Low-Stabilizer-Complexity Quantum States Are Not Pseudorandom

Sabee Grewal
The University of Texas at Austin, TX, USA

Vishnu Iyer
The University of Texas at Austin, TX, USA

William Kretschmer
The University of Texas at Austin, TX, USA

Daniel Liang
The University of Texas at Austin, TX, USA

Abstract

We show that quantum states with "low stabilizer complexity" can be efficiently distinguished from Haar-random. Specifically, given an n-qubit pure state $|\psi\rangle$, we give an efficient algorithm that distinguishes whether $|\psi\rangle$ is (i) Haar-random or (ii) a state with stabilizer fidelity at least $\frac{1}{k}$ (i.e., has fidelity at least $\frac{1}{k}$ with some stabilizer state), promised that one of these is the case. With black-box access to $|\psi\rangle$, our algorithm uses $O\big(k^{12}\log(1/\delta)\big)$ copies of $|\psi\rangle$ and $O\big(nk^{12}\log(1/\delta)\big)$ time to succeed with probability at least $1-\delta$, and, with access to a state preparation unitary for $|\psi\rangle$ (and its inverse), $O\big(k^{3}\log(1/\delta)\big)$ queries and $O\big(nk^{3}\log(1/\delta)\big)$ time suffice.

As a corollary, we prove that $\omega(\log(n))$ T-gates are necessary for any Clifford+T circuit to prepare computationally pseudorandom quantum states, a first-of-its-kind lower bound.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases Pseudorandom quantum states, Clifford + T, Haar random, Bell sampling, stabilizer formalism, stabilizer extent, stabilizer fidelity, learning theory, complexity theory

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.64

Related Version *Full Version*: `https://arxiv.org/abs/2209.14530`

Funding SG, VI, DL are supported by Scott Aaronson's Vannevar Bush Fellowship from the US Department of Defense, the Berkeley NSF-QLCI CIQC Center, a Simons Investigator Award, and the Simons "It from Qubit" collaboration.
William Kretschmer: Supported by an NDSEG Fellowship.

Acknowledgements We thank Scott Aaronson for helpful comments.

1 Introduction

The stabilizer formalism [11] plays a central role in quantum information. Stabilizer states are states that lie in the intersection of the positive eigenspaces of 2^n commuting Pauli operators. Stabilizer states can be generated by Clifford circuits, which are the group of unitary transformations that normalize the Pauli group. Stabilizer states and the Clifford group have widespread applications in quantum error correction [28, 8], measurement-based quantum computation [27], randomized benchmarking [19], and quantum learning algorithms [16]. These applications are largely thanks to the rich algebraic structure afforded by the stabilizer formalism.

Stabilizer states are also one of the few classes of states that admit efficient learning algorithms. Montanaro [22] gave an algorithm that takes $O(n)$ copies of an n-qubit stabilizer state and correctly identifies the state with high probability in time $O(n^3)$. Gross, Nezami,

14th Innovations in Theoretical Computer Science Conference (ITCS 2023).
Editor: Yael Tauman Kalai; Article No. 64; pp. 64:1–64:20
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

and Walter [13] gave an algorithm for *property testing* stabilizer states, which is the task of distinguishing whether a state is a stabilizer state or is far from any stabilizer state. Remarkably, this algorithm requires only 6 copes of the state.

Despite finding numerous applications, Clifford circuits are not universal for quantum computation. Furthermore, in 1998, Gottesman and Knill showed that Clifford circuits acting on stabilizer states can be efficiently classically simulated [12, 1]. However, with the additional ability to apply a T-gate (the gate $|0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$), the resulting gate set becomes universal. Therefore, efficient simulation of so-called Clifford+T circuits would imply $\mathsf{BPP} = \mathsf{BQP}$, and a large line of work has been devoted to developing better simulation algorithms [25, 7, 26, 6].

Currently, the best-performing simulation algorithms are based on modeling the output state of a quantum circuit as a decomposition of stabilizer states [6]. These decompositions give rise to simulation algorithms whose runtimes scale polynomially in the complexity of the decomposition. One such complexity measure is the *stabilizer extent.* Consider the state $|\psi\rangle = \sum_i c_i |\phi_i\rangle$ for $c_i \in \mathbb{C}$ and stabilizer states $|\phi_i\rangle$. The stabilizer extent is the minimum $\left(\sum_i |c_i|\right)^2$ over all such decompositions of $|\psi\rangle$, and scales exponentially in the number of T-gates in the circuit producing the state. A closely-related complexity measure is the *stabilizer fidelity*, which is the maximum overlap between $|\psi\rangle$ and any stabilizer state. Indeed, the inverse of stabilizer fidelity lower bounds stabilizer extent [6]. Collectively, we informally refer to states with either low stabilizer extent or non-negligible stabilizer fidelity as states of low "stabilizer complexity".

