now we fix some u_1, and consider the degree-d semi-polynomial

$$F_{u_1}(u_2, \ldots, u_n) = F(u_1, u_2, \ldots, u_n)$$

which is always non-negative. Since $(u_2, \ldots, u_n) = ru'$ for some $r \in \mathbb{R}$, and u' follows the Haar measure over the unit sphere in $\mathbb{C}^{n-1}$, we can apply the induction hypothesis for $n-1$ on $F_{u_1}(ru')$ to get

$$\Pr\big[F_{u_1}(ru') \le \varepsilon\,\mathbf{E}_{u'}[F_{u_1}(ru')]\big] \le C'(n-1, 1, d) \cdot \varepsilon^{C(n-1,1,d)}. \tag{14}$$

Therefore we conclude that, for every $p \in (0,1)$,

$$\begin{aligned}
&\Pr[F(u_1,\dots,u_n) \le \varepsilon\, \mathbf{E}[F]] \\
\le\ &\Pr[P(u_1) \le \varepsilon^p\, \mathbf{E}[F]] + \Pr\big[F(u_1,\dots,u_n) \le \varepsilon^{1-p} P(u_1)\big] \\
=\ &\Pr[P(u_1) \le \varepsilon^p\, \mathbf{E}[F]] + \Pr\big[F_{u_1}(u_2,\dots,u_n) \le \varepsilon^{1-p}\, \mathbf{E}[F_{u_1}]\big] \\
\le\ &4d(n+1)\varepsilon^{p/(4d)} + C'(n-1,1,d)\cdot \varepsilon^{(1-p)C(n-1,1,d)}. \qquad (15)
\end{aligned}$$

We can take

$$C(n,1,d) = \max_p \min\Big\{\frac{p}{4d}, (1-p)C(n-1,1,d)\Big\} = \frac{1}{4d + C(n-1,1,d)^{-1}} = \frac{1}{4nd},$$

and $C'(n,1,d) = 4d(n+1) + C'(n-1,1,d) = O(n^2 d)$.

3.4 $m > 1, n > 1$

Now we handle the general case when the inputs to the semi-polynomial consist of m columns of a Haar random unitary. The proof is similar to the last stage, using the fact that the input distribution can be viewed as a unitary-invariant distribution over m orthonormal vectors in $\mathbb{C}^n$. In particular, let the vectors be $v_1,\dots,v_m$, and we consider the function

$$P(v_1,\dots,v_{m-1}) = \mathop{\mathbf{E}}_{v_m}[F(v_1,\dots,v_m)].$$

Here v_m is a Haar-random vector over the unit sphere in the $(n-m)$-diemsnional orthogonal subspace of $\mathrm{span}(v_1,\dots,v_m)$. We would like to show that P is a semi-polynomial in order to use induction, and we first show it with v_m replaced with a Gaussian distribution.

Lemma 3.3. *Let $v_1,\dots,v_m$ be a set of $m < n$ orthonormal vectors in C^n, and let $g = (g_1,\dots,g_n) \in \mathbb{C}^n$ distributed as a standard $(n-m)$-dimensional complex Gaussian in the orthogonal subspace of* $\mathrm{span}(v_1,\dots,v_m)$.

Let $G : \mathbb{C}^n \to \mathbb{C}$ be a degree-d semi-polynomial in $(g_1,\dots,g_n)$. Then

$$Q(v_1,\dots,v_m) = \mathbf{E}[G(g_1,\dots,g_n)]$$

is a degree-d semi-polynomial in the entries of $v_1,\dots,v_m$.

Proof. Notice that $g = (g_1,\dots,g_n)$ can be obtained by taking a standard n-dimensional complex Gaussian $g' \in \mathbb{C}^n$, and apply the Gram-Schmidt orthogonalization:

$$g = g' - \sum_{i=1}^{m} v_i v_i^\dagger g'. \qquad (16)$$

Therefore the covariance matrix of g is $\left(I_n - \sum v_i v_i^\dagger\right)^2 = I_n - \sum v_i v_i^\dagger$, where each entry is a degree-2 semi-polynomial in $v_1,\dots,v_m$. By the complex Wick's theorem [FPR19], the expectation of a monomial in $G(g)$

$$\mathbf{E}\Big[g_1^{\alpha_1}\overline{g_1}^{\beta_1}\cdots g_n^{\alpha_n}\overline{g_n}^{\beta_n}\Big]$$

is non-zero only when $\sum \alpha_i = \sum \beta_i$, in which case it is a polynomial function over the entries of the covariance matrix of g with degree $\sum \alpha_i$. Therefore $Q = \mathbf{E}[G]$ is a degree-d semi-polynomial in the entries of $v_1, \ldots, v_m$. □

Corollary 3.4. *$P(v_1, \ldots, v_{m-1}) = \mathbf{E}_{v_m}[F(v_1, \ldots, v_m)]$ is a degree-d semi-polynomial in the entries of $v_1, \ldots, v_{m-1}$.*

Proof. Notice that v_m is equidistributed as $g/\|g\|_2$, where $g = (g_1, \ldots, g_n)$ is the Gaussian in Lemma 3.3. In other words, $g = r \cdot v_m$ where $r \in \mathbb{R}$ follows a fixed χ distribution independent of v_m.

Now consider each monomial in F, and let G be the part of monomial over entries of v_m, then it suffices to show that $\mathbf{E}[G(v_m)]$ is a degree-d semi-polynomial in $v_1, \ldots, v_{m-1}$. Lemma 3.3 already showed this for $\mathbf{E}[G(g)]$, and since G is a monomial of degree $\ell \le d$, we have

$$\mathbf{E}[G(g)] = \mathbf{E}[G(r \cdot v_m)] = \mathbf{E}[r^\ell]\, \mathbf{E}[G(v_m)], \tag{17}$$

where $\mathbf{E}[r^\ell]$ is a non-zero constant irrelevant to the choice of $v_1, \ldots, v_{m-1}$. Therefore $\mathbf{E}[G(v_m)]$ is also a degree-d semi-polynomial in $v_1, \ldots, v_m$. □

Since P is an expectation over F, it is also always non-negative and has the same expectation as $\mathbf{E}[F]$. Thus the induction hypothesis gives

$$\Pr[P(v_1, \ldots, v_{m-1}) \le \varepsilon\, \mathbf{E}[F]] \le C'(n, m-1, d) \cdot \varepsilon^{C(n,m-1,d)}. \tag{18}$$

Now we fix some $v_1, \ldots, v_{m-1}$ and consider the degree-d semi-polynomial

$$F_{v_1,\ldots,v_{m-1}}(v_m) = F(v_1, \ldots, v_{m-1}, v_m),$$

which is always non-negative. Since there exists a linear map $A : \mathbb{C}^{n-m+1} \to \mathbb{C}^n$ such that $v_m = Au$, where u is a Haar-random unit vector in $\mathbb{C}^{n-m+1}$, we can apply (15) from the previous stage for $m = 1$ on $F_{v_1,\ldots,v_{m-1}}(Au)$ to get

$$\Pr\Big[F_{v_1,\ldots,v_{m-1}}(Au) \le \varepsilon\, \mathbf{E}_u\Big[F_{v_1,\ldots,v_{m-1}}(Au)\Big]\Big] \le C'(n, 1, d) \cdot \varepsilon^{C(n,1,d)}. \tag{19}$$

Therefore we conclude that, for every $p \in (0, 1)$,

$$\begin{aligned}
&\Pr[F(v_1, \ldots, v_m) \le \varepsilon\, \mathbf{E}[F]] \\
\le\ &\Pr[P(v_1, \ldots, v_{m-1}) \le \varepsilon^p\, \mathbf{E}[F]] + \Pr\big[F(v_1, \ldots, v_m) \le \varepsilon^{1-p} P(v_1, \ldots, v_{m-1})\big] \\
=\ &\Pr[P(v_1, \ldots, v_{m-1}) \le \varepsilon^p\, \mathbf{E}[F]] + \Pr\Big[F_{v_1,\ldots,v_{m-1}}(v_m) \le \varepsilon^{1-p}\, \mathbf{E}[F_{v_1,\ldots,v_{m-1}}]\Big] \\
\le\ &C'(n, m-1, d) \cdot \varepsilon^{pC(n,m-1,d)} + C'(n, 1, d) \cdot \varepsilon^{(1-p)C(n,1,d)},
\end{aligned} \tag{20}$$

Similar to the previous stage, we can take

$$C(n, m, d) = \frac{1}{C(n, m-1, d)^{-1} + C(n, 1, d)^{-1}} = \frac{1}{4nmd},$$

and $C'(n, m, d) = C'(n, m-1, d) + C'(n, 1, d) = O(n^2 md)$. This completes the proof of Theorem 3.1.

4 Mixing Bound for Random Circuits

In this section we prove Theorem 1.1. Since the output qubit $\Phi_{\mathcal{C}}(\rho)$ is in the lightcone of the input qubit ρ, there exists gates $G_1, \ldots, G_D$ in the circuit $\mathcal{C}$ that connect the input and output qubits. That is, there are qubits $\rho_0, \rho_1, \ldots, \rho_D$ with $\rho_0 = \rho$ and $\rho_D = \Phi_{\mathcal{C}}(\rho)$, such that the gate G_i has ρ_{i-1} as an input and ρ_i as an output. Each gate G_i is independently drawn from the Haar measure $\mathcal{U}(2^k)$.

