On verifiable quantum advantage with peaked circuit sampling

Scott Aaronson[*1] and Yuxuan Zhang[†2,3]

[1]Department of Computer Science, The University of Texas at Austin.
[2]Department of Physics and Centre for Quantum Information and Quantum Control,
University of Toronto
[3]Vector Institute for Artificial Intelligence, W1140-108 College Street, Schwartz Reisman
Innovation Campus, Toronto, Ontario M5G 0C6, Canada

May 22, 2024

Abstract

Over a decade after its proposal, the idea of using quantum computers to sample hard distributions has remained a key path to demonstrating quantum advantage. Yet a severe drawback remains: verification seems to require classical computation that is exponential in the system size, n. As an attempt to overcome this difficulty, we propose a new candidate for quantum advantage experiments with otherwise-random "peaked circuits", i.e., quantum circuits whose outputs have high concentrations on a computational basis state. Naturally, the heavy output string can be used for classical verification.

In this work, we analytically and numerically study an explicit model of peaked circuits, in which τ_r layers of uniformly random gates are augmented by τ_p layers of gates that are optimized to maximize peakedness. We show that getting $1/\mathrm{poly}(n)$ peakedness from such circuits requires $\tau_p = \Omega((\tau_r/n)^{0.19})$ with overwhelming probability. However, we also give numerical evidence that nontrivial peakedness is possible in this model—decaying exponentially with the number of qubits, but more than can be explained by any approximation where the output of a random quantum circuit is treated as a Haar-random state. This suggests that these peaked circuits have the potential for future verifiable quantum advantage experiments.

Our work raises numerous open questions about random peaked circuits, including how to generate them efficiently, and whether they can be distinguished from fully random circuits in classical polynomial time.

---

[*]aaronson@cs.utexas.edu

[†]quantum.zhang@utoronto.ca

1   Introduction

Demonstrating quantum advantage [AA11, Pre12, AA13, CGW13, AC16, BFNV18, Mov18], that is, having a quantum computer perform a task that even the best classical computers would find practically impossible, has been one of the most exciting challenges in quantum computation. In 2019, Google's Sycamore processor claimed quantum advantage by performing a random circuit sampling task in 200 seconds that, they then estimated, would take the world's most powerful classical computer approximately 10,000 years to complete [AAB+19]. Since then, a continuous intellectual tug-of-war has taken place between various quantum advantage claims by groups like USTC and Xanadu [ZWD+20, MLA+22, ZCC+22] and improved classical simulation techniques to spoof the experiments' results [HZN+20, BCG20, GKC+21, PCZ22, OJF23]. These attacks generally exploit the noise and lack of error-correction on near-term devices [NJF20, GKC+21, DHJB21]. To some skeptics, the attacks raise serious doubts about whether quantum supremacy was achieved at all—or if it was, then whether it remains achieved.

Shouldn't it be easy to defeat the classical spoofing attacks by simply scaling the experiments up? This brings us to the most fundamental drawback of the current experiments. Namely, even checking their results takes exponential classical computation. Worse, this seems to be inherent—ironically, by the very same theoretical evidence that tells us that spoofing should be exponentially hard! Thus, if we insist on directly verifying the quantum computer's outputs, then in practice, we can't currently scale much beyond ~ 60 qubits or photons. It of course helps that verification, unlike spoofing, can be done at leisure—one can spend weeks on it, burning hundreds of thousands of dollars of computer time! Nevertheless, we seem locked into a "cat-and-mouse game": we can never put spoofing completely beyond classical reach, lest we put verification beyond reach as well. As long as this remains true, it will be a question mark hanging over quantum advantage itself.

But what about other possibilities for quantum advantage? Can we reach quantum advantage by, for example, running known quantum algorithms? At a high level, there are three desired properties of a near-term advantage experiment candidate:

- Feasible on near-term devices

- Hard to simulate classically

- Easy to verify classically

Arguably, we know how to satisfy any two out of the three, but no current quantum protocol satisfies all three requirements. The problem, in a sentence, is that the quantum algorithms that deliver clear speedups don't seem to work on near-term devices, while the quantum algorithms that work on near-term devices don't seem to deliver clear speedups.

Reaching quantum advantage with algorithms like Shor's algorithm [Sho94] and the recent breakthrough by Yamakawa and Zhandry [YZ22], while providing convincing speedups and efficiently verifiable, requires delicate control of quantum coherence and would most likely not be feasible for near-term devices. In a different direction, despite numerous recent efforts devoted to near-term algorithms like the quantum approximate optimization algorithm (QAOA) [FGG14, FH16, ZWC+20, ZZP21] and variational quantum eigensolver (VQE) [PMS+14, KMT+17, GEBM19, BCM+21, KMCVY22], they still haven't yielded plausible signs for an in-principle quantum speed up. In a third direction, there are protocols for verifying quantumness that use, for example, post-quantum secure trapdoor claw-free functions [BCM+21, KMCVY22]. Still, these protocols all require delicate controls over superpositions and are likely to be unsuitable for noisy intermediate-scale quantum (NISQ) [Pre18] devices. Other NISQy proposals use pseudorandomness: A challenger
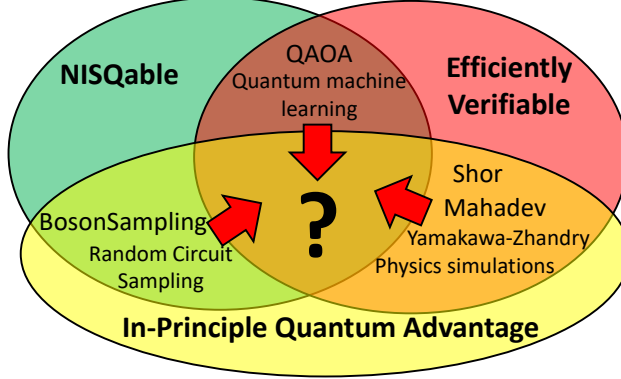
Figure 1: **Field guide to verifiable quantum advantage.** Out of three possible paths to verifiable quantum advantage, we study whether it is possible to make sampling-based protocols efficiently checkable.

creates a pseudorandom quantum circuit C that conceals a secret s and sends C to a quantum computer; the latter has to find s by running C. One such attempt uses exotic classical error correction codes [SB09, BMS17], but the classical security of such protocols is still under debate [KM19, CvdW22, BCJ23, BCJ23, BKNY23, BEG+24, MBT+24, RWL24].