As a generalization of stabilizer states, it is natural to ask whether states of low stabilizer complexity are also efficiently learnable, and indeed a similar question has been raised before [2]. Nevertheless, this problem remains largely open except in some highly restricted settings [21]. This could be in part because many of the useful properties of stabilizer states provably fail to generalize to states with low stabilizer complexity. For example, [15] observed that one can efficiently learn the output distribution of any Clifford circuit, given samples from this distribution.[1] However, this task already becomes intractable for circuits with a *single* T-gate (producing a state of constant stabilizer extent), where [15] proved that learning the output distribution is as hard as the learning parities with noise problem.

Furthermore, it is known that stabilizer states form a t-*design* for $t = 3$, meaning that random stabilizer states duplicate the first 3 moments of the Haar measure [20, 29]. By contrast, [14] showed that circuits with $\mathsf{poly}(t)$ non-Clifford gates are sufficient to generate approximate t-designs. Thus, for any constant t, states of constant stabilizer extent can form approximate t-designs. This suggests that states of low stabilizer complexity can give much stronger information-theoretic approximations to the Haar measure than ordinary stabilizer states, because stabilizer states fail to form a t-design for any $t > 3$ [30].

In this work, we investigate whether these properties that differentiate stabilizer states from low-stabilizer-complexity states can be pushed further, to prove hardness of learning low-stabilizer-complexity states. One natural approach towards proving that low-stabilizer-complexity states are hard to learn would be to show that they are *pseudorandom.* Ji, Liu, and Song [18] define an ensemble of n-qubit states to be (computationally) pseudorandom if every $\mathsf{poly}(n)$-time quantum adversary has at most a negligible advantage in distinguishing copies of a state drawn randomly from the ensemble from copies of a Haar-random n-qubit state. Note that pseudorandom states are not efficiently learnable, as any algorithm for learning some set of quantum states gives an algorithm to distinguish those states from the Haar measure.

[1] Indeed, every such distribution is simply an affine subspace of $\mathbb{F}_2^n$.

Our main result is an efficient algorithm for distinguishing states of non-negligible stabilizer fidelity from Haar-random states, showing that such states *cannot* be pseudorandom. This type of distinguishing is sometimes known as *weak learning* in learning theory.

▶ **Theorem 1** (Informal version of Theorem 23). *Let $|\psi\rangle$ be an unknown n-qubit pure state, and let $k \leq \frac{4}{5}2^{n/12}$. There is an efficient algorithm that distinguishes whether $|\psi\rangle$ is Haar-random or a state with stabilizer fidelity at least $\frac{1}{k}$, promised that one of these is the case. In particular, the algorithm uses $O(k^{12}\log(1/\delta))$ copies of $|\psi\rangle$ and $O(nk^{12}\log(1/\delta))$ time to succeed with probability at least $1-\delta$.*

Theorem 1 also generalizes to distinguishing states with low stabilizer extent from Haar-random. To the best of our knowledge, prior to our work, it was even unknown whether states of stabilizer extent at most a *constant* could be efficiently distinguished from Haar-random. We also emphasize that the contrast between our positive learning result and the hardness result of [15] stems in part from the differing access models: we assume access to copies of the quantum state, whereas [15] considers algorithms that only have outcomes of standard basis measurements of the state.

As a simple corollary, we prove a first-of-its-kind lower bound on the number of T-gates required to prepare computationally pseudorandom quantum states.

▶ **Corollary 2** (Corollary 25). *Any family of Clifford+T circuits that produces an ensemble of n-qubit computationally pseudorandom quantum states must use at least $\omega(\log n)$ T-gates.*

In some sense, Corollary 2 contrasts sharply with the result of [14], where circuits containing just a few non-Clifford gates are sufficient to produce strong information-theoretic approximations to the Haar measure (i.e. t-designs). Nevertheless, we emphasize that our result and [14] are formally incomparable, because computationally pseudorandom states need not form approximate t-designs for constant t, nor vice-versa.

1.1 Main Ideas

Let $x = (p, q) \in \mathbb{F}_2^{2n}$, where p and q are the first and last n bits of x, respectively. Define $W_x := i^{p\cdot q}X^pZ^q$ (a Pauli operator without phase), and let $|\Phi^+\rangle := 2^{-n/2}\sum_{x\in\mathbb{F}_2^n}|x,x\rangle$ be a maximimally entangled state. Then, the set $\{|W_x\rangle := (W_x \otimes I)|\Phi^+\rangle \mid x \in \mathbb{F}_2^{2n}\}$ is the *Bell basis*, an orthonormal basis of $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$.

Our algorithm uses *Bell difference sampling* [22, 13], which works as follows (see Section 2.3 for more detail): Given four copies of an n-qubit pure state $|\psi\rangle$, perform a Bell-basis measurement on $|\psi\rangle^{\otimes 2}$ to get measurement outcome $x \in \mathbb{F}_2^{2n}$, repeat this on the remaining two copies to get measurement outcome $y \in \mathbb{F}_2^{2n}$, and return $z = x + y$.