Note that even when gate G_i is given, we cannot directly claim any relationship between ρ_{i-1} and ρ_i, as the other input qubits to G_i are correlated and possibly entangled with ρ_{i-1}. To handle this, we let τ_{i-1} be the composite state of the k input qubits to G_i, and by Lemma 2.5 we have

$$\left\|\tau_{i-1} - \tau'_{i-1}\right\|_{\mathrm{F}} \geq 2^{-k/2}\left\|\rho_{i-1} - \rho'_{i-1}\right\|_{\mathrm{F}}, \tag{21}$$

where ρ'_i and τ'_i are the corresponding states when the input state is $\rho'_0 = \rho'$. Therefore we only need to bridge the remaining gaps by proving

$$\left\|\rho_i - \rho'_i\right\|_{\mathrm{F}} \geq \lambda_i\left\|\tau_{i-1} - \tau'_{i-1}\right\|_{\mathrm{F}} \tag{22}$$

where λ_i is some function of G_i, and then bound the distribution of λ_i by applying the anti-concentration bound from Theorem 1.6.

At a first glance, this looks impossible as τ_{i-1} is a k-qubit state while ρ_i is single-qubit, which means that as long as $k > 1$, whatever G_i is, there will be input states $\tau_{i-1} \neq \tau'_{i-1}$ to G_i with the output qubits $\rho_i = \rho'_i$. The key observation is that the states τ_i cannot be arbitrary k-qubit states: Since all the input qubits to the circuit $\mathcal{C}$ are fixed except ρ, when the circuit $\mathcal{C}$ is given, each τ_i is the result of ρ through a fixed quantum channel. As the difference $\rho - \rho'$ ranges within the 3-dimensional Euclidean space Δ_1, the difference $\tau_{i-1} - \tau'_{i-1}$ could also only range within a 3-dimensional subspace of Δ_k.

This allows us to define and bound the distribution of λ_i that uniformly holds for every such subspace as follows:

Lemma 4.1. *For every $k \in \mathbb{N}$, there exists a distribution Λ_k over $[0, \infty)$ that satisfies:*

- *There exists $t > 0$ such that $\mathbf{E}[\Lambda_k^{-t}] < \infty$.*
- *For every fixing of the input qubits other than ρ, and layers $1, \ldots, i-1$ of the circuit $\mathcal{C}$, there exists a function $\lambda_i \colon \mathbb{U}(2^k) \to [0, \infty)$ at layer i such that*

$$\left\|\rho_i - \rho'_i\right\|_{\mathrm{F}} \geq \lambda_i(G_i)\left\|\tau_{i-1} - \tau'_{i-1}\right\|_{\mathrm{F}}$$

holds for all input states ρ and ρ', and $\lambda_i(G_i) \sim \Lambda_k$ when $G_i \sim \mathcal{U}(2^k)$.

We will prove Lemma 4.1 in Section 4.1. For now let us show how Lemma 4.1 would imply Theorem 1.1.

Proof of Theorem 1.1. From Lemma 4.1 and (21) we get

$$\left\|\rho_i - \rho_i'\right\|_{\mathrm{F}} \geq \lambda_i(G_i)\left\|\tau_{i-1} - \tau_{i-1}'\right\|_{\mathrm{F}} \geq 2^{-k/2}\lambda_i(G_i)\left\|\rho_{i-1} - \rho_{i-1}'\right\|_{\mathrm{F}} \tag{23}$$

for every $i = 1, \ldots, D$. Here each function $\lambda_i(G_i)$ depends on the previous layers, but as random variables $\lambda_i = \lambda_i(G_i)$ they are independent, since λ_i follows the same distribution Λ_k no matter how $\lambda_1, \ldots, \lambda_{i-1}$ are fixed.

Since $\left\|\rho_0 - \rho_0'\right\|_{\mathrm{F}} = \left\|\rho - \rho'\right\|_{\mathrm{F}}$ and $\left\|\rho_D - \rho_D'\right\|_{\mathrm{F}} = \left\|\Phi_{\mathcal{C}}(\rho) - \Phi_{\mathcal{C}}(\rho')\right\|_{\mathrm{F}}$, we have

$$\left\|\Phi_{\mathcal{C}}(\rho) - \Phi_{\mathcal{C}}(\rho')\right\|_{\mathrm{F}} \geq 2^{-kD/2}\lambda_1 \cdots \lambda_D\left\|\rho - \rho'\right\|_{\mathrm{F}}. \tag{24}$$

To bound the product of λ_i we use Markov's inequality, which states that for every $\alpha > 0$,

$$\begin{aligned}\Pr[\lambda_1 \cdots \lambda_D \leq \alpha] &= \Pr[(\lambda_1 \cdots \lambda_D)^{-t} \geq \alpha^{-t}] \\ &\leq \alpha^t \,\mathbf{E}[\lambda_1^{-t} \cdots \lambda_D^{-t}] = \alpha^t \,\mathbf{E}[\Lambda_k^{-t}]^D\end{aligned} \tag{25}$$

where we take $t > 0$ to be the constant in Lemma 4.1. Take α such that $\gamma = \alpha^t \,\mathbf{E}[\Lambda_k^{-t}]^D$, we conclude that with probability at least $1 - \gamma$,

$$\begin{aligned}\left\|\Phi_{\mathcal{C}}(\rho) - \Phi_{\mathcal{C}}(\rho')\right\|_{\mathrm{F}} &\geq 2^{-kD/2}\alpha\left\|\rho - \rho'\right\|_{\mathrm{F}} \\ &= 2^{-kD/2}\gamma^{1/t}\,\mathbf{E}[\Lambda_k^{-t}]^{D/t}\left\|\rho - \rho'\right\|_{\mathrm{F}} \\ &= (2^{-D}\gamma)^{O_k(1)}\left\|\rho - \rho'\right\|_{\mathrm{F}}.\end{aligned}$$

□

4.1 Proof of Lemma 4.1

The basic idea of the proof is to lower bound the ratio $\left\|\rho_i - \rho_i'\right\|_{\mathrm{F}} / \left\|\tau_{i-1} - \tau_{i-1}'\right\|_{\mathrm{F}}$ with a polynomial function on the entries of G_i and apply Theorem 1.6.

The quantum channel defined by G_i that maps τ_{i-1} to ρ_i induces the linear map

$$M_i : \tau_{i-1} - \tau_{i-1}' \mapsto \rho_i - \rho_i'.$$

The domain of M_i is a 3-dimensional subspace of Δ_k which we denote as $\mathcal{S}_i$, while the range of M_i is Δ_1. Notice that the map M_i is completely determined by the domain $\mathcal{S}_i$ and the gate G_i, while $\mathcal{S}_i$ depends only on the fixed inputs to the circuit $\mathcal{C}$ and the gates of $\mathcal{C}$ in layers $1, \ldots, i-1$.

Since both the domain and the range are Euclidean spaces, the absolute determinant $|\det M_i|$ is independent of the choices of bases when writing M_i as matrix in $\mathbb{R}^{3\times 3}$. We will show that $|\det M_i|$ is basically the lower bound that we seek for, via the following propositions.

Proposition 4.2. *It always holds that*

$$\left\|\rho_i - \rho_i'\right\|_{\mathrm{F}} \geq 2^{-k}|\det M_i| \cdot \left\|\tau_{i-1} - \tau_{i-1}'\right\|_{\mathrm{F}}.$$

Proof. Let $\sigma_1 \le \sigma_2 \le \sigma_3$ be the singular values of M_i, then $\left\|\rho_i - \rho_i'\right\|_{\mathrm{F}} \ge \sigma_1 \left\|\tau_{i-1} - \tau_{i-1}'\right\|_{\mathrm{F}}$ as the norms in both spaces coincide with the Frobenius norm. On the other hand, we know that $\sigma_2 \le \sigma_3 \le 2^{k/2}$ by Lemma 2.5. Therefore, $|\det M_i| = \sigma_1\sigma_2\sigma_3 \le 2^k\sigma_1$ and thus the claim holds. □

Proposition 4.3. *For each fixed domain $\mathcal{S}_i$, $\det M_i$ is a degree-6 semi-polynomial in the entries of G_i.*

Proof. After fixing the orthonormal bases $\{\xi_1, \xi_2, \xi_3\}$ for $\mathcal{S}_i$ and $\{\sigma_1, \sigma_2, \sigma_3\}$ for Δ_1, the (ℓ, r)-th entry in the matrix representation of M_i is

$$\mathrm{Tr}[\sigma_r \cdot M_i(\xi_\ell)] = \mathrm{Tr}[(I_A \otimes \sigma_r) \cdot G_i \xi_\ell G_i^\dagger] \tag{26}$$

where A is the system that consists of the output qubits of G_i other than ρ_i. This is a quadratic form in the entries of G_i and thus a degree-2 semi-polynomial, and therefore $\det M_i$ is a degree-6 semi-polynomial. □

Proposition 4.4. *There exists a constant $\mu_k > 0$ such that for every possible domain $\mathcal{S}_i$,*

$$\mathop{\mathbf{E}}_{G_i \sim \mathcal{U}(2^k)} \left[|\det M_i|^2\right] \ge \mu_k.$$

Proof. When $\mathcal{S}_i$ is fixed, $|\det M_i|^2$ is a continuous function of $G_i \in \mathbb{U}(2^k)$. For at least one G_i, which is a permutation over the k qubits that swaps ρ_{i-1} to ρ_i, we have $|\det M_i| > 0$. This implies that $\mathbf{E}\left[|\det M_i|^2\right] > 0$ always holds.