In this work, we start from random circuit sampling and look for a way to make it verifiable using so-called "peaked circuits." Roughly speaking, starting with the all-zero state, a peaked circuit lets the state wander around the Hilbert space, *seemingly* at random, but then ending at a state that has a significant overlap with a computational basis state.

Definition 1.1 (Peaked Circuit)**.** *Given $\delta \in (0,1]$, we call the unitary C δ-peaked if:*

$$\max_{s \in \{0,1\}^n} |\langle s|C|0^n\rangle|^2 \geq \delta$$

with a corresponding peak weight $\delta_s \equiv |\langle s|C|0^n\rangle|^2$.

In other words, a circuit C is δ-peaked if, when applied to the all-0 initial state and then measured in the computational basis, it yields some particular output string with probability at least δ.

Note that, without loss of generality, one can often focus on some particular δ_s, such as δ_{0^n}. This is because, given a circuit with a peak at any $s \in \{0,1\}^n$, one can move the peak to 0^n by (for example) adding a small number of NOT gates at the last layer.

Peaked circuits can be used for efficient verification of quantum advantage, as follows: an challenger provides an alleged quantum computer with a circuit C, which is promised *either* to have been chosen uniformly at random, or to have been chosen from a distribution of peaked circuits. Using a quantum computer, one can simply run C a few times to see whether it is peaked (and the challenger knows which). Of course, the question remains of whether distinguishing peaked from uniformly random quantum circuits (RQCs) is hard for a classical computer.

One extremely interesting method to obtain peaked quantum circuits is to start with truly random circuits, then *postselect on the event that the circuits happen to be δ-peaked*, for some fixed δ (say, $1/10$). One could then ask the question:

Problem 1.2. *Can the resulting peaked circuits be distinguished, in classical polynomial time, from truly random quantum circuits?*

2

(Of course the circuits can be distinguished in *quantum* polynomial time: just run them $O(1)$ times, and check whether a peak emerges in the output distribution!)

There are conflicting intuitions about the answer to Problem 1.2: on the one hand, maybe the distribution over peaked circuits is dominated by those that are peaked for "trivial" reasons, such as containing a large number of gates that are promptly cancelled by their inverses, giving an implementation of the identity. On the other hand, maybe the distribution is dominated by circuits that "take an otherwise random tour through Hilbert space," which *so happens* (because of the postselection) to end up near a computational basis state.

Note that we could pose the same question in Nielsen's geometric picture of quantum circuits [Nie05]. There, the question becomes: suppose we pick a random polynomial-length path p in the complexity geometry, which starts at the computational basis state $|0\rangle$, and which is constrained to end near a random computational basis state $|s\rangle$. If we feed a description of p to a classical computer, can the classical computer easily distinguish p from a random unconstrained path, for example by "contracting" it to an essentially trivial path from $|0\rangle$ to $|s\rangle$? Or, relatedly, can the classical computer efficiently learn the endpoint $|s\rangle$?

1.1 Our Results

In this paper, we focus on a different but related method for generating random peaked circuits. Consider circuits that have τ_r layers of random gates, followed by τ_p 'peaking' layers of gates that can be chosen to optimize the peakedness of the overall circuit (see Fig. 2). Note that, when $\tau_p \geq \tau_r$, we are guaranteed a 1-peaked circuit, since we can always just choose the peaking gates to invert the random gates. Thus, we are interested in what happens when $\tau_p < \tau_r$. For example,

Problem 1.3. *Suppose $\tau_p = \tau_r/2$, or $\tau_p = \sqrt{\tau_r}$: can we obtain a nontrivially peaked circuit then, with high probability over the τ_r random layers?*

A central reason to modify the question in this way is that the original Problem 1.2 turns out to be prohibitive to study numerically, as truly random quantum circuits are very unlikely to be peaked because their output distributions are known to be not too concentrated on a small number of output strings [HBVSE18, HHB$^+$20, BCHJ$^+$21, DHJB22]. A more quantitative statement can be found in Corollary 2.3,

Note that our new question could be rephrased as: does the state $|\psi_C\rangle = C|0\rangle$ output by a polynomial-size random quantum circuit C have any "exploitable structure" at all to distinguish it from a Haar-random state—other than the obvious, namely that $C^{-1}|\psi_C\rangle = |0\rangle$?

Perhaps surprisingly, our numerical results provide strong evidence that the answer to this question is 'yes.' In other words: whether or not it can be used for verifiable quantum advantage experiments, there *is* structure in the states output by random quantum circuits, which lets us achieve nontrivial peakedness with a surprisingly small number of additional gates. We leave the explanation of this structure as our central open problem.

What analytic results we did manage to prove are in Section 2. First, for $1d$ and all-to-all geometries, we show that the chance of finding $\Omega(2^{-0.49})$-peaked circuits in a logarithmic-depth RQCs is already exponentially small in n. Moreover, by using the known fact that polynomial-depth random quantum circuits give t-designs, we show that obtaining $1/\text{poly}(n)$ peakedness, starting from a random circuit of depth τ, requires $\Omega((\tau/n)^{0.19})$ gates for a $1d$ brick wall architecture.

Next, in Section 3, we present our numerical results. Here, we fix $\tau_p := c\tau_r$, for some $c \in (0, 1)$, then we fix τ_r layers of random gates, and finally, we use gradient descent to choose the τ_p peaking layers to optimize the overall peakedness. Our central finding is that nontrivial peakedness is

achievable even for constants $c \ll 1$: for example, with $n = 12$ qubits and $\tau_r = 40$ random layers of gates, by adding merely $\tau_p = 10$ peaking layers, we can obtain, on average, a peakedness of $\delta \approx 0.2$.

Examining the actual peaked circuits, two trends emerge. First, we find that the output distributions are very similar to the distributions that arise from truly random circuits, *except* that the probability of the single peaked string has been massively enhanced. Second, we find that the obtained peakedness δ is tightly concentrated about its mean; it fluctuates little from one circuit C to another. These observations suggest, though of course they don't prove, that these peaked circuits might have "universal," "pseudorandom" properties that make them challenging to distinguish from truly random circuits.