We refer to $p_\psi(x) := 2^{-n}|\langle\psi|W_x|\psi\rangle|^2$ as the *characteristic distribution of* $|\psi\rangle$. To see that p_ψ is a distribution, recall that since the Pauli operators form an orthonormal basis over Hermitian matrices, we can always decompose $|\psi\rangle\langle\psi| = \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\langle\psi|W_x|\psi\rangle \cdot W_x$. By assumption, $|\langle\psi|\psi\rangle|^2 = 1$, so by Parseval's identity,

$$\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}|\langle\psi|W_x|\psi\rangle|^2 = 1.$$

Gross, Nezami, and Walter [13] showed that Bell difference sampling an arbitrary pure state $|\psi\rangle$ corresponds to sampling a random operator W_x according to the following distribution:

$$q_\psi(x) = \sum_{y\in\mathbb{F}_2^{2n}} p_\psi(y)p_\psi(x+y).$$

We call q_ψ the *Weyl distribution of* $|\psi\rangle$. Note that the Weyl distribution of $|\psi\rangle$ is the scaled convolution of the characteristic distribution with itself (i.e., $q_\psi = 4^n(p_\psi * p_\psi)$, where "$*$" is the convolution operator).

Define the $\{\pm 1\}$-outcome measurement $M_x := \left\{\frac{I \pm W_x}{2}\right\}$ (projections onto the ± 1-eigenspaces of W_x). Our algorithm begins by repeating the following process m times: sample a random Weyl operator W_x (via Bell difference sampling) and perform the measurement $M_x^{\otimes 2}$ on $|\psi^{\otimes 2}\rangle$. Then, average all of the measurement outcomes. If the average is at least $1/\mathsf{poly}(k)$, we decide that $|\psi\rangle$ has stabilizer fidelity at least $\frac{1}{k}$. Otherwise, we decide that $|\psi\rangle$ is Haar-random.

What statistic are we computing in our algorithm? Denote the measurement outcome on the ith iteration as $X_i \in \{\pm 1\}$. Observe that for all X_i,

$$\mathbf{E}[X_i] = \sum_{x \in \mathbb{F}_2^{2n}} q_\psi(x) |\langle\psi|W_x|\psi\rangle|^2 = 2^n \sum_{x \in \mathbb{F}_2^{2n}} q_\psi(x) p_\psi(x) = 2^n \mathop{\mathbf{E}}_{x \sim q_\psi}[p_\psi(x)],$$

where the expectation $\mathbf{E}[X_i]$ is taken over sampling $x \sim q_\psi$ and the randomness from performing the measurement $M_x^{\otimes 2}$. Hence, for our algorithm to work, $\mathbf{E}_{x \sim q_\psi}[p_\psi(x)]$ must be "different enough" when $|\psi\rangle$ either is Haar-random or has low stabilizer complexity. Proving that this is the case is the main technical ingredient of our work:

▶ **Lemma 3** (Informal version of Lemma 15). *Let $|\psi\rangle$ be an n-qubit pure state. Suppose the stabilizer fidelity of $|\psi\rangle$ is at least $\frac{1}{k}$. Then,*

$$2^n \mathop{\boldsymbol{E}}_{x \sim q_\psi}[p_\psi(x)] \geq \frac{1}{k^6}.$$

In contrast, suppose $|\psi\rangle$ is a Haar-random quantum state. Then, with overwhelming probability over the Haar measure,

$$2^n \mathop{\boldsymbol{E}}_{x \sim q_\psi}[p_\psi(x)] \leq 2^{-n/2}.$$

Our proof uses Fourier analysis of Boolean functions, and some parts of our proof are reminiscent of the celebrated Blum-Luby-Rubinfield linearity test [3]. Intuitively, q_ψ is significantly closer to linear when $|\psi\rangle$ has non-negligible stabilizer fidelity, as opposed to when $|\psi\rangle$ is a Haar-random state.

With the above lemma, all that remains is "merely" a sample complexity analysis, namely: what m is sufficient to distinguish whether the average is close to 0 or $\Omega(1/k^6)$? In the simplest case, we show that $O(k^{12} \log(1/\delta))$ samples are sufficient by Hoeffding's inequality. However, this complexity can be improved if given access to a unitary that prepares $|\psi\rangle$ (and its inverse). In this model, we are able to achieve a quartic speedup in both sample and time complexity, which we explain in Appendix A.

2 Preliminaries

First, we establish some notation used throughout this work. We denote $[n] := \{1, \ldots, n\}$. For $v \in \mathbb{C}^n$, $\|v\|_p := (\sum_{i \in [n]} |v_i|^p)^{1/p}$ is the ℓ_p-norm. Logarithms are assumed to be in base 2. For a probability distribution P on a set S, we denote drawing a sample $s \in S$ according to P by $s \sim P$. We denote drawing a sample $s \in S$ uniformly at random by $s \sim S$.

2.1 Stabilizer States and Stabilizer Complexity Measures

We define the 1-qubit Pauli group to be the collection of matrices $\{I, X, Y, Z\}$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The n-qubit Pauli group $\mathcal{P}_n$ is the set $\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$. The Clifford group $\mathcal{C}_n$ is the group of unitary transformations generated by H, S, and CNOT gates, where H is the Hadamard gate, $S \coloneqq |0\rangle\langle 0| + i\,|1\rangle\langle 1|$ is the phase gate, and CNOT is the controlled-not gate. We refer to unitary transformations in the Clifford group as Clifford circuits. Clifford circuits with the addition of the T-gate are universal, where the T-gate is defined by $T \coloneqq |0\rangle\langle 0| + e^{i\pi/4}\,|1\rangle\langle 1|$.