Now we think of $\mathbf{E}\left[|\det M_i|^2\right]$ as a continuous function of $\mathcal{S}_i$, while the set of all possible $\mathcal{S}_i$ is a closed subset of the Grassmannian $\mathbf{Gr}_3(\mathbb{R}^{4^k-1})$ and thus is compact. That means the function admits a global minimum μ_k, which depends only on k, and $\mu_k > 0$. □

Now we are ready to prove Lemma 4.1.

Proof of Lemma 4.1. Applying Theorem 1.6 with Propositions 4.3 and 4.4 gives

$$\begin{aligned}\Pr\left[2^{-k}|\det M_i| \le \varepsilon\right] &\le \Pr\left[|\det M_i|^2 \le 2^{2k}\mu_k^{-1}\varepsilon^2 \,\mathbf{E}\left[|\det M_i|^2\right]\right] \\ &\le C'(2^k, 6) \cdot (2^{2k}\mu_k^{-1}\varepsilon^2)^{C(2^k,6)}\end{aligned} \tag{27}$$

which holds for every domain $\mathcal{S}_i$ and every $\varepsilon \ge 0$. We define Λ_k as the distribution over $[0, \infty)$ with the following cumulative function:

$$\Pr[\Lambda_k \le x] = \min\left\{C'(2^k, 6) \cdot (2^{2k}\mu_k^{-1}x^2)^{C(2^k,6)}, 1\right\}.$$

Take $t = C(2^k, 6) > 0$ and let $C = C'(2^k, 6) \cdot (2^{2k}\mu_k^{-1})^{C(2^k,6)} > 0$, then we have

$$\begin{aligned}\mathbf{E}[\Lambda_k^{-t}] &= \int_0^{\infty} x^{-t} \mathrm{d}\Pr[\Lambda_k \le x] \\ &= \int_0^{C^{-1/(2t)}} x^{-t} \mathrm{d}(Cx^{2t}) \\ &= \int_0^{C^{-1/(2t)}} 2tC \cdot x^{t-1} \mathrm{d}x = 2tC^{1/2} < \infty. \end{aligned} \tag{28}$$

Now suppose the input qubits other than ρ are fixed, and the layers $1, \ldots, i-1$ of the circuit $\mathcal{C}$ is given. This fixes the domain $\mathcal{S}_i$ for M_i, and provides the cumulative function

$$P(x) = \Pr\Big[2^{-k}|\det M_i| \le x\Big].$$

We then define the function $\lambda_i : \mathbb{U}(2^k) \to [0, \infty)$ as follows: For each $G_i \in \mathbb{U}(2^k)$, let $\lambda_i(G_i)$ be the smallest $\lambda \ge 0$ such that

$$P\big(2^{-k}|\det M_i|\big) = \Pr[\Lambda_k \le \lambda].$$

When $G_i \sim \mathcal{U}(2^k)$, we have $\lambda_i(G_i) \sim \Lambda_k$ since

$$\Pr[\lambda_i(G_i) \le x] = \Pr\Big[P\big(2^{-k}|\det M_i|\big) \le \Pr[\Lambda_k \le x]\Big] = \Pr[\Lambda_k \le x]. \tag{29}$$

We also have $2^{-k}|\det M_i| \ge \lambda_i(G_i)$ since $P(x) \le \Pr[\Lambda_k \le x]$ holds for all $x \ge 0$. Combined with Proposition 4.2 we get

$$\big\|\rho_i - \rho_i'\big\|_{\mathrm{F}} \ge 2^{-k}|\det M_i| \cdot \big\|\tau_{i-1} - \tau_{i-1}'\big\|_{\mathrm{F}} \ge \lambda_i(G_i)\big\|\tau_{i-1} - \tau_{i-1}'\big\|_{\mathrm{F}}. \qquad \square$$

5 Applications

5.1 Depth Lower Bound for Approximate Designs

In this section we prove Theorem 1.2. We first recall the definition of an approximate unitary design.

Definition 5.1. *For a distribution $\mathcal{D}$ over $\mathbb{U}(n)$ and $t \in \mathbb{N}_+$, define the moment superoperator as the following channel:*

$$\Phi_{\mathcal{D}}^{(t)} : \rho \mapsto \int_{\mathbb{U}(n)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} \mathrm{d}\mathcal{D}(U).$$

The distribution $\mathcal{D}$ is an ε-approximate unitary t-design if

$$\Big\|\Phi_{\mathcal{D}}^{(t)} - \Phi_{\mathcal{U}(n)}^{(t)}\Big\|_{\diamond} \le \varepsilon.$$

Note that there are several other definitions of the approximate design (see e.g. [BHH16]), and we choose the weaker one so that our Theorem 1.2 is still compatible with the stronger definitions of designs.

Proof of Theorem 1.2. Without loss of generality, let us assume that the first input qubit ρ and the first output qubit π are depth D apart. We fix all other input qubits to be maximally mixed, so that when ρ is also maximally mixed, the entire output is maximally mixed regardless of the circuit $\mathbb{C}$, and thus $\pi = I/2$. On the other hand, when $\rho = |0\rangle\langle 0|$, we know the following about the output qubit π via Theorem 1.1 that with probability $1 - 2^{-D}$ over the circuit $\mathcal{C}$,

$$\|\pi - I/2\|_{\mathrm{F}} \geq \||0\rangle\langle 0| - I/2\|_{\mathrm{F}} \cdot (2^{-2D})^{c_k} = \frac{1}{\sqrt{2}} \cdot 2^{-2Dc_k}. \tag{30}$$

We can expand the left hand side of (30) as

$$\|\pi - I/2\|_{\mathrm{F}}^2 = \mathrm{Tr}[(\pi - I/2)^2] = \mathrm{Tr}[\pi^2] - 1/2. \tag{31}$$

Since $\mathrm{Tr}[\pi^2] \leq 1$ always holds, we get

$$\mathbf{E}_{\mathcal{C}}[\mathrm{Tr}[\pi^2]] \geq \frac{1}{2} + \frac{1}{2} \cdot 2^{-4Dc_k} + \frac{1}{2} \cdot 2^{-D}. \tag{32}$$

Now imagine feeding two copies of the input state $|0\rangle\langle 0| \otimes (I/2)^{\otimes(n-1)}$ to the superoperators $\Phi_{\mathcal{C}}^{(2)}$ and $\Phi_{\mathcal{U}(n)}^{(2)}$, and apply a swap test on the first output qubits in the two copies. The output probability is determined by $\mathrm{Tr}[\pi^2]$. We know already from [EAZ05] that when going through an n-qubit Haar random unitary, we have $\mathbf{E}_{\mathcal{U}(n)}[\mathrm{Tr}[\pi^2]] = 1/2$. Therefore, we conclude that the difference $2^{-4Dc_k} + 2^{-D} \leq O(\varepsilon)$ which means that $D \geq \Omega_k(\log \varepsilon^{-1})$. □

5.2 Depth Test

In this section we prove Theorem 1.3, where we learn the exact depth of a brickwork random circuit $\mathcal{C}$.

1 Arbitrarily fix all input qubits except the first one ρ.
2 **for** $D = 0, 1, \ldots$ **do**
3 Let $\varepsilon = (2^{-2D}\gamma)^{c_2}/4$;
4 Apply $\mathcal{C}$ with $\rho = |0\rangle\langle 0|$ and let π be the $(D+2)$-th output qubit;
5 Apply $\mathcal{C}$ with $\rho = |1\rangle\langle 1|$ and let π' be the $(D+2)$-th output qubit;
6 Estimate π and π' up to ε error by state tomography;
7 **if** $\left\|\pi - \pi'\right\|_{\mathrm{F}} \leq 2\varepsilon$ **then return** D.

Algorithm 1: Algorithm for depth testing.

The processed is described in Algorithm 1. Here c_2 is the constant c_k in Theorem 1.1 with $k = 2$ for brickwork circuits, and $\gamma > 0$ is the target error probability. Notice that in a brickwork circuit of depth D, the $(D+2)$-th output qubit lies outside the lightcone of the first input qubit. Therefore, when the algorithm iterates to the correct depth D, we have $\pi = \pi'$ and D must be returned even when both π and π' are estimated with ε error.

On the other hand, when D is smaller than the actual depth, the $(D+2)$-th output qubit lies inside the lightcone of the first input qubit. By Theorem 1.1, with probability $1 - 2^{-D}\gamma$ over $\mathcal{C}$ we have

$$\left\|\pi - \pi'\right\|_{\mathrm{F}} \geq \left\||0\rangle\langle 0| - |1\rangle\langle 1|\right\|_{\mathrm{F}} \cdot (2^{-2D}\gamma)^{c_2} > 4\varepsilon. \tag{33}$$

This means when both π and π' are estimated with ε error, we still have $\left\|\pi - \pi'\right\|_{\mathrm{F}} > 2\varepsilon$. By a union bound over D, with probability $1 - \gamma$ all those D smaller than the actual depth will be skipped, and thus the outputted depth is correct.