Admittedly, for fixed c and τ_r/n, the peakedness δ that we are able to achieve seems to decay exponentially with n. Having said that, extrapolating our numerically-found relationships to larger n, we estimate that when (say) we have $n = 50$ qubits, $\tau_r = 50$ random layers, and $\tau_p = 25$ peaking layers, a peakedness of $\delta \approx 0.0005$ should still be achievable, which would be feasible to detect in an experiment.[1]

But there is an additional issue: the computation time needed to optimize the τ_p peaking layers. On the one hand, it is entirely possible that our gradient descent algorithm got stuck in local optima, and that a better optimization method would reveal that much higher peakedness values δ are achievable; on the other hand, one might say, peaked pseudorandom quantum circuits are of limited use for quantum advantage experiments, if there is no efficient way to *find* those circuits! This leads to a second fundamental open question left by this paper:

Open Problem 1.4. *For given δ, is there an efficient algorithm to generate quantum circuits that have peakedness δ and that are otherwise "as random as possible" (for example, that contain a large initial segment of uniformly random gates, as in this paper)?*

2 Analytical results

2.1 Peaked circuits are rare in RQCs

Given a quantum circuit C, let p_C be the associated probability distribution over the 2^n possible output strings. Then C's *collision probability* can be defined as $\pi_C := \sum_s p_C[s]^2$. Next, given an ensemble of random circuits C, we will call it "well-spread" if the averaged collision probability is a constant times that of the maximally mixed state (which has collision probability exactly 2^{-n}):

Definition 2.1. *A circuit ensemble is well-spread if the expected collision probability satisfies*

$$\mathop{\mathbb{E}}_C\left[\pi_C\right] \leq \frac{\gamma}{2^n} \tag{1}$$

for some constant γ.

Intuitively, with overwhelming probability over the choice of circuit C, the output distribution cannot be too peaked. This implies the following bound:

Theorem 2.2 (Probability of finding peaked circuits in an well-spread circuit ensemble). *Let P_δ be the probability of finding a δ-peaked circuit in a well-spread ensemble. Then $P_\delta = O(\frac{1}{\delta^2 2^n})$.*

---

[1]To compare, Google's first quantum advantage demonstration on 53 qubits took 5×10^6 total samples over each random circuit instance [AAB+19]; in practice, this is more than enough to catch the peakedness even if merely 1% overall state fidelity can be achieved.
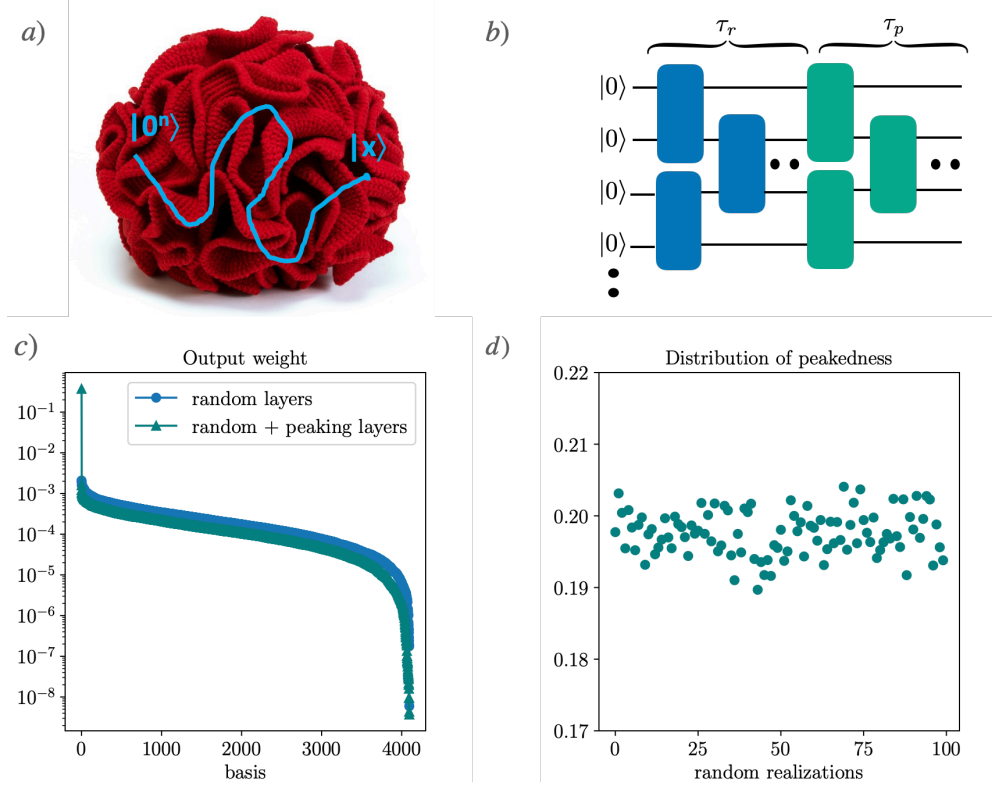
Figure 2: **Generating peaked circuits from random circuits. a)** A peaked circuit is a non-trivial short path connecting two computational bases. **b)** An $1d$ circuit structure is shown here. Each block stands for a two-qubit gate: The blue blocks are drawn from the Haar-random distribution and the teal blocks are the 'peaking' quantum gates. In a numerical solver, we optimize the parameters of the peaking gates, aiming at maximizing the peak weight. **c)** Example of the (sorted) output weight distribution of a peaked circuit generated with our construction. At system size $n = 12$, the blue curve is the output weight distribution after $\tau_r = 40$ random brickwall layers, and teal represents the distribution after merely $\tau_p = 10$ additional peaking layers. **d)** we repeat the process in **c** for 100 random circuits and examine the distribution over δ, which turns out to have a small variance.

Proof. Given any δ-peaked circuit C, by Definition 1.1, its collision probability satisfies

$$\pi_C = \sum_s p_C[s]^2 \geq \max_s p_C[s]^2 \geq \delta^2.$$

So taking the expectation over all C, we have

$$\mathbb{E}_C \left[\pi_C \right] \geq \delta^2 P_\delta.$$

Combined with Definition 2.1 we have

$$\delta^2 P_\delta \leq \mathbb{E}_C \left[\pi_C \right] \leq \frac{\gamma}{2^n}.$$

$\square$

This shows that, in a well-spread ensemble, the probability of finding an δ-peaked circuit where $\delta = \Omega(2^{-0.49n})$ is exponentially small in n. Furthermore, random quantum circuits for $1d$ and fully connected architectures are known to well-spread even in logarithmic depth [DHJB22], which gives the following corollary:

Corollary 2.3 (Peaked circuits are rare in logarithmic depth). *Assuming a $1d$, fully-connected random circuit architecture with circuit depth $\tau = \Omega(\log n)$, the probability that a random circuit C is δ-peaked, where $\delta = \Omega(2^{-0.49n})$, is $\exp(-\Omega(n))$.*

Numerically, for example, we found that in the $1d$ brick wall architecture, with $\tau_r = n = 10$, the maximum peakedness in 10,000 random trials was already below 0.04 (see Fig. 2).