A unitary transformation U *stabilizes* a state $|\psi\rangle$ when $U\,|\psi\rangle = |\psi\rangle$. It is folklore that if an n-qubit state can be reached from the $|0^n\rangle$ state by applying a Clifford circuit, then the state is stabilized by a group of 2^n commuting members of the subset $\{\pm 1\} \times \{I, X, Y, Z\}^{\otimes n} \subset (\mathcal{P}_n \setminus -I^{\otimes n})$, called its *stabilizer group*. Such states are called *stabilizer states*, and we denote the set of stabilizer states by $\mathcal{S}_n$. For $|\psi\rangle \in \mathcal{S}_n$, we denote its stabilizer group as $\mathrm{Stab}(|\psi\rangle)$. For more background on stabilizer states, see, e.g., [23].

We now define some complexity measures that characterize more general states in terms of stabilizer state decompositions.

▶ **Definition 4** (stabilizer extent [6]). *Suppose $|\psi\rangle$ is a pure n-qubit state. The* stabilizer extent *of $|\psi\rangle$, denoted $\xi(|\psi\rangle)$, is the minimum of $\|c\|_1^2$ over all decompositions $|\psi\rangle = \sum_i c_i\,|\phi_i\rangle$, where $|\phi_i\rangle \in \mathcal{S}_n$ and c is some vector in $\mathbb{C}^{|\mathcal{S}_n|}$.*

▶ **Definition 5** (stabilizer fidelity [6]). *Suppose $|\psi\rangle$ is a pure n-qubit state. The* stabilizer fidelity *of $|\psi\rangle$, denoted $F_{\mathcal{S}}$, is*

$$F_{\mathcal{S}}(|\psi\rangle) \coloneqq \max_{|\phi\rangle \in \mathcal{S}_n} |\langle \phi|\psi\rangle|^2 .$$

Below we give a useful relation between the complexity measures defined above.

▷ Claim 6. Let $|\psi\rangle$ be an n-qubit pure state. Then,

$$\xi(|\psi\rangle) \geq \frac{1}{F_{\mathcal{S}}(|\psi\rangle)}.$$

Proof. Let $|\psi\rangle = \sum_{|\phi\rangle \in \mathcal{S}_n} c_\phi\,|\phi\rangle$ be such that $\left(\sum_\phi |c_\phi|\right)^2 = \xi(|\psi\rangle)$. Suppose towards a contradiction that $F_{\mathcal{S}}(|\psi\rangle) < \frac{1}{\xi(|\psi\rangle)}$ and therefore $|\langle\phi|\psi\rangle| < \frac{1}{\xi(|\psi\rangle)}$ for all $|\phi\rangle \in \mathcal{S}_n$. Then,

$$\begin{aligned} 1 = |\langle\psi|\psi\rangle| = \left| \sum_{|\phi\rangle \in \mathcal{S}_n} c_\phi^*\,\langle\phi|\psi\rangle \right| &\leq \sum_{|\phi\rangle \in \mathcal{S}_n} |c_\phi|\,|\langle\phi|\psi\rangle| \\ &\leq \max_i |\langle\phi_i|\psi\rangle| \sum_{|\phi\rangle \in \mathcal{S}_n} |c_\phi| \\ &\leq \sqrt{F_{\mathcal{S}}(|\psi\rangle)\xi(|\psi\rangle)} \\ &< 1, \end{aligned}$$

which is a clear contradiction. ◁

The claim above also follows as a special case of [6, Theorem 4], though its proof is more complicated.

To prove lower bounds on the number of T-gates necessary to prepare pseudorandom quantum states, we need to upper bound the stabilizer extent of a quantum state prepared by a Clifford+T circuit comprised of t T-gates.

▷ Claim 7. For $|\psi\rangle = \alpha |v\rangle + \beta |w\rangle$,

$$\xi(|\psi\rangle) \leq \left(|\alpha|\sqrt{\xi(|v\rangle)} + |\beta|\sqrt{\xi(|w\rangle)}\right)^2.$$

Proof. Let $|v\rangle = \sum_i c_i |\phi_i\rangle$ and $|w\rangle = \sum_j d_j |\varphi_j\rangle$ be the minimal decompositions in terms of stabilizer extent (i.e., $\left(\sum_i |c_i|\right)^2 = \xi(|v\rangle)$). Since $|\psi\rangle = \alpha |v\rangle + \beta |w\rangle = \alpha \sum_i c |\phi_i\rangle + \beta \sum_j d |\varphi_j\rangle$, we have a stabilizer decomposition of $|\psi\rangle$. The stabilizer extent of this decomposition is at most

$$\left(\sum_i |\alpha c_i + \beta d_i|\right)^2 \leq \left(|\alpha| \sum_i |c_i| + |\beta| \sum_i |d_i|\right)^2 = \left(|\alpha|\sqrt{\xi(v)} + |\beta|\sqrt{\xi(w)}\right)^2. \qquad ◁$$