Note that the efficiency of the algorithm depends on the single-qubit tomography process, which by Proposition 2.3 is $\mathrm{poly}(1/\varepsilon)$. As a conclusion, we obtain the following more general statement which implies Theorem 1.3:

Theorem 5.2. *Let $\mathcal{C}$ be a brickwork random quantum circuit of an unknown depth D , where each gate is independently Haar random.. Given oracle access to $\mathcal{C}$, for any $\gamma \in (0, 1)$, Algorithm 1 outputs D with probability at least $1 - \gamma$ in time $\mathrm{poly}(2^D, \gamma^{-1})$.*

Remark. The only property of the brickwork architecture we used here is that the set of qubits within the lightcone of an input qubit is strictly expanding when the depth grows, which allows us to distinguish between different depths. Therefore the algorithm can be easily modified, with the same efficiency, to work with higher dimensional brickwork circuits and other architectures.

5.3 Learning Brickwork Random Circuits

5.3.1 Learning the First Gate

Here we prove Theorem 1.4, where we learn the gate $G_{1,1}$, namely the gate in the first layer acting on the first and second qubit, in a brickwork circuit of depth $D = O(\log n)$ with Haar random gates. The same arguments also work for other gates in the first layer.

To learn $G_{1,1}$, we try to uncompute $G_{1,1}$ by first apply some two-qubit unitary $G^\dagger \in \mathbb{U}(4)$ and then apply the circuit $\mathbb{C}$. We distinguish whether G is close to $G_{1,1}$ or not using the similar idea as in Section 5.2. Specifically, if $G = G_{1,1}$ so that $G^\dagger$ perfectly uncomputes the gate $G_{1,1}$, then the $(D+1)$-th output qubit will lie outside the lightcone of the first input qubit. Note that this is also true when $G^\dagger$ cancels $G_{1,1}$ into unentangled single-qubit gates, that is when there exists $U_1, U_2 \in \mathbb{U}(2)$ that $G_{1,1}G^\dagger = U_1 \otimes U_2$. In contrast, when $G^\dagger$ does not cancel $G_{1,1}$ into unentangled single-qubit gates, the first two qubits will be entangled after the first layer of gates, and thus the $(D+1)$-th output qubit will be affected when the first input qubit changes.

To put the above intuition more formally, we first define the distance between two-qubit gates when taking the quotient over unentangled single-qubit gates:

Definition 5.3. *For $G, G' \in \mathbb{U}(4)$, we define the distance*

$$d_{\otimes}(G, G') = \min_{U_1, U_2 \in \mathbb{U}(2)} d_{\diamond}(G, (U_1 \otimes U_2) \cdot G').$$

We note that $d_{\otimes}$, like the diamond distance $d_{\diamond}$, is a pseudometric on $\mathbb{U}(4)$. That is, a metric except that two distinct unitaries could have distance zero. However, $d_{\otimes}(G, G') = 0$ if and only if $G' \cdot G^{-1} = U_1 \otimes U_2$ for some $U_1, U_2 \in \mathbb{U}(2)$.

The learning algorithm is described in Algorithm 2, with $\delta, \gamma > 0$ being the target error rate. Notice that within each loop of σ_2, the second input qubit ρ_2 is fixed, while the first one changes with a difference σ_1 that goes through the Pauli basis. The input qubits ρ_1 and ρ_2 are Pauli eigenstates except when $\sigma_2 = \rho_2 = I/2$, which can be obtained by randomly choosing $|0\rangle$ or $|1\rangle$.

To prove the correctness of the algorithm, we need the following lemmas that connects the distance $d_{\otimes}(U, I \otimes I)$ with the behavior of U over the Pauli basis.

Arbitrarily fix all input qubits except the first and second ones ρ_1, ρ_2.
Let $\varepsilon = 10^{-4}\delta^2(2^{-D}\gamma)^{c_2}$;
foreach G from an ε-net of $\mathbb{U}(4)$ under distance $d_{\otimes}$ **do**
    for $\sigma_1 \in \{X, Y, Z\}$ and $\sigma_2 \in \{I, X, Y, Z\}$ **do**
        Let $\rho_1 = (I + \sigma_1)/2, \rho_2 = (I + \sigma_2)/2$ and apply $G^\dagger$ on the first two qubits,
            then apply $\mathcal{C}$ and let π be the $(D+1)$-th output qubit;
        Let $\rho_1 = (I - \sigma_1)/2, \rho_2 = (I + \sigma_2)/2$ and apply $G^\dagger$ on the first two qubits,
            then apply $\mathcal{C}$ and let π' be the $(D+1)$-th output qubit;
        Estimate π and π' up to ε error by state tomography;
        if $\left\|\pi - \pi'\right\|_{\mathrm{F}} \geq 5\varepsilon$ **then** reject G.
    return G if not rejected.

Algorithm 2: Algorithm for learning the gate $G_{1,1}$

Lemma 5.4. *For $U \in \mathbb{U}(4)$, if $d_{\otimes}(U, I \otimes I) \leq \delta$ then for every $\sigma_1 \in \{X, Y, Z\}$ and $\sigma_2 \in \{I, X, Y, Z\}$,*

$$\left\|\mathrm{Tr}_A\left[U(\sigma_1 \otimes \sigma_2)U^\dagger\right]\right\|_{\mathrm{F}} \leq 2\delta,$$

where Tr_A is the partial trace that traces out the first qubit.

Proof. By definition, $d_{\otimes}(U, I \otimes I) \leq \delta$ means that there exists $U_1, U_2 \in \mathbb{U}(2)$ that $d_{\diamond}(U, U_1 \otimes U_2) \leq \delta$. Therefore,

$$\begin{aligned}
\left\|\mathrm{Tr}_A\left[U(\sigma_1 \otimes \sigma_2)U^\dagger\right]\right\|_{\mathrm{F}} &\leq \left\|\mathrm{Tr}_A\left[U(\sigma_1 \otimes \sigma_2)U^\dagger\right]\right\|_1 \\
&= \left\|\mathrm{Tr}_A\left[U(\sigma_1 \otimes \sigma_2)U^\dagger\right] - \mathrm{Tr}_A\left[U_1\sigma_1U_1^\dagger \otimes U_2\sigma_2U_2^\dagger\right]\right\|_1 \\
&\leq \left\|U(\sigma_1 \otimes \sigma_2)U^\dagger - (U_1 \otimes U_2)(\sigma_1 \otimes \sigma_2)(U_1 \otimes U_2)^\dagger\right\|_1 \\
&\leq 2\delta.
\end{aligned}$$

□

Lemma 5.5. *For $U \in \mathbb{U}(4)$, if for every $\sigma_1 \in \{X, Y, Z\}$ and $\sigma_2 \in \{I, X, Y, Z\}$ we have*

$$\left\| \mathrm{Tr}_A \left[U(\sigma_1 \otimes \sigma_2) U^\dagger \right] \right\|_{\mathrm{F}} \leq \delta,$$

then $d_\otimes(U, I \otimes I) \leq 20\sqrt{\delta}$.

The proof of Lemma 5.5 is rather technical and thus is deferred to the end of this section. For now, let us show how Lemmas 5.4 and 5.5 would imply the completeness and the soundness of Algorithm 2.

We apply Theorem 1.1 to the circuit $\mathcal{C}$ minus its first layer, which is a circuit of depth $D-1$. Notice that among the input qubits to the second layer of $\mathcal{C}$, the third to n-th qubits only depends on the gates $G_{1,3}, \ldots, G_{1,n}$ and thus can be viewed as fixed. The first qubit does not affect the $(D+1)$-th output qubit and thus its entire lightcone can be removed from the picture. That leaves us the second qubit, which is

$$\mathrm{Tr}_A \left[G_{1,1} G^\dagger (\rho_1 \otimes \rho_2) G G_{1,1}^\dagger \right].$$

Therefore, with ρ_1 changed with a difference σ_1 and $\rho_2 = (I + \sigma_2)/2$ unchanged, Theorem 1.1 implies that with probability $1 - \gamma$, the following holds for every G.

$$\left\| \pi - \pi' \right\|_{\mathrm{F}} \geq \left\| \mathrm{Tr}_A \left[G_{1,1} G^\dagger (\sigma_1 \otimes \rho_2) G G_{1,1}^\dagger \right] \right\|_{\mathrm{F}} \cdot (2^{-D}\gamma)^{c_2}. \tag{34}$$

Meanwhile, Lemma 2.5 implies that

$$\left\| \pi - \pi' \right\|_{\mathrm{F}} \leq \left\| \mathrm{Tr}_A \left[G_{1,1} G^\dagger (\sigma_1 \otimes \rho_2) G G_{1,1}^\dagger \right] \right\|_{\mathrm{F}} \cdot \sqrt{2}. \tag{35}$$

For completeness, since we take G from an ε-net, the algorithm must have tested some G with $d_\otimes(G_{1,1}, G) = d_\otimes(G_{1,1} G^\dagger, I \otimes I) \leq \varepsilon \leq \delta$. Hence by Lemma 5.4 and (35), for such G it always holds that $\left\| \pi - \pi' \right\|_{\mathrm{F}} \leq 2\sqrt{2}\varepsilon$, and thus G will not be rejected even with ε tomography errors in π and π'.