2.2 How many layers are necessary to 'peak' a RQC?

For the rest of the paper, we focus on the circuit model discussed in Problem 1.3. Specifically, we are interested in the relationship among τ_p, τ_r, and δ: for example, for given δ, how many peaking layers must we add to a given number of random layers to obtain a δ-peaked circuit?

In this section, we prove that when $\delta = 1/\mathrm{poly}(n)$, the number τ_p of peaking layers needs to grow at least polynomially with τ_r.

Theorem 2.4 (Circuit lower bound for $1/\mathrm{poly}(n)$-peaked circuits). *In a n-qubit system, obtaining a δ-peaked circuit, where δ is at least $1/\mathrm{poly}(n)$, from a random quantum circuit C with depth $\tau \gg n$, with high probability over C, requires at least $\Omega((\tau_r/n)^{0.19})$ layers.*

Our lower bound can be proved with the two following results:

1. Polynomial-depth random circuits form approximate unitary t-designs [AE07, GAE07, DCEL09, BHH16, Haf22, MHJ23, LZL$^+$23].

2. Circuits sampled from an approximate unitary t-design have high "strong complexity" (a notion to be defined later) and thus cannot be approximated with a shallow circuit [BCHJ$^+$21].

2.2.1 Unitary t-design

A probability distribution $\mathcal{E}$ over unitary operations forms a unitary t-design if there is *no* super-operator acting on a t-fold Hilbert space to distinguish it from the Haar distribution up to some given precision:

Definition 2.5 (Approximate unitary t-design). *For some constant ϵ, a probability distribution $\mathcal{E}$ on $U(d)$, where $d = 2^n$, forms an ϵ-approximate unitary t-design if it obeys*

$$||\Phi_{\mathcal{E}}^{(t)} - \Phi_{\mathrm{Haar}}^{(t)}||_\diamond \leq \epsilon \tag{2}$$

where $\Phi_{\mathcal{E}}^{(t)}(A)$ is the t-fold moment superoperator of a operator A with respect to the probability distribution $\mathcal{E}$, on $\mathcal{H}^{\otimes t}$, defined as:

$$\Phi_{\mathcal{E}}^{(t)}(A) = \int_{\mathcal{E}} U^{\otimes t} A U^{\dagger \otimes t} d\mathcal{E}(U) \tag{3}$$

Currently, the best-known result on approximate t-designs from random quantum circuits is provided by [Haf22]:

Lemma 2.6 (Random circuits form approximate designs)**.** *Random quantum circuits generate ϵ-approximate unitary t-designs in depth $\tau > nt^{5+o(1)}$.*

The samples drawn from a unitary t-design are known to have well-spread properties with overwhelmingly high probability; that is, the output distribution will have a peak weight that is exponentially small in the system size n.

2.2.2 Strong circuit complexity

While circuit complexity refers to the minimum number of elementary gates needed to perform a certain computation, the "*strong* circuit complexity," defined by Brandão et al. [BCHJ$^+$21], captures the difficulty of *distinguishing* a given circuit from the completely depolarizing channel, $\mathcal{D}$:

Definition 2.7 (Strong circuit complexity, ancilla-free)**.** *The strong complexity of a quantum circuit C is the minimal circuit size required to implement a measurement, with no ancilla qubits, that distinguishes $\rho \to C\rho C^\dagger$ from the completely depolarizing channel $\mathcal{D} : \rho \to \mathbb{I}/d$ with fixed constant bias (say, $1/2$).*

Similarly, the strong *state* complexity is defined as the minimum number of gates required to implement some measurement M to *distinguish* a given quantum state $|\psi\rangle$ with the maximally mixed state $\rho_0 = \mathbb{I}/d$ to some certain resolution η. Formally, let $\beta(r, |\psi\rangle)$ be the maximum bias with which $|\psi\rangle$ can be distinguished from the maximally mixed state, via a circuit with at most r gates from the gate set $\mathcal{G} \subseteq U(4)$:

$$\beta(r, |\psi\rangle) = \max |\operatorname{Tr}\{M(|\psi\rangle\langle\psi| - \rho_0)\}| \tag{4}$$

$$\text{s.t. } M \text{ can be implemented with at most } r \text{ gates} \tag{5}$$

Then the strong state complexity is defined as:

Definition 2.8 (Strong state complexity)**.** *For a given $r \in \mathbb{N}$ and $\eta \in (0,1)$, a pure state $|\psi\rangle$ has strong η-state complexity at most r if and only if $\beta(r, |\psi\rangle) \geq 1 - 1/d - \eta$. We denote this $\mathcal{C}_\eta(|\psi\rangle) \leq r$.*

It is not hard to see that the strong state complexity is an upper bound on the conventional circuit complexity, of approximately *preparing* a state:

Lemma 2.9 (Strong state complexity to regular state complexity)**.** *If a quantum state $|\psi\rangle$ has strong complexity $\mathcal{C}_\eta(|\psi\rangle) \geq r$ for some $r \in \mathbb{N}$ and $\eta \in (0,1)$, then*

$$\min_{size[V]<r} \frac{1}{2} |||\psi\rangle\langle\psi| - V|0\rangle\langle0|V^\dagger||_1 > \sqrt{\eta} \tag{6}$$

or equivalently,

$$\max_{size[V]<r} \frac{1}{2}|\langle0|V|\psi\rangle|^2 < 1 - \eta \tag{7}$$

The proof of Lemma 2.9 is simply that one can invert the circuit to prepare $|\psi\rangle$.

Much more interestingly, [BCHJ$^+$21] proved a lower bound on the strong complexity of states that are generated via approximate unitary t-designs acting on arbitrary initial states:

Theorem 2.10 (Strong state complexity of states sampled from t-designs). *Consider a (pure) state in $d = 2^n$ dimensions that results from applying a randomly sampled unitary associated with an ϵ-approximate $2t$-design to a fixed, arbitrary initial state $|\psi_0\rangle$. Then probability that $U|\psi_0\rangle$ has strong complexity at least r is:*

$$\Pr[\mathcal{C}_\eta(|\psi\rangle) \le r] \le 2(1+\epsilon)dn^r|G|^r \left(\frac{16t^2}{d(1-\eta)^2}\right)^t \tag{8}$$

In other words, so long as

$$r \lessapprox \frac{t[n + 2\log(1-\eta) - 2\log(t)]}{\log(n)}$$

this probability remains tiny, provided that $n \ge |G|$ and $t < d/2$.