▶ **Lemma 8.** *Let C be any Clifford+T circuit comprised of t T-gates and $|\psi\rangle = C|0^n\rangle$. Then,*

$$\xi(|\psi\rangle) \leq \left(1 + \frac{1}{\sqrt{2}}\right)^t.$$

Proof. We note that a Clifford+T circuit can be broken into layers of Clifford circuits, followed by a single T-gate, followed by more layers of Clifford circuits, and so on. Since Clifford circuits preserve stabilizer extent, we only need to show that the T-gate increases the stabilizer extent of any state by at most a constant multiplicative factor. Since the SWAP gate is a Clifford operation, we assume without loss of generality that each T-gate is applied to the first qubit.

We proceed by induction on the layers of the circuit. In the first layer, when no T-gates have been applied, the bound is trivially true because the stabilizer extent of any stabilizer state is 1. Now, assume that, after applying some portion of the circuit C' to $|0^n\rangle$ with $t-1$ T-gates, we get the state $|\varphi\rangle$. Observe that the T-gate can be expressed as $\cos(\pi/8)e^{i\pi/8}I + \sin(\pi/8)e^{i13\pi/8}Z$. Thus, $(T \otimes I^{\otimes n-1})|\varphi\rangle = \cos(\pi/8)e^{i\pi/8}|\varphi\rangle + \sin(\pi/8)e^{i13\pi/8}\left(Z \otimes I^{\otimes n-1}\right)|\varphi\rangle$. Since $Z \otimes I^{\otimes n-1}$ is a Clifford operation, $\left(Z \otimes I^{\otimes n-1}\right)|\varphi\rangle$ has the same extent as $|\varphi\rangle$. Therefore, applying Claim 7,

$$\xi(|\psi\rangle) \leq (\cos(\pi/8) + \sin(\pi/8))^2 \, \xi(|\varphi\rangle) \leq \left(1 + \frac{1}{\sqrt{2}}\right)^t. \qquad ◀$$

2.2 Boolean Fourier Analysis

We review the basics of Fourier analysis over the Boolean hypercube.

▶ **Definition 9.** *Let $S \subseteq [n]$ be an index of bits. Then the* parity function *on S is defined to be*

$$\chi_S(x) := \prod_{i \in S} (-1)^{x_i}.$$

Alternatively, we can define $\chi_S(x) = (-1)^{x \cdot s}$ where $s_i = 1$ if and only if $i \in S$. This form will prove to be more natural for our purposes.

The parity functions are orthonormal under the inner product $\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)g(x)$. Since there are 2^n distinct parity functions, this gives a complete basis. Given a function $f : \mathbb{F}_2^n \to \mathbb{R}$, we can then write

$$f(x) = \sum_{S \subseteq [n]} \widehat{f}(S)\chi_S(x).$$

The $\widehat{f}(S)$ are real numbers known as the *Fourier coefficients* (collectively known as the *Fourier spectrum*), and are equivalently given by the formula

$$\widehat{f}(S) = \langle f(x), \chi_S(x) \rangle.$$

As a basis change, we can then rethink inner products to be over the Fourier coefficients as well.

▶ **Fact 10** (Plancherel's theorem).

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{S \subseteq [n]} \widehat{f}(S)\widehat{g}(S).$$

Finally, the convolution is an operation that appears frequently in Fourier analysis over the reals. We can similarly define it over Boolean inputs.

▶ **Definition 11.** *For functions $f, g : \mathbb{F}_2^n \to \mathbb{R}$, we define the* convolution *$f * g$ as*

$$(f * g)(x) := \frac{1}{2^n} \sum_{t \in \mathbb{F}_2^n} f(t)g(x + t).$$

Much like Fourier transforms over the reals, convolution maps to multiplication in the Fourier domain.

▶ **Fact 12** (Convolution theorem). $\widehat{f * g}(S) = \widehat{f}(S)\widehat{g}(S)$

For proofs of all of these facts, as well as for a comprehensive reference on analysis of Boolean functions, we recommend [24].

2.3 Weyl Operators and Bell Difference Sampling

For $x = (p, q) \in \mathbb{F}_2^{2n}$, define the *Weyl operator* as

$$W_x := i^{p \cdot q}(X^{p_1}Z^{q_1}) \otimes \ldots \otimes (X^{p_n}Z^{q_n}) = i^{p \cdot q}X^p Z^q.$$

Each Weyl operator is a Pauli operator, and every Pauli operator is a Weyl operator (up to a phase). Note also that $W_x W_y = W_{x+y}$, up to a phase. We use Weyl operators (rather than Pauli operators) when it is convenient to identify members of the Pauli group with length-$2n$ bit strings.