For soundness, assume that $d_\otimes(G_{1,1}, G) > \delta$, then by Lemma 5.5 we know that for some $\sigma_1 \in \{X, Y, Z\}$ and $\sigma_2 \in \{I, X, Y, Z\}$,

$$\left\| \mathrm{Tr}_A \left[G_{1,1} G^\dagger (\sigma_1 \otimes \sigma_2) G G_{1,1}^\dagger \right] \right\|_{\mathrm{F}} > \frac{1}{400} \delta^2. \tag{36}$$

As $\sigma_2 = 2\rho_2 - I$, that means there exists some ρ_2 such that

$$\left\| \mathrm{Tr}_A \left[G_{1,1} G^\dagger (\sigma_1 \otimes \rho_2) G G_{1,1}^\dagger \right] \right\|_{\mathrm{F}} > \frac{1}{1200} \delta^2. \tag{37}$$

Thus by (34) we have $\left\| \pi - \pi' \right\|_{\mathrm{F}} > \delta^2 (2^{-D}\gamma)^{c_2} / 1200 > 7\varepsilon$, and G will be rejected when π and π' are estimated with ε error.

The efficiency of the algorithm depends on the size of the ε-net and the state tomography process, which are both $\mathrm{poly}(1/\varepsilon) = \mathrm{poly}(1/\delta, 1/\gamma)$. Notice that the algorithm similarly works for every gate in the first layer, and as a result, we obtained the following formal statement of Theorem 1.4:

Theorem 5.6. *Let $\mathcal{C}$ be a brickwork random quantum circuit of depth D, where each gate is independently Haar random. Let $G_{1,1}$ be the gate in the first layer of $\mathcal{C}$ that acts on the first and second qubit. Given oracle access to $\mathcal{C}$, for any $\delta, \gamma \in (0,1)$, with probability at least $1-\gamma$ over $\mathcal{C}$, Algorithm 2 outputs some $G \in \mathbb{U}(4)$ such that $d_{\otimes}(G, G_{1,1}) \leq \delta$ in time* $\mathrm{poly}(2^D, 1/\delta, 1/\gamma)$.

The rest of this section is devoted to prove Lemma 5.5.

Proof of Lemma 5.5. In the proof we assume that $\delta \leq 1/2$, as otherwise the claim is trivial.

For any Hermitian operator $\sigma \in \mathbb{C}^{4\times 4}$ with trace zero, the value $\|\mathrm{Tr}_A[\sigma]\|_{\mathrm{F}}/\sqrt{2}$ is exactly the length of the projection of σ on to the subspace $I \otimes \mathrm{span}\{X,Y,Z\}$. Therefore, the assumptions would imply that for every $\sigma \in \mathrm{span}\{X,Y,Z\} \otimes \{I,X,Y,Z\}$ and $\sigma' \in I \otimes \mathrm{span}\{X,Y,Z\}$, we have

$$\mathrm{Tr}[U\sigma U^\dagger \sigma'] \leq \frac{\delta}{\sqrt{2}} \cdot \|\sigma\|_{\mathrm{F}} \|\sigma'\|_{\mathrm{F}}. \tag{38}$$

Now consider any single-qubit state ρ, and let σ be the projection of $U^\dagger(I\otimes\rho)U$ onto the subspace $\mathrm{span}\{X,Y,Z\} \otimes \{I,X,Y,Z\}$. Inequality (38) gives

$$\begin{aligned}
\mathrm{Tr}[U^\dagger(I\otimes\rho)U\sigma] &= \mathrm{Tr}[U\sigma U^\dagger(I\otimes\rho)] \\
&= \mathrm{Tr}[U\sigma U^\dagger(I\otimes(\rho - I/2))] \\
&\leq \frac{\delta}{\sqrt{2}} \cdot \|\sigma\|_{\mathrm{F}} \cdot \sqrt{2}\|\rho - I/2\|_{\mathrm{F}} \ \leq \delta.
\end{aligned}$$

That means the projection of $U^\dagger(I\otimes\rho)U$ onto the orthogonal subspace $I \otimes \mathrm{span}\{I,X,Y,Z\}$ must be large. Since this projection is exactly $\frac{1}{2}I \otimes \mathrm{Tr}_A[U^\dagger(I\otimes\rho)U]$, we have

$$\frac{1}{2}\left\|\mathrm{Tr}_A\left[U^\dagger(I\otimes\rho)U\right]\right\|_{\mathrm{F}}^2 \geq \left\|U^\dagger(I\otimes\rho)U\right\|_{\mathrm{F}}^2 - \delta = 2\|\rho\|_{\mathrm{F}}^2 - \delta. \tag{39}$$

If we define the following channel

$$\Phi(\rho) = \frac{1}{2}\mathrm{Tr}_A\left[U^\dagger(I\otimes\rho)U\right]$$

then inequality (39) translates to

$$\|\Phi(\rho)\|_{\mathrm{F}}^2 \geq \|\rho\|_{\mathrm{F}}^2 - \delta/2. \tag{40}$$

That means Φ is almost norm preserving and thus almost a unitary channel. In fact, as $\Phi(I) = I$ by definition, Φ is a unital channel and has a canonical form [CL23] $\Phi'(\rho) = W\Phi(V\rho V^\dagger)W^\dagger$ for some $V, W \in \mathbb{U}(2)$ such that

$$\Phi'(X) = d_x X, \quad \Phi'(Y) = d_y Y, \quad \Phi'(Z) = d_z Z, \quad d_x, d_y, d_z \in [-1,1].$$

By taking $\rho = (I+X)/2$ we get $d_x^2 \geq 1-\delta$, and the same also holds for d_y and d_z. The canonical form has an additional property that (d_x, d_y, d_z) is a convex combination of

vectors $(1,1,1),(1,-1,-1),(-1,1,-1),(-1,-1,1)$, and as $\delta \leq 1/2$, Φ' must be close to a Pauli rotation in $\{I,X,Y,Z\}$. That means there exists $U_2 \in \{VW, VXW, VYW, VZW\}$ such that for every single-qubit state ρ,

$$\left\|\Phi(\rho) - U_2^\dagger \rho U_2\right\|_{\mathrm{F}}^2 \leq \frac{1}{2}\left(1-\sqrt{1-\delta}\right)^2 \leq \frac{1}{2}\delta^2. \tag{41}$$

Therefore, for any two single-qubit states ρ and ρ' with $\mathrm{Tr}[\rho\rho'] = 0$ we have

$$\begin{aligned}
\mathrm{Tr}\left[U_2\Phi(\rho)U_2^\dagger\rho'\right] &= \mathrm{Tr}\left[\left(U_2\Phi(\rho)U_2^\dagger - \rho\right)\rho'\right] \\
&\leq \left\|U_2\Phi(\rho)U_2^\dagger - \rho\right\|_{\mathrm{F}} \left\|\rho'\right\|_{\mathrm{F}} \\
&= \left\|\Phi(\rho) - U_2^\dagger\rho U_2\right\|_{\mathrm{F}} \left\|\rho'\right\|_{\mathrm{F}} \leq \frac{1}{\sqrt{2}}\delta.
\end{aligned} \tag{42}$$

Now consider the unitary $U' = U(I \otimes U_2^\dagger) \in \mathbb{U}(4)$, and we denote the entries of U' as u_{ij} for $i,j = 1,\ldots,4$. Notice that

$$U_2\Phi(\rho)U_2^\dagger = \frac{1}{2}\mathrm{Tr}_A\left[(I\otimes U_2)U^\dagger(I\otimes\rho)U(I\otimes U_2^\dagger)\right] = \frac{1}{2}\mathrm{Tr}_A\left[U'^\dagger(I\otimes\rho)U'\right],$$

and this allows us to write out $\mathrm{Tr}\left[U_2\Phi(\rho)U_2^\dagger\rho'\right]$ exactly. In particular, when $\rho = |0\rangle\langle 0|$ and $\rho' = |1\rangle\langle 1|$, we get from (42) that

$$|u_{12}|^2 + |u_{14}|^2 + |u_{32}|^2 + |u_{34}|^2 \leq \sqrt{2}\delta. \tag{43}$$

When $\rho = |1\rangle\langle 1|$ and $\rho' = |0\rangle\langle 0|$, we get

$$|u_{21}|^2 + |u_{23}|^2 + |u_{41}|^2 + |u_{43}|^2 \leq \sqrt{2}\delta. \tag{44}$$

And when $\rho = |+\rangle\langle +|$ and $\rho' = |-\rangle\langle -|$, we get

$$\begin{aligned}
&|u_{11}+u_{21}-u_{12}-u_{22}|^2 + |u_{13}+u_{23}-u_{14}-u_{24}|^2 \\
&+ |u_{31}+u_{41}-u_{32}-u_{42}|^2 + |u_{33}+u_{43}-u_{34}-u_{44}|^2 \leq 4\sqrt{2}\delta.
\end{aligned} \tag{45}$$