Qualitatively, choosing any η such that $1 - \eta = 1/\operatorname{poly}(n)$, and taking the $n \to \inf$ limit where $\log(t) \ll n$, the probability of getting a circuit with strong complexity $o(nt)$ is exponentially small in t. Combining Lemma 2.6 and Theorem 2.10 gives rise to Theorem 2.4, which can be proved with the following argument:

Proof of Theorem 2.4. Let a unitary C_r drawn from an approximate t-design act on the all-0 state without loss of generality. Call the resulting state $|\psi_r\rangle$. Assume that with a high (say, constant) probability over C_r, there exists a circuit C_p such that C_pC_r is a δ-peaked circuit for some $\delta = 1/\operatorname{poly}(n)$ and $\tau_p < t$. Then from Definition 1.1 it follows that $|\langle 0|C_p|\psi_r\rangle|^2 > \delta$.

However, asymptotically in t, Theorem 2.10 says that $|\psi_r\rangle$ cannot have strong state complexity $o(nt)$; further, Lemma 2.9 shows that approximating such a state to a $1/\operatorname{poly}(n)$ precision requires $\Omega(nt)$ elementary gates, or $\Omega(t)$ in circuit depth. Lemma 2.6 then implies that $t = \Omega((\tau_r/n)^{0.19})$. It follows that achieving a peakedness $\delta = \Omega(1/\operatorname{poly}(n))$ requires $\tau_p = \Omega((\tau_r/n)^{0.19})$. $\square$

It is further conjectured that $1d$ random circuits acting on qudits already form t-designs at depth $O(nt)$ [HJ19], which would imply $\tau_p = \Omega(\tau_r/n)$, in which case only an $O(n)$ multiplicative gap between τ_p and τ_r might suffice for a polynomially small peakedness δ. Indeed, we conjecture that a *constant* multiplicative gap might already suffice for this.

3 Numerical results on the peakability of RQCs

Having proved a lower bound on the number of layers τ_p needed for a peaked circuit, we now ask what peakedness *can* be obtained with $\tau_p \ll \tau_r$, with high probability over the τ_r random layers.

We focus, without loss of generality, on δ_{0^n}, the output weight of the all-0 string. We denote by $\overline{\delta_{0^n}}$ the average of this weight over all choices for the random layers.

Our goal in this section is to explore whether there is *any* nontrivial peakedness to be obtained in the regime $\tau_p \ll \tau_r$. For simplicity, we present our results for the case of a $1D$ brick wall circuit geometry, although we found quantitatively similar results in other architectures, such as all-to-all connected circuits.

In Appendix A, we prove that, in the special case that the RQC consists of *two* layers, there exists a single peaking layer we can add that increases the average peak weight from $(25/48)^{n/2}$ to $(7/8)^{n/2}$.

But what about the more interesting case where the RQC has a large depth—say, linear or polynomial in n? Here, lacking an analytic result, we try to gain insight using a numerical optimizer based on machine learning and tensor-network packages PYTORCH [PGM+19] and QUIMB [Gra18].
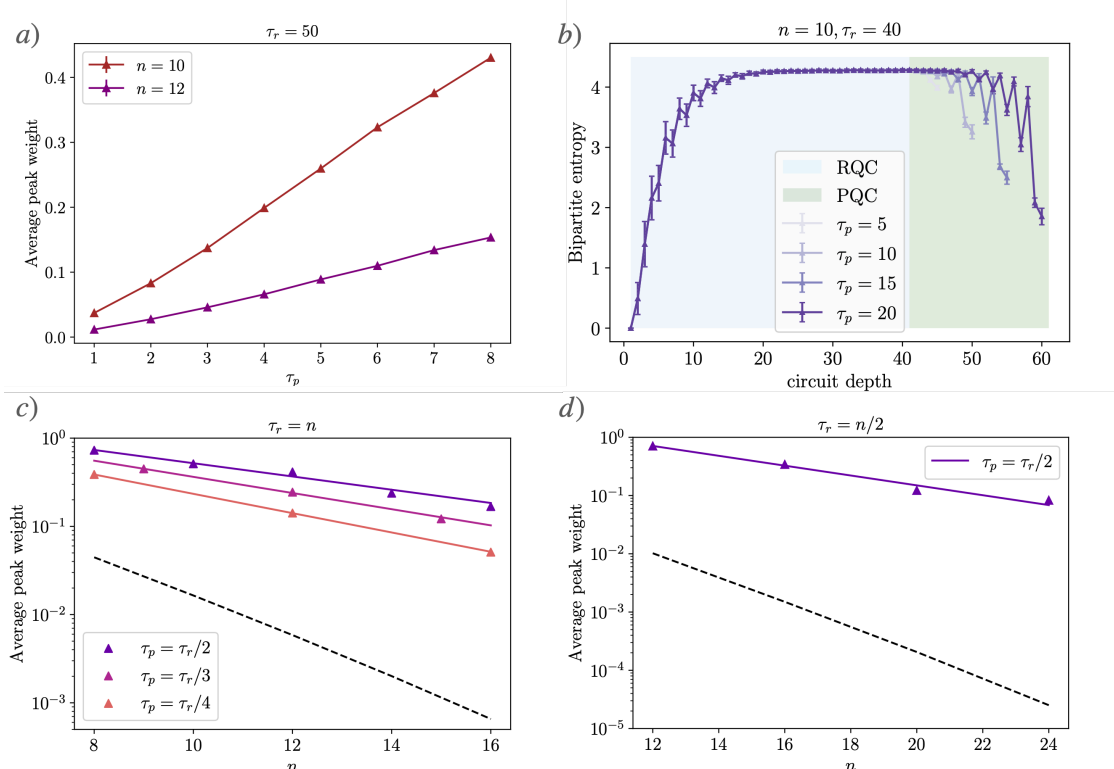
8

Figure 3: **Numerical results on peakability. a)** we fix the number of random layers at 50 and vary the number of peaking layers, with $n = 10$ and $n = 12$ qubits. Error bars for the average peak weights are too small to be visible. Each point is averaged over 100 random instances. **b)** The entanglement entropy of the state at different depths, averaged over 100 instances, if we split the qubits into equal left and right halves. **c)** For each line, we fix the number of peaking layers τ_p to be a constant fraction of the number of random layers τ_r, which we in turn set equal to the system size n. The triangles are data points and the straight lines are fitted curves. The dashed curve shows a 'base' value for average peak weight at $\tau_r = n/2$. This shows that the optimized peaking layers are *not* the trivial inverse of the last τ_p random layers, which could be hard for a classical distinguisher to extract the output string s. **d)** Same as **c** but now the random depth is fixed to be $n/2$ to allow probing larger system sizes.