A critical subroutine in our work is *Bell difference sampling*, which was introduced in [22, 13]. Let $|\Phi^+\rangle := 2^{-n/2} \sum_{x \in \mathbb{F}_2^n} |x, x\rangle$. Then, the set of quantum states $\{|W_x\rangle := (W_x \otimes I)|\Phi^+\rangle \mid x \in \mathbb{F}_2^{2n}\}$ forms an orthonormal basis of $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$, which we call the *Bell basis*. Bell sampling a state $|\psi\rangle$ refers to measuring $|\psi\rangle^{\otimes 2}$ in the Bell basis, and the measurement outcome is a length-$2n$ bit string x that corresponds to a Weyl operator W_x.

Bell difference sampling a state $|\psi\rangle$ refers to Bell sampling twice to get measurement outcomes $x, y \in \mathbb{F}_2^{2n}$ and returning $z = x + y$, which corresponds to a Weyl operator W_z and uses four copies of $|\psi\rangle$. Montanaro showed Bell difference sampling can be performed in $O(n)$ time [22].

Bell difference sampling returns a random Weyl operator, but according to what distribution? Gross, Nezami, and Walter [13] showed that the underlying distribution depends on the so-called characteristic distribution of $|\psi\rangle$.

▶ **Definition 13** (characteristic distribution). *The* characteristic distribution *of $|\psi\rangle$ is defined as*

$$p_\psi(x) := 2^{-n}|\langle\psi|W_x|\psi\rangle|^2.$$

▶ **Lemma 14** ([13, Theorem 3.2]). *Let $|\psi\rangle$ be an arbitrary n-qubit pure state. Bell difference sampling corresponds to drawing a sample from the following distribution:*

$$q_\psi(x) := 4^n(p_\psi * p_\psi)(x) = \sum_{y \in \mathbb{F}_2^{2n}} p_\psi(y)p_\psi(x+y).$$

Additionally, if $|\psi\rangle \in \mathcal{S}_n$ is a stabilizer state, then

$$q_\psi(x) = p_\psi(x) = 2^{-n}|\langle\psi|W_x|\psi\rangle|^2.$$

We refer to q_ψ as the *Weyl distribution.* Using this terminology, the characteristic distribution and Weyl distribution are equal only when $|\psi\rangle$ is a stabilizer state (i.e., when $4^n(p_\psi * p_\psi) = p_\psi$).

3 Certificate of Low Stabilizer Complexity

To efficiently distinguish a state with low stabilizer complexity (meaning, a state with low stabilizer extent or non-negligible stabilizer fidelity) from a Haar-random one, we require a property or statistic of the state that distinguishes it from Haar-random. As such, we present the following technical lemma, which forms the backbone of our algorithm.

▶ **Lemma 15.** *Let $|\psi\rangle$ be an n-qubit pure state. If the stabilizer fidelity of $|\psi\rangle$ is at least $\frac{1}{k}$, then*

$$\mathop{\boldsymbol{E}}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \geq \frac{1}{k^6}.$$

In contrast, if $|\psi\rangle$ is Haar-random and $n \geq 33$, then, with probability at least $1 - \exp\left(-2^{n/2-15}\right)$ *over the Haar measure,*

$$\mathop{\boldsymbol{E}}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \leq 2^{-n/2}.$$

Our algorithm then amounts to estimating the quantity $\mathbf{E}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$ via a procedure involving Bell difference sampling.

To prove Lemma 15, as a first step, we relate $\mathbf{E}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$ to the Fourier coefficients of p_ψ. Note that this analysis closely resembles the BLR linearity test [3] (see also [24, Section 1.6]).

▶ **Fact 16.** *Let $|\psi\rangle$ be an n-qubit pure state. Then,*

$$\mathop{\boldsymbol{E}}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] = 32^n \sum_{x \in \mathbb{F}_2^{2n}} \widehat{p_\psi}(x)^3.$$

Proof.

$$\begin{aligned}
\mathop{\mathbf{E}}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] &= 2^n \mathop{\mathbf{E}}_{x\sim q_\psi}[p_\psi(x)] \\
&= 2^n \sum_{x\in\mathbb{F}_2^{2n}} p_\psi(x)q_\psi(x) \\
&= 8^n \sum_{x\in\mathbb{F}_2^{2n}} p_\psi(x)(p_\psi * p_\psi)(x) \\
&= 32^n \mathop{\mathbf{E}}_{x\sim\mathbb{F}_2^{2n}}[p_\psi(x)(p_\psi * p_\psi)(x)] \\
&= 32^n \sum_{x\in\mathbb{F}_2^{2n}} \widehat{p_\psi}(x)\widehat{p_\psi * p_\psi}(x)) && \text{(Fact 10)} \\
&= 32^n \sum_{x\in\mathbb{F}_2^{2n}} \widehat{p_\psi}(x)^3. && \text{(Fact 12)}
\end{aligned}$$

◀

For the remainder of this section, we use the following convention: when $x = (v, w) \in \mathbb{F}_2^{2n}$, v and w denote the first and last n bits of x, respectively, and, we will sometimes write $p_\psi(v, w)$ and $q_\psi(v, w)$, rather than $p_\psi(x)$ and $q_\psi(x)$.

3.1 The Fourier Spectrum of the Characteristic Distribution

By Fact 16, it is clear that understanding the Fourier spectrum of p_ψ is one avenue to proving Lemma 15.