Combine (43) to (45) together we also get

$$|u_{11}-u_{22}|^2 + |u_{13}-u_{24}|^2 + |u_{31}-u_{42}|^2 + |u_{33}-u_{44}|^2 \leq 16\sqrt{2}\delta. \tag{46}$$

Inequalities (43), (44) and (46) imply that there exists a matrix $M \in \mathbb{C}^{2\times 2}$ such that

$$\left\|U' - M\otimes I\right\|_{\mathrm{F}}^2 \leq 10\sqrt{2}\delta. \tag{47}$$

Let $M = V'\Sigma W'$ be the singular value decomposition of M, then we have

$$\begin{aligned}
\left\|U' - V'W'\otimes I\right\|_{\mathrm{F}} &\leq \left\|U' - M\otimes I\right\|_{\mathrm{F}} + \left\|V'W'\otimes I - M\otimes I\right\|_{\mathrm{F}} \\
&= \left\|U' - M\otimes I\right\|_{\mathrm{F}} + \min_{U''\in\mathbb{U}(4)}\left\|U'' - \Sigma\otimes I\right\|_{\mathrm{F}} \\
&\leq 2\left\|U' - M\otimes I\right\|_{\mathrm{F}} \leq 10\sqrt{\delta}.
\end{aligned} \tag{48}$$

Therefore, if we let $U_1 = V'W'$, then with the bound of diamond norm [Haa+23] we get

$$\begin{aligned} d_{\otimes}(U, I \otimes I) &\leq d_{\diamond}(U, U_1 \otimes U_2) \\ &\leq 2\|U - U_1 \otimes U_2\|_{\mathrm{F}} = 2\left\|U' - U_1 \otimes I\right\|_{\mathrm{F}} \leq 20\sqrt{\delta}. \end{aligned}$$

□

5.3.2 Learning the Circuit with Discretized Distribution

It is tempting to use Theorem 5.6 to learn the entire circuit $\mathcal{C}$. Indeed, if the statement is errorless that $d_{\otimes}(G, G_{1,1}) = 0$, we could view the single-qubit gates $G_{1,1}G^{\dagger} = U_1 \otimes U_2$ as part of the second layer. That means after learning the first layer, we can perfectly uncompute it and hence use Algorithm 2 to learn the second layer, and proceed until we are only left with single qubit gates, which are easily learnable.

However, when there are learning errors, which are inevitable for a continuous gate distribution like $\mathcal{U}(4)$, the above framework runs into a problem. Since we cannot perfectly uncompute the first layer, the inputs to the rest of the circuit are not clean enough: In particular, the error in $\sigma_1 \otimes \rho_2$ could have much larger influence on the output difference $\pi - \pi'$ than σ_1 itself. To control the influence of the errors, we need to reduce the learn error in the previous layer to be polynomially smaller than the target error in the current layer, and therefore a circuit of depth $D = \Theta(\log n)$ would require error as small as $2^{-\Omega(\log^2 n)}$ and incur quasi-polynomial running time.

Here we present a bypass to the problem which allows us to prove an errorless version of Theorem 5.6 and thus make the proposed framework work. The idea is to change the distribution from $\mathbb{U}(4)$ into a discrete one that approximates $\mathbb{U}(4)$. Intuitively, any ε-net where the elements are distributed according to $\mathcal{U}(4)$ would be a good approximation. We formalize this intuition as the following:

Definition 5.7. *An ε-net of a distribution $\mathcal{D}$ over a pseudometric space (S, d) is a distribution $\mathcal{D}_\varepsilon$ over S with a finite support, such that $\mathcal{D}_\varepsilon = f(\mathcal{D})$ for some (possibly randomized) map $f : S \to S$, with the following properties:*

- *For every $x \in S$, $d(x, f(x)) \leq \varepsilon$.*
- *For every $x_1, x_2 \in S$, either $d(f(x_1), f(x_2)) = 0$ or $d(f(x_1), f(x_2)) \geq \varepsilon$.*

Notice that under Definition 5.7, the set $\operatorname{supp} \mathcal{D}_\varepsilon$ is indeed an ε-net in the normal sense. Actually, the definition is general enough so that we can first choose any ε-net as the support, and then take f to be an arbitrary rounding scheme into the support. We show that $\mathcal{D}_\varepsilon$ approximates $\mathcal{D}$ via the following lemma.

Lemma 5.8. *If $F : S \to \mathbb{R}$ is L-Lipschitz, that is for all $x_1, x_2 \in S$,*

$$|F(x_1) - F(x_2)| \leq L \cdot d(x_1, x_2),$$

then for every $\delta \in \mathbb{R}$ we have

$$\Pr_{x \sim \mathcal{D}_\varepsilon}[F(x) \leq \delta] \leq \Pr_{x \sim \mathcal{D}}[F(x) \leq \delta + \varepsilon L].$$

Proof. Let $f : S \to S$ be the map in Definition 5.7, then

$$\begin{aligned}\Pr_{x\sim\mathcal{D}_\varepsilon}[F(x) \le \delta] &= \Pr_{x\sim\mathcal{D}}[F(f(x)) \le \delta] \\ &\le \Pr_{x\sim\mathcal{D}}[F(x) \le \delta + |F(x) - F(f(x))|] \\ &\le \Pr_{x\sim\mathcal{D}}[F(x) \le \delta + L \cdot d(x, f(x))] \\ &\le \Pr_{x\sim\mathcal{D}}[F(x) \le \delta + \varepsilon L].\end{aligned}$$

□

From now on, for each $\varepsilon > 0$ we fix some ε-net of the Haar measure $\mathcal{U}(4)$ under the $d_\otimes$ distance, and denote it by $\mathcal{U}_\varepsilon(4)$. We will show that when the gates in the brickwork circuit are drawn the net, we can actually use the framework at the start of this section to learn the circuit. To do so, we first prove an errorless version of Theorem 5.6 as follows.

Theorem 5.9. *Let $\mathcal{C}$ be a brickwork random quantum circuit of depth D, where each gate is independently drawn from $\mathcal{U}_\varepsilon(4)$. Let $G_{1,1}$ be the gate in the first layer of $\mathcal{C}$ that acts on the first and second qubit. Given oracle access to $\mathcal{C}$, for every $\gamma \in (0, 1)$ there is an algorithm that with probability at least $1 - \gamma$ over $\mathcal{C}$ outputs some $G \in \mathbb{U}(4)$ such that $d_\otimes(G, G_{1,1}) = 0$ in time $\mathrm{poly}(2^D, 1/\varepsilon, 1/\gamma)$.*

Proof. The algorithm is basically the same as Algorithm 2, except that we now iterate G through the support of $\mathcal{U}_\varepsilon(4)$. The proof is also mostly the same: When $G = G_{1,1}$, we have $\pi = \pi'$ and thus G will not be rejected; Otherwise $d_\otimes(G, G_{1,1}) \ge \varepsilon$, and the proof goes through as long as we have the corresponding version of Theorem 1.1.

Since Theorem 1.1 is proved via Lemma 4.1, it suffices to prove Lemma 4.1 where $\mathcal{U}(4)$ is replaced with $\mathcal{U}_\gamma(4)$. The crux is to prove the inequality (27), that is for some $C, C' > 0$, it holds for all $x \ge 0$ that

$$\Pr[|\det M| \le x] \le C' x^C, \tag{49}$$

where M is the matrix form of the linear map $M : \tau - \tau' \mapsto \mathrm{Tr}_A[G(\tau - \tau')G^\dagger]$, for $\tau - \tau'$ in a certain fixed 3-dimensional subspace of Δ_2.

Note that by Proposition 4.2, each entry of M is in $[-2, 2]$, while by (26), each entry of M is a Lipschitz function of G under distance $d_\diamond$. This is because when $G, G' \in \mathbb{U}(4)$ that $d_\diamond(G, G') \le \delta$ corresponds to matrices M and M', for any $\tau - \tau' \in \Delta_2$ and $\sigma \in \Delta_1$ with $\|\tau - \tau'\|_{\mathrm{F}} = \|\sigma\|_{\mathrm{F}} = 1$ we have

$$\begin{aligned}\left|\mathrm{Tr}[\sigma M(\tau - \tau')] - \mathrm{Tr}[\sigma M'(\tau - \tau')]\right| &= \left|\mathrm{Tr}\left[(I \otimes \sigma)\left(G(\tau - \tau')G^\dagger - G'(\tau - \tau')G'^\dagger\right)\right]\right| \\ &\le \left\|G(\tau - \tau')G^\dagger - G'(\tau - \tau')G'^\dagger\right\|_1 \\ &\le \left\|G\tau G^\dagger - G'\tau G'^\dagger\right\|_1 + \left\|G\tau' G^\dagger - G'\tau' G'^\dagger\right\|_1 \\ &\le 2\delta.\end{aligned} \tag{50}$$

As $\det M$ consists of 6 monomials of degree 3 in the entries of M, we conclude that $|\det M|$ is $2^3 \cdot 3 \cdot 6 = 144$-Lipschitz in G under $d_\diamond$. But when $G' = (U_1 \otimes U_2)G$ we have $M' = U_2 M U_2^\dagger$ which means $|\det M| = \left|\det M'\right|$, and thus $|\det M|$ is also 144-Lipschitz in G under $d_\otimes$.