We stick with the circuit structure in Fig. 2: the first τ_r layers consist of fixed gates that are sampled from a two-qubit Haar distribution. They are followed by τ_p layers of parameterized quantum circuits (PQC) that depend on some variational parameter $\boldsymbol{\theta}$. Call the resulting circuit $C(\boldsymbol{\theta})$. We then run stochastic gradient-descent optimization [KB14] with the following target function:

$$\max_{\boldsymbol{\theta}} \delta_{0^n}(C(\boldsymbol{\theta})) = \max_{\boldsymbol{\theta}} |\langle 0^n | C(\boldsymbol{\theta}) | 0^n \rangle|^2. \tag{9}$$

That is, we maximize the concentration of $C(\boldsymbol{\theta})$ on the all-zero output string. Notice that we don't need to optimize over all output strings s, as any two computational bases are trivially connected with at most one additional layer of NOT gates in the end, which can also be absorbed into the last layer of the PQC.

As shown in the left panel of Figure 3, we first fix $\tau_r = 50$ and examine over τ_p. To our surprise, attaching only $\tau_p = 8$ layers led to an average peak weight of more than 0.15 at system size $n = 10, 12$.

9

On the other hand, as one might expect, the reachable average peak weight drops with system size n at a given ratio τ_p/τ_r. To systematically study the scalability of our peaked circuit construction, we try setting $\tau_r = n$ (bottom left) and $\tau_r = n/2$ (bottom right), and then take τ_p to be various constant fractions of τ_r, namely $\tau_r/2$, $\tau_r/3$, and $\tau_r/4$.

On a log scale, it seems clear that the average peak weights are decreasing exponentially with system size n. Therefore we fit them onto a curve, namely

$$\text{average peak weight} = c \cdot a^{-n}.$$

When $\tau_r = n$ and $\tau_p = n/2$, for example, we get averaged peakedness that falls off as 1.189^{-n}. While this falls off exponentially with n, it falls off much less rapidly than 2^{-n}, or even the $2^{-.49n}$ from Theorem 2.2. This shows that some nontrivial structure in the states output by RQCs is already being exploited.

This numerical result suggests an exponential decay in peakedness even in the regime of constant τ_p/τ_r:

Conjecture 3.1 (Upper bound on average peak weight). *At $\tau_r = \text{poly}(n)$ and $\tau_p = k\tau_r$, where $0 < k < 1$, we have*

$$\text{average peak weight} = O(\exp(-n)).$$

While the exponential decay might be a little disappointing, we've found empirically that $\tau_p \ll \tau_r$ peaking layers—not nearly enough to reverse the τ_r random layers—are nevertheless enough to improve the average peakedness δ almost to the cube root of what it would've been had we merely reversed the last τ_p random layers.

Conjecture 3.2 (Peaking layers improve average peak weight). *At $\tau_r = \text{poly}(n)$ and $\tau_p = k\tau_r$, where $0 < k < 1$, there exists a constant $0 < \alpha < 1$ such that*

$$\text{average peak weight}(\tau_r, \tau_p, n) = \text{average peak weight}(\tau_r - \tau_p, 0, n)^\alpha.$$

If the pattern we observed numerically were to persist, it would imply that an average peak weight of $\sim 5 \times 10^{-4}$ could be obtained on a noiseless 50-qubit machine, at $\tau_r = n = 50$ and $\tau_p = n/2 = 25$. Thus, *if* we also had a fast way to generate these circuits, and *if* their structure was hard to detect classically, then this could provide a solution to the problem of verifiable quantum advantage on NISQ devices.

4 Future directions

A central open problem, of course, is to obtain a rigorous understanding of how much peakedness can be attained in mostly random quantum circuits. In this paper, we showed only that obtaining $1/\text{poly}(n)$ peakedness with high probability requires $\Omega((\tau_r/n)^{0.19})$ peaking layers, while $\tau_p = \tau_r$ layers suffice. Our numerical results strongly indicate that nontrivial peakedness is possible with fewer peaking layers, but we do not yet understand this. Indeed, we do not know what sort of structure in the states output by random quantum circuits could make such results possible: we leave this as a mystery.

A second open problem is how to generate these sorts of circuits efficiently. Our numerical study was limited by the infamous barren plateau issue: that is, exponentially vanishing gradient values with n [MBS+18]. To increase numerical stability, we ran batches of independent optimizations with random initializations for each RQC instance and took the best result from the batch. We

also attempted sequential optimization, as used in [HGPC21, ZJN$^+$22, ZJR$^+$24], but it showed no significant improvement. As we are optimizing a global function, the barren plateau issue shows up even at a constant depth and is particularly hard to mitigate [CSV$^+$21]. If we understood what sort of structure our circuits were exploiting, perhaps a completely different approach to generating such circuits would suggest itself, not reliant on gradient descent or other optimization heuristics.

A final open problem is what *other* ensembles of peaked quantum circuits might be possible. For example, what are the possibilities for obfuscating the identity transformation? A few obfuscation protocols exist but are generally hard to implement on a NISQ device [AF16, BKNY23]. Here, if we set $\tau_p \gg \tau_r$, we are guaranteed to have many different implementations of the identity; are any of them indistinguishable from random?

5   Acknowledgments

References

[AA11]   Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[AA13]   Scott Aaronson and Alex Arkhipov. Bosonsampling is far from uniform. *arXiv preprint arXiv:1309.7460*, 2013.

[AAB⁺19]   Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando Brandao, David Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, and John Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 10 2019.

[AC16]   Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*, 2016.

[AE07]   Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 129–140. IEEE, 2007.

[AF16]   Gorjan Alagic and Bill Fefferman. On quantum obfuscation. *arXiv preprint arXiv:1602.01771*, 2016.