▶ **Proposition 17.** *The Fourier coefficients of $p_\psi(v, w)$ are $\widehat{p_\psi}(v, w) = \frac{1}{2^n} p_\psi(w, v)$.*

Proof. Define $f : \mathbb{F}_2^{2n} \to [-1, 1]$ as $f(v, w) := \langle\psi|i^{v\cdot w}X^vZ^w|\psi\rangle$, where $v, w \in \mathbb{F}_2^n$. We begin by computing the Fourier expansion of f.

$$\begin{aligned}
f(v, w) &= \langle\psi|\, i^{v\cdot w}X^vZ^w\,|\psi\rangle \\
&= \left(\sum_{x\in\mathbb{F}_2^n} c_x^* \langle x|\right) i^{v\cdot w}X^vZ^w \left(\sum_{x\in\mathbb{F}_2^n} c_x |x\rangle\right) \\
&= i^{v\cdot w}\left(\sum_{x\in\mathbb{F}_2^n} c_x^* \langle x+v|\right)\left(\sum_{x\in\mathbb{F}_2^n} (-1)^{x\cdot w} c_x |x\rangle\right) \\
&= i^{v\cdot w}\sum_{x\in\mathbb{F}_2^n} c_{x+v}^* c_x (-1)^{w\cdot x}. \qquad (1)
\end{aligned}$$

In the second line we are simply writing $|\psi\rangle$ in the computational basis.

Observe now that $p_\psi(v, w) = \frac{1}{2^n}|f(v, w)|^2$, which we can also treat as a function on Boolean variables. Hence,

$$\begin{aligned}
p_\psi(v, w) &= \frac{1}{2^n}\left(i^{v\cdot w}\sum_{x\in\mathbb{F}_2^n} c_{x+v}^* c_x(-1)^{w\cdot x}\right)\left((-i)^{v\cdot w}\sum_{x\in\mathbb{F}_2^n} c_{x+v}c_x^*(-1)^{w\cdot x}\right) \\
&= \frac{1}{2^n}\sum_{x,y\in\mathbb{F}_2^n} c_{v+y}^* c_y c_{v+x+y} c_{x+y}^* (-1)^{w\cdot x},
\end{aligned}$$

where the first equality follows by substituting in Equation (1).

We can now compute the Fourier spectrum of p_ψ by taking the inner product between p_ψ and an arbitrary Fourier character (this is the simplest approach to computing Fourier coefficients).

$$\begin{aligned}
\widehat{p_\psi}(v,w) &= \frac{1}{4^n}\sum_{s,t\in\mathbb{F}_2^n} p_\psi(s,t)(-1)^{s\cdot v+t\cdot w}\\
&= \frac{1}{8^n}\sum_{s,t,x,y\in\mathbb{F}_2^n} c_{s+y}^* c_y c_{s+x+y} c_{x+y}^* (-1)^{t\cdot x+v\cdot s+w\cdot t}\\
&= \frac{1}{8^n}\sum_{s,x,y\in\mathbb{F}_2^n} c_{s+y}^* c_y c_{s+x+y} c_{x+y}^* (-1)^{v\cdot s}\sum_{t\in\mathbb{F}_2^n}(-1)^{t\cdot(x+w)}\\
&= \frac{1}{4^n}\sum_{s,y\in\mathbb{F}_2^n} c_{s+y}^* c_y c_{s+w+y} c_{w+y}^* (-1)^{v\cdot s}\\
&= \frac{1}{2^n} p_\psi(w,v).
\end{aligned}$$

◀

3.2 Low-Stabilizer-Complexity States

We prove the first part of Lemma 15; namely, that

$$\mathop{\mathbf{E}}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \geq \frac{1}{k^6}$$

when $|\psi\rangle$ has low stabilizer complexity.

▷ Claim 18. For an n-qubit pure state $|\psi\rangle = \sum_{x\in\mathbb{F}_2^n} c_x |x\rangle$,

$$32^n \sum_{x\in\mathbb{F}_2^{2n}} \widehat{p_\psi}(x)^3 \geq |c_0|^{12}.$$

Proof.

$$\begin{aligned}
32^n \sum_{v,w\in\mathbb{F}_2^{2n}} \widehat{p_\psi}(v,w)^3 &= 4^n \sum_{v,w\in\mathbb{F}_2^{2n}} p_\psi(w,v)^3 && \text{(Proposition 17.)}\\
&\geq 4^n \sum_{v\in\mathbb{F}_2^n} p_\psi(0,v)^3 && (\forall x,y, p_\psi(x,y)\geq 0.)\\
&= \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} |\langle\psi|Z^v|\psi\rangle|^6\\
&\geq \frac{1}{2^{6n}}\left(\sum_{v\in\mathbb{F}_2^n}\langle\psi|Z^v|\psi\rangle\right)^6 && \left(\sum_{i=1}^m |a_i|^6 \geq \frac{1}{m^5}\left(\sum_{i=1}^m |a_i|\right)^6.\right)\\
&\geq |c_0|^{12}. && \left(\sum_{v\in\mathbb{F}_2^n} Z^v = 2^n |0^n\rangle\langle 0^n|.\right)
\end{aligned}$$