As a result, since we already know that (49) holds when $G \sim \mathcal{U}(4)$, by Lemma 5.8 we have

$$\Pr_{G\sim\mathcal{U}_\varepsilon(4)}[|\det M| \le x] \le \Pr_{G\sim\mathcal{U}(4)}[|\det M| \le x + 144\varepsilon] \le C'(x+144\varepsilon)^C. \tag{51}$$

However, this will not yield Lemma 4.1 as the bound is even non-zero when $x = 0$. Fortunately, we can simply use the union bound to ignore the cases when $|\det M| \le \varepsilon$ for any gate G on the path, which will only add $\mathrm{poly}(\varepsilon)D$ to the error probability γ. And conditioned on $|\det M| > \varepsilon$, for every $x \ge 0$ we have

$$\Pr_{G\sim\mathcal{U}_\varepsilon(4)}[|\det M| \le x] \le C'(145x)^C, \tag{52}$$

which allows us to prove Lemma 4.1 on $\mathcal{U}_\varepsilon(4)$, albeit with different constants. □

Now we can state Theorem 1.5 formally as follows, and prove the theorem using the idea presented at the start of this section.

Theorem 5.10. *Let $\mathcal{C}$ be a brickwork random quantum circuit on n qubits of depth D, where each gate is independently drawn from $\mathcal{U}_\varepsilon(4)$. Given oracle access to $\mathcal{C}$, for every $\delta, \gamma \in (0,1)$ there is an algorithm that with probability at least $1-\gamma$ outputs a circuit $\tilde{\mathcal{C}}$ in time $\mathrm{poly}(n, 2^D, 1/\varepsilon, 1/\delta, 1/\gamma)$, with the same architecture of $\mathcal{C}$ and $d_\diamond(\mathcal{C}, \tilde{\mathcal{C}}) \le \delta$.*

Proof. By applying Theorem 5.9 on all $n/2$ gates in the first layer of $\mathcal{C}$, we get $G_1, \dots, G_{n/2} \in \mathbb{U}(4)$ such that

$$(G_{1,1} \otimes \cdots \otimes G_{1,n}) \cdot (G_1^\dagger \otimes \cdots G_{n/2}^\dagger) = U_1 \otimes \cdots \otimes U_n \tag{53}$$

for some single-qubit gates $U_1, \dots, U_n \in \mathbb{U}(2)$. Notice that for the gate $G_{2,2} \sim \mathcal{U}_\varepsilon(4)$ in the second layer, the distribution of $G_{2,2}(U_2 \otimes U_3)$ is also an ε-net of $\mathcal{U}(4)$ under $d_\otimes$, which means that we can think of $U_1, \dots, U_n$ as combined into the second layer, and learn the combined gates by Theorem 5.9 using the new circuit oracle $\mathcal{C} \cdot (G_1^\dagger \otimes \cdots G_{n/2}^\dagger)$.

Continue doing so for each of the rest layers of the circuit, and eventually we obtain a brickwork circuit $\mathcal{C}'$ such that

$$\mathcal{C}\mathcal{C}'^\dagger = U_1' \otimes \cdots \otimes U_n' \tag{54}$$

for some single-qubit gates $U_1', \dots, U_n' \in \mathbb{U}(2)$. We can learn each gate U_i' up to δ/n error via quantum process tomography Proposition 2.4, and hence $(U_1' \otimes \cdots \otimes U_n')\mathcal{C}'$ is a brickwork circuit of depth D that is δ-close to $\mathcal{C}$. □

Acknowledgments

B.F., S.G., and W.Z. acknowledge support from AFOSR (FA9550-21-1-0008). The authors thank Anurag Anshu, Adam Bouland, Lijie Chen, Jonas Haferkamp, Robert Huang, Issac Kim, Yunchao Liu, Tony Metger, Marcus Michelen and Tommy Schuster for helpful comments and discussions. This material is based upon work partially supported by the National Science Foundation under Grant CCF-2044923 (CAREER), by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers (Q-NEXT) and by the DOE QuantISED grant DE-SC0020360.

References

[AA11] Scott Aaronson and Alex Arkhipov. "The computational complexity of linear optics". In: STOC '11. San Jose, California, USA: Association for Computing Machinery, 2011, pp. 333–342. ISBN: 9781450306911. DOI: 10.1145/1993636.1993682.

[Aar+23] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. *Quantum Pseudoentanglement*. 2023. arXiv: 2211.00747 [quant-ph].

[AH23] Scott Aaronson and Shih-Han Hung. "Certified Randomness from Quantum Supremacy". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. STOC 2023. Orlando, FL, USA: Association for Computing Machinery, 2023, pp. 933–944. ISBN: 9781450399135. DOI: 10.1145/3564246.3585145.

[Aru+19] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (Oct. 2019), pp. 505–510. ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5.

[Bas+24] Roozbeh Bassirian, Adam Bouland, Bill Fefferman, Sam Gunn, and Avishay Tal. *On Certified Randomness from Fourier Sampling or Random Circuit Sampling*. 2024. arXiv: 2111.14846 [quant-ph].

[BP20] Bruno Bertini and Lorenzo Piroli. "Scrambling in random unitary circuits: Exact results". In: *Phys. Rev. B* 102 (6 Aug. 2020), p. 064305. DOI: 10.1103/PhysRevB.102.064305.

[Boi+18] Sergio Boixo et al. "Characterizing quantum supremacy in near-term devices". In: *Nature Physics* 14.6 (Apr. 2018), pp. 595–600. ISSN: 1745-2481. DOI: 10.1038/s41567-018-0124-x.

[Bou+22] Adam Bouland, Bill Fefferman, Zeph Landau, and Yunchao Liu. "Noise and the Frontier of Quantum Supremacy". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, Feb. 2022. DOI: 10.1109/focs52979.2021.00127.

[Bou+18] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. "On the complexity and verification of quantum random circuit sampling". In: *Nature Physics* 15.2 (Oct. 2018), pp. 159–163. ISSN: 1745-2481. DOI: 10.1038/s41567-018-0318-2.

[Bra+24] Paolo Braccia, Pablo Bermejo, Lukasz Cincio, and M. Cerezo. *Computing exact moments of local random quantum circuits via tensor networks*. 2024. arXiv: 2403.01706 [quant-ph].

[BHH16] Fernando G.S.L. Brandão, Aram W. Harrow, and Michał Horodecki. "Local Random Quantum Circuits are Approximate Polynomial-Designs". In: *Commun. Math. Phys.* 346.2 (2016), pp. 397–434. DOI: 10.1007/s00220-016-2706-8.

[BF13] Winton Brown and Omar Fawzi. *Scrambling speed of random quantum circuits*. 2013. arXiv: 1210.6644 [quant-ph].

[Buh+01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. "Quantum Fingerprinting". In: *Physical Review Letters* 87.16 (Sept. 2001). ISSN: 1079-7114. DOI: 10.1103/physrevlett.87.167902.

[CW01] Anthony Carbery and James Wright. "Distributional and L^q norm inequalities for polynomials over convex bodies in $\mathbb{R}^n$". In: *Mathematical Research Letters* 8.3 (2001), pp. 233–248. DOI: 10.4310/mrl.2001.v8.n3.a1.

[Che+24a] Chi-Fang Chen, Adam Bouland, Fernando G. S. L. Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. *Efficient unitary designs and pseudorandom unitaries from permutations*. 2024. arXiv: 2404.16751 [quant-ph].

[Che+24b] Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, and Patrick Hayden. *Efficient Unitary T-designs from Random Sums*. 2024. arXiv: 2402.09335 [quant-ph].

[Che+24c] Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp, Yunchao Liu, Tony Metger, and Xinyu Tan. *Incompressibility and spectral gaps of random circuits*. 2024. arXiv: 2406.07478 [quant-ph].

[CL21] Chi-Fang Chen and Andrew Lucas. "Operator Growth Bounds from Graph Theory". In: *Communications in Mathematical Physics* 385.3 (July 2021), pp. 1273–1323. ISSN: 1432-0916. DOI: 10.1007/s00220-021-04151-6.

[CLY23] Chi-Fang Chen, Andrew Lucas, and Chao Yin. "Speed limits and locality in many-body quantum dynamics". In: *Reports on Progress in Physics* 86.11 (Sept. 2023), p. 116001. ISSN: 1361-6633. DOI: 10.1088/1361-6633/acfaae.

[CL23] Man-Duen Choi and Chi-Kwong Li. "On unital qubit channels". In: *Quantum Inf. Comput.* 23.7-8 (2023), pp. 562–576. DOI: 10.26421/QIC23.7-8-2.

[DHB22a] Alexander M. Dalzell, Nicholas Hunter-Jones, and Fernando G. S. L. Brandão. "Random Quantum Circuits Anticoncentrate in Log Depth". In: *PRX Quantum* 3.1 (Mar. 2022). ISSN: 2691-3399. DOI: 10.1103/prxquantum.3.010333.