[BCG20]   Boaz Barak, Chi-Ning Chou, and Xun Gao. Spoofing linear cross-entropy benchmarking in shallow quantum circuits. *arXiv preprint arXiv:2005.02421*, 2020.

[BCHJ⁺21] Fernando GSL Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. Models of quantum complexity growth. *PRX Quantum*, 2(3):030316, 2021.

[BCJ23]   Michael J Bremner, Bin Cheng, and Zhengfeng Ji. Iqp sampling and verifiable quantum advantage: Stabilizer scheme and classical security. *arXiv preprint arXiv:2308.07152*, 2023.

[BCM⁺21]   Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(5):1–47, 2021.

[BEG⁺24]   Dolev Bluvstein, Simon J Evered, Alexandra A Geim, Sophie H Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, Madelyn Cain, Marcin Kalinowski, Dominik Hangleiter, et al. Logical quantum processor based on reconfigurable atom arrays. *Nature*, 626(7997):58–65, 2024.

[BFNV18]   Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. Quantum supremacy and the complexity of random circuit sampling. *arXiv preprint arXiv:1803.04402*, 2018.

[BHH16]   Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346:397–434, 2016.

[BKNY23]   James Bartusek, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Obfuscation of pseudo-deterministic quantum circuits. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1567–1578, 2023.

[BMS17]   Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1:8, 2017.

[CGW13]   Andrew M Childs, David Gosset, and Zak Webb. Universal computation by multi-particle quantum walk. *Science*, 339(6121):791–794, 2013.

[CSV$^+$21]   Marco Cerezo, Akira Sone, Tyler Volkoff, Lukasz Cincio, and Patrick J Coles. Cost function dependent barren plateaus in shallow parametrized quantum circuits. *Nature communications*, 12(1):1–12, 2021.

[CvdW22]   Julien Codsi and John van de Wetering. Classically simulating quantum supremacy iqp circuits trough a random graph approach. *arXiv preprint arXiv:2212.08609*, 2022.

[DCEL09]   Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):012304, 2009.

[DHJB21]   Alexander M Dalzell, Nicholas Hunter-Jones, and Fernando GSL Brandão. Random quantum circuits transform local noise into global white noise. *arXiv preprint arXiv:2111.14907*, 2021.

[DHJB22]   Alexander M Dalzell, Nicholas Hunter-Jones, and Fernando GSL Brandao. Random quantum circuits anticoncentrate in log depth. *PRX Quantum*, 3(1):010333, 2022.

[FGG14]   Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[FH16]   Edward Farhi and Aram W Harrow. Quantum supremacy through the quantum approximate optimization algorithm. *arXiv preprint arXiv:1602.07674*, 2016.

[GAE07]   David Gross, Koenraad Audenaert, and Jens Eisert. Evenly distributed unitaries: On the structure of unitary designs. *Journal of mathematical physics*, 48(5), 2007.

[GEBM19]   Harper R Grimsley, Sophia E Economou, Edwin Barnes, and Nicholas J Mayhall. An adaptive variational algorithm for exact molecular simulations on a quantum computer. *Nature communications*, 10(1):3007, 2019.

[GKC$^+$21]   Xun Gao, Marcin Kalinowski, Chi-Ning Chou, Mikhail D Lukin, Boaz Barak, and Soonwon Choi. Limitations of linear cross-entropy as a measure for quantum advantage. *arXiv preprint arXiv:2112.01657*, 2021.

[Gra18]   Johnnie Gray. quimb: a python library for quantum information and many-body calculations. *Journal of Open Source Software*, 3(29):819, 2018.

[Haf22]   Jonas Haferkamp. Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$. *Quantum*, 6:795, September 2022.

[HBVSE18] Dominik Hangleiter, Juan Bermejo-Vega, Martin Schwarz, and Jens Eisert. Anticoncentration theorems for schemes showing a quantum speedup. *Quantum*, 2:65, 2018.

[HGPC21]   Reza Haghshenas, Johnnie Gray, Andrew C. Potter, and Garnet Kin-Lic Chan. The variational power of quantum circuit tensor networks, 2021.

[HHB+20]   Jonas Haferkamp, Dominik Hangleiter, Adam Bouland, Bill Fefferman, Jens Eisert, and Juani Bermejo-Vega. Closing gaps of a quantum advantage with short-time hamiltonian dynamics. *Physical Review Letters*, 125(25):250501, 2020.

[HJ19]   Nicholas Hunter-Jones. Unitary designs from statistical mechanics in random quantum circuits. *arXiv preprint arXiv:1905.12053*, 2019.

[HZN+20]   Cupjin Huang, Fang Zhang, Michael Newman, Junjie Cai, Xun Gao, Zhengxiong Tian, Junyin Wu, Haihong Xu, Huanjun Yu, Bo Yuan, et al. Classical simulation of quantum supremacy circuits. *arXiv preprint arXiv:2005.06787*, 2020.

[KB14]   Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

[KM19]   Gregory D Kahanamoku-Meyer. Forging quantum data: classically defeating an iqp-based quantum test. *arXiv preprint arXiv:1912.05547*, 2019.

[KMCVY22]   Gregory D Kahanamoku-Meyer, Soonwon Choi, Umesh V Vazirani, and Norman Y Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 18(8):918–924, 2022.

[KMT+17]   Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *nature*, 549(7671):242–246, 2017.

[LTBM08]   Arul Lakshminarayan, Steven Tomsovic, Oriol Bohigas, and Satya N Majumdar. Extreme statistics of complex random and quantum chaotic states. *Physical review letters*, 100(4):044103, 2008.

[LZL+23]   Zimu Li, Han Zheng, Junyu Liu, Liang Jiang, and Zi-Wen Liu. Designs from local random quantum circuits with su (d) symmetry. *arXiv preprint arXiv:2309.08155*, 2023.

[MBS+18]   Jarrod R McClean, Sergio Boixo, Vadim N Smelyanskiy, Ryan Babbush, and Hartmut Neven. Barren plateaus in quantum neural network training landscapes. *Nature communications*, 9(1):4812, 2018.

[MBT+24]   Dmitri Maslov, Sergey Bravyi, Felix Tripier, Andrii Maksymov, and Joe Latone. Fast classical simulation of harvard/quera iqp circuits. *arXiv preprint arXiv:2402.03211*, 2024.

[MHJ23]   Shivan Mittal and Nicholas Hunter-Jones. Local random quantum circuits form approximate designs on arbitrary architectures. *arXiv preprint arXiv:2310.19355*, 2023.

[MLA+22]   Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[Mov18]   Ramis Movassagh. Efficient unitary paths and quantum computational supremacy: A proof of average-case hardness of random circuit sampling. *arXiv preprint arXiv:1810.04681*, 2018.

[MP67]   V A Marčenko and L A Pastur. Distribution of eigenvalues for some sets of random matrices. *Mathematics of the USSR-Sbornik*, 1(4):457, apr 1967.

[Nie05]   Michael A Nielsen. A geometric approach to quantum circuit lower bounds. *arXiv preprint quant-ph/0502070*, 2005.

[NJF20]   Kyungjoo Noh, Liang Jiang, and Bill Fefferman. Efficient classical simulation of noisy random quantum circuits in one dimension. *Quantum*, 4:318, 2020.

[OJF23]   Changhun Oh, Liang Jiang, and Bill Fefferman. Spoofing cross-entropy measure in boson sampling. *Physical Review Letters*, 131(1):010401, 2023.

[PCZ22]   Feng Pan, Keyang Chen, and Pan Zhang. Solving the sampling problem of the sycamore quantum circuits. *Physical Review Letters*, 129(9):090502, 2022.

[PGM+19]   Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-performance deep learning library. *Advances in neural information processing systems*, 32, 2019.

[PMS+14]   Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik, and Jeremy L O'brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1):4213, 2014.

[Pre12]   John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012.

[Pre18]   John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[RWL24]   Joel Rajakumar, James D Watson, and Yi-Kai Liu. Polynomial-time classical simulation of noisy iqp circuits with constant depth. *arXiv preprint arXiv:2403.14607*, 2024.

[SB09]   Dan Shepherd and Michael J Bremner. Temporally unstructured quantum computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 465(2105):1413–1439, 2009.

[Sho94]   Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[TW94]   Craig A Tracy and Harold Widom. Level-spacing distributions and the airy kernel. *Communications in Mathematical Physics*, 159:151–174, 1994.

[YZ22]   Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 69–74. IEEE, 2022.

[ZCC+22]   Qingling Zhu, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, Ming Gong, et al. Quantum computational advantage via 60-qubit 24-cycle random circuit sampling. *Science bulletin*, 67(3):240–245, 2022.

[ZJN+22]   Yuxuan Zhang, Shahin Jahanbani, Daoheng Niu, Reza Haghshenas, and Andrew C Potter. Qubit-efficient simulation of thermal states with quantum tensor networks. *Physical Review B*, 106(16):165126, 2022.

[ZJR+24]   Yuxuan Zhang, Shahin Jahanbani, Ameya Riswadkar, S Shankar, and Andrew C Potter. Sequential quantum simulation of spin chains with a single circuit qed device. *Physical Review A*, 109(2):022606, 2024.

[Žni06]   Marko Žnidarič. Entanglement of random vectors. *Journal of Physics A: Mathematical and Theoretical*, 40(3):F105, 2006.

[ZWC+20]   Leo Zhou, Sheng-Tao Wang, Soonwon Choi, Hannes Pichler, and Mikhail D Lukin. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *Physical Review X*, 10(2):021067, 2020.

[ZWD+20]   Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[ZZP21]   Yuxuan Zhang, Ruizhe Zhang, and Andrew C Potter. Qed driven qaoa for network-flow optimization. *Quantum*, 5:510, 2021.

A   Improved average peak weight of a two-layer RQC from a single layer quantum circuit

In this appendix, we consider $\tau_r = 2$ and $\tau_p = 1$. We show that, given the two random layers, there exists a peaking circuit that on average polynomially increases the peak weight compared with a $\tau_r - \tau_p = 1$-layer RQC.

Assume without loss of generality that n is even. Call the first and second random layers R_1 and R_2 respectively, and call the peaking layer P. Observe that the output state, after we apply R_1 to the initial state $|0^n\rangle$, can be written as

$$R_1 |0^n\rangle = \prod_i^{n/2} (\alpha_i |\psi_i^0\rangle |\psi_{i+1}^0\rangle + \beta_i |\psi_i^1\rangle |\psi_{i+1}^1\rangle) = \prod_i^{n/2} U_{2i} U_{2i+1}(\alpha_i |00\rangle + \beta_i |11\rangle)$$

Here we have written the state as a product of 2-local states in their Schmidt decomposed form (assuming $|\alpha_i| > |\beta_i|$), where $\{|\psi_i^0\rangle, |\psi_i^1\rangle\}$ is some local orthonormal basis on the i-th qubit. We claim:

Theorem A.1. *For any choice of $R_2 R_1$, there exists a single-layer circuit P, such that the output state $P R_2 R_1 |0^n\rangle$ has polynomially higher average peak weight than $R_1 |0^n\rangle$.*

Proof. We choose

$$P := \prod_i^{n/2} U_{2i}^\dagger U_{2i+1}^\dagger R_2^{-1}.$$

First, we calculate the average peak weight of $R_1 |0^n\rangle$ over the Haar ensemble. We notice that the resulting state is simply a tensor product of 2-qubit Haar random states, whose distribution after measurement follows the famous Porter-Thomas distribution. The quantity that interests us is

$$\int dU \ \text{Max}|U_{0,i}|^2,$$

which can be calculated using random matrix theory [LTBM08] to be $\frac{1}{d} \sum_i^d \frac{1}{d}$. For $d = 2^2 = 4$, this means the average peak weight for a 2-qubit Haar random state is $\frac{25}{48}$. Putting everything together, the average peak weight generated by single random layer is $R_1 |0^n\rangle$ is $(\frac{25}{48})^{n/2}$.

On the other hand, the resulting state after the peaking circuit is

$$P R_2 R_1 |0^n\rangle = \prod_i^{n/2} (\alpha_i |00\rangle + \beta_i |11\rangle).$$

To calculate the average peak weight, we just need to know the expectation of the highest Schmidt weight α_i. For Haar random quantum states, the entanglement spectrum is known to follow the Marchenko-Pastur distribution [MP67]; meanwhile, the distribution of the largest eigenvalue has been calculated [TW94, Žni06]. In particular, for two-qubit random states, $\mathbb{E}[|\alpha_i|^2] = 7/8$. This means that the output state of $P R_2 R_1 |0^n\rangle$ has an average peak weight of $(\frac{7}{8})^{n/2}$. $\qquad\square$