[DHB22b] Alexander M. Dalzell, Nicholas Hunter-Jones, and Fernando G.S.L. Brandão. "Random Quantum Circuits Anticoncentrate in Log Depth". In: *PRX Quantum* 3 (1 Mar. 2022), p. 010333. DOI: 10.1103/PRXQuantum.3.010333.

[Dan+09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. "Exact and approximate unitary 2-designs and their application to fidelity estimation". In: *Phys. Rev. A* 80 (1 July 2009), p. 012304. DOI: 10.1103/PhysRevA.80.012304.

[EAZ05] Joseph Emerson, Robert Alicki, and Karol Zyczkowski. "Scalable Noise Estimation with Random Unitary Operators". In: *Journal of Optics B: Quantum and Semiclassical Optics* 7 (Mar. 2005). DOI: 10.1088/1464-4266/7/10/021.

[FPR19] Claudia Fassino, Giovanni Pistone, and Maria Piera Rogantin. "Computing the Moments of the Complex Gaussian: Full and Sparse Covariance Matrix". In: *Mathematics* 7.3 (2019). ISSN: 2227-7390. DOI: 10.3390/math7030263.

[Fef+23] Bill Fefferman, Soumik Ghosh, Michael Gullans, Kohdai Kuroiwa, and Kunal Sharma. *Effect of non-unital noise on random circuit sampling*. 2023. arXiv: 2306.16659 [quant-ph].

[Fis+23] Matthew P.A. Fisher, Vedika Khemani, Adam Nahum, and Sagar Vijay. "Random quantum circuits". In: *Annual Review of Condensed Matter Physics* 14.1 (2023), pp. 335–379. ISSN: 1947-5462. DOI: 10.1146/annurev-conmatphys-031720-030658.

[Haa+23] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. "Query-optimal estimation of unitary channels in diamond distance". In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2023, pp. 363–390. DOI: 10.1109/FOCS57990.2023.00028.

[HLT24] Jeongwan Haah, Yunchao Liu, and Xinyu Tan. *Efficient approximate unitary designs from random Pauli rotations*. 2024. arXiv: 2402.05239 [quant-ph].

[Haf22] Jonas Haferkamp. "Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$". In: *Quantum* 6 (Sept. 2022), p. 795. ISSN: 2521-327X. DOI: 10.22331/q-2022-09-08-795.

[Han+18] Dominik Hangleiter, Juan Bermejo-Vega, Martin Schwarz, and Jens Eisert. "Anticoncentration theorems for schemes showing a quantum speedup". In: *Quantum* 2 (May 2018), p. 65. ISSN: 2521-327X. DOI: 10.22331/q-2018-05-22-65.

[HG24] Dominik Hangleiter and Michael J. Gullans. "Bell Sampling from Quantum Circuits". In: *Phys. Rev. Lett.* 133 (2 July 2024), p. 020601. DOI: 10.1103/PhysRevLett.133.020601.

[Har+21] Aram W. Harrow, Linghang Kong, Zi-Wen Liu, Saeed Mehraban, and Peter W. Shor. "Separation of Out-Of-Time-Ordered Correlation and Entanglement". In: *PRX Quantum* 2 (2 June 2021), p. 020339. DOI: 10.1103/PRXQuantum.2.020339.

[HL09] Aram W. Harrow and Richard A. Low. "Random Quantum Circuits are Approximate 2-designs". In: *Communications in Mathematical Physics* 291.1 (July 2009), pp. 257–302. ISSN: 1432-0916. DOI: 10.1007/s00220-009-0873-6.

[HM23] Aram W. Harrow and Saeed Mehraban. "Approximate Unitary t-Designs by Short Random Quantum Circuits Using Nearest-Neighbor and Long-Range Gates". In: *Commun. Math. Phys.* 401.2 (2023), pp. 1531–1626. DOI: 10.1007/s00220-023-04675-z.

[HP07] Patrick Hayden and John Preskill. "Black holes as mirrors: quantum information in random subsystems". In: *Journal of High Energy Physics* 2007.09 (Sept. 2007), pp. 120–120. ISSN: 1029-8479. DOI: 10.1088/1126-6708/2007/09/120.

[Hua+24] Hsin-Yuan Huang, Yunchao Liu, Michael Broughton, Isaac Kim, Anurag Anshu, Zeph Landau, and Jarrod R. McClean. "Learning Shallow Quantum Circuits". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. STOC 2024. Vancouver, BC, Canada: Association for Computing Machinery, 2024, pp. 1343–1351. DOI: 10.1145/3618260.3649722.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. *Pseudorandom Quantum States*. Cryptology ePrint Archive, Paper 2018/544. 2018. URL: https://eprint.iacr.org/2018/544.

[JBS22] Shao-Kai Jian, Gregory Bentsen, and Brian Swingle. *Linear Growth of Circuit Complexity from Brownian Dynamics*. 2022. arXiv: 2206.14205 [quant-ph].

[Kan17] Daniel Kane. "A structure theorem for poorly anticoncentrated polynomials of Gaussians and applications to the study of polynomial threshold functions". In: *The Annals of Probability* 45.3 (2017), pp. 1612–1679. DOI: 10.1214/16-AOP1097.

[LL24] Zeph Landau and Yunchao Liu. *Learning quantum states prepared by shallow circuits in polynomial time*. 2024. URL: https://people.eecs.berkeley.edu/~yunchaoliu/files/learningstate.pdf.

[LR72] Elliott H. Lieb and Derek W. Robinson. English (US). In: *Communications In Mathematical Physics* 28.3 (Sept. 1972), pp. 251–257. ISSN: 0010-3616. DOI: 10.1007/BF01645779.

[Liu+22] Yunchao Liu, Matthew Otten, Roozbeh Bassirianjahromi, Liang Jiang, and Bill Fefferman. *Benchmarking near-term quantum computers via random circuit sampling*. 2022. arXiv: 2105.05232 [quant-ph].

[Lov10] Shachar Lovett. *An elementary proof of anti-concentration of polynomials in Gaussian variables*. Electronic Colloquium on Computational Complexity (ECCC). 2010. URL: https://eccc.weizmann.ac.il/report/2010/182.

[Mec19] Elizabeth S Meckes. *The random matrix theory of the classical compact groups*. Vol. 218. Cambridge University Press, 2019. DOI: 10.1017/9781108303453.

[MNV16] Raghu Meka, Oanh Nguyen, and Van Vu. "Anti-concentration for Polynomials of Independent Random Variables". In: *Theory of Computing* 12.11 (2016), pp. 1–17. DOI: 10.4086/toc.2016.v012a011.

[MZ13] Raghu Meka and David Zuckerman. "Pseudorandom Generators for Polynomial Threshold Functions". In: *SIAM Journal on Computing* 42.3 (2013), pp. 1275–1301. DOI: 10.1137/100811623.

[Met+24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. *Simple constructions of linear-depth t-designs and pseudorandom unitaries*. 2024. arXiv: 2404.12647 [quant-ph].

[Mor+23] A. Morvan et al. *Phase transition in Random Circuit Sampling*. 2023. arXiv: 2304.11119 [quant-ph].

[Mov23] Ramis Movassagh. "The hardness of random quantum circuits". In: *Nature Physics* 19.11 (Nov. 2023), pp. 1719–1724. ISSN: 1745-2481. DOI: 10.1038/s41567-023-02131-2.

[Nah+17a] Adam Nahum, Jonathan Ruhman, Sagar Vijay, and Jeongwan Haah. "Quantum Entanglement Growth under Random Unitary Dynamics". In: *Physical Review X* 7.3 (July 2017). ISSN: 2160-3308. DOI: 10.1103/physrevx.7.031016.

[Nah+17b] Adam Nahum, Jonathan Ruhman, Sagar Vijay, and Jeongwan Haah. "Quantum Entanglement Growth under Random Unitary Dynamics". In: *Phys. Rev. X* 7 (3 July 2017), p. 031016. DOI: 10.1103/PhysRevX.7.031016.

[NVH18] Adam Nahum, Sagar Vijay, and Jeongwan Haah. "Operator Spreading in Random Unitary Circuits". In: *Phys. Rev. X* 8 (2 Apr. 2018), p. 021014. DOI: 10.1103/PhysRevX.8.021014.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[PR61] Erdős Paul and Alfréd Rényi. "On a classical problem of probability theory". In: *Magyar Tud. Akad. Mat. Kutató Int. Közl* 6.1 (1961), pp. 215–220.

[PSQ20] Lorenzo Piroli, Christoph Sünderhauf, and Xiao-Liang Qi. "A random unitary circuit model for black hole evaporation". In: *Journal of High Energy Physics* 2020.4 (Apr. 2020). ISSN: 1029-8479. DOI: 10.1007/jhep04(2020)063.

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. *Random unitaries in extremely low depth*. 2024. arXiv: 2407.07754 [quant-ph].

[WW22] Henrik Wilming and Albert H. Werner. "Lieb-Robinson bounds imply locality of interactions". In: *Phys. Rev. B* 105 (12 Mar. 2022), p. 125101. DOI: 10.1103/PhysRevB.105.125101.

[YE23] Lisa Yang and Netta Engelhardt. *The Complexity of Learning (Pseudo)random Dynamics of Black Holes and Other Chaotic Systems*. 2023. arXiv: 2302.11013 [hep-th].

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il