◁

Proof of first part of Lemma 15. Let $|\psi\rangle$ be an n-qubit pure state, and suppose that the stabilizer fidelity of $|\psi\rangle$ is at least $\frac{1}{k}$. Then there exists a Clifford circuit $C\in\mathcal{C}_n$ such that $C|\psi\rangle = \sum_{x\in\mathbb{F}_2^n} c_x|x\rangle$ where $|c_0|^2\geq\frac{1}{k}$. Call $|\phi\rangle := C|\psi\rangle$. By Claim 18,

$$32^n \sum_{v,w\in\mathbb{F}_2^n} \widehat{p_\phi}(v,w)^3 \geq |c_0|^{12} \geq \frac{1}{k^6}.$$

A Clifford circuit C is a permutation of the Pauli group under conjugation (i.e., $C^\dagger \mathcal{P}_n C = \mathcal{P}_n$ for any $C \in \mathcal{C}_n$). Hence, for all $C \in \mathcal{C}_n$ and $g : \mathcal{P}_n \to \mathbb{R}$,

$$\sum_{x \in \mathbb{F}_2^{2n}} g(W_x) = \sum_{x \in \mathbb{F}_2^{2n}} g(C^\dagger W_x C).$$

Therefore, we conclude that

$$32^n \sum_{v,w \in \mathbb{F}_2^n} \widehat{p_\psi}(v,w)^3 \geq \frac{1}{k^6}$$

as well. Combining this bound with Fact 16 completes the proof. ◀

3.3 Haar-Random States

We complete the proof of Lemma 15 by showing that $\mathbf{E}_{x \sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$ is small when $|\psi\rangle$ is a Haar-random state. We begin by showing that, for a Haar-random state, all of the Weyl measurements (except $W_x = I$) are exponentially close to 0 with overwhelming probability.

▶ **Lemma 19** (Lévy's Lemma, see e.g. [10]). *Let $\mathbb{S}^N$ denote the set of all N-dimensional pure quantum states, and let $f : \mathbb{S}^N \to \mathbb{R}$ be L-Lipschitz, meaning that $|f(|\psi\rangle) - f(|\varphi\rangle)| \leq L \cdot \||\psi\rangle - |\varphi\rangle\|_2$. Then:*

$$\Pr_{|\psi\rangle \sim \mu_{\text{Haar}}}\left[|f(|\psi\rangle) - \boldsymbol{E}[f]| \geq \varepsilon\right] \leq 2\exp\left(-\frac{N\varepsilon^2}{9\pi^3 L^2}\right).$$

▶ **Lemma 20.** *For any n-qubit Weyl operator W_x, the function $f_x : \mathbb{S}^{2^n} \to \mathbb{R}$ defined by $f_x(|\psi\rangle) = \langle\psi| W_x |\psi\rangle$ is 2-Lipschitz.*

Proof. Write $W_x = \Pi_+ - \Pi_-$ where Π_+ and Π_- are the projectors onto the positive and negative eigenspaces of W_x, respectively. Then,

$$\begin{aligned}
|f_x(|\psi\rangle) - f_x(|\varphi\rangle)| &= |\langle\psi| W_x |\psi\rangle - \langle\varphi| W_x |\varphi\rangle| \\
&= |\langle\psi| \Pi_+ |\psi\rangle - \langle\varphi| \Pi_+ |\varphi\rangle - \langle\psi| \Pi_- |\psi\rangle + \langle\varphi| \Pi_- |\varphi\rangle| \\
&\leq |\langle\psi| \Pi_+ |\psi\rangle - \langle\varphi| \Pi_+ |\varphi\rangle| + |\langle\psi| \Pi_- |\psi\rangle + \langle\varphi| \Pi_- |\varphi\rangle| \\
&= |\ \|\Pi_+ |\psi\rangle\|_2 - \|\Pi_+ |\varphi\rangle\||_2 + ||\Pi_- |\psi\rangle\|_2 - \|\Pi_- |\varphi\rangle\|_2| \\
&\leq \|\Pi_+(|\psi\rangle - |\varphi\rangle)\|_2 + \|\Pi_-(|\psi\rangle - |\varphi\rangle)\|_2 \\
&\leq 2\||\psi\rangle - |\varphi\rangle\|_2,
\end{aligned}$$

where the third and fifth lines apply the triangle inequality, and the fourth and sixth lines use the fact that Π_+ and Π_- are projectors. ◀

▶ **Corollary 21.** *Let W_x be any n-qubit Weyl operator in which $x \neq 0$ (i.e. $W_x \neq I$). Then:*

$$\Pr_{|\psi\rangle \sim \mu_{\text{Haar}}}\left[|\langle\psi|W_x|\psi\rangle| \geq \varepsilon\right] \leq 2\exp\left(-\frac{2^n\varepsilon^2}{36\pi^3}\right).$$

Proof. Define $f_x(|\psi\rangle) = \langle\psi| W_x |\psi\rangle$ as in Lemma 20. By Lemma 20, we know that f_x is 2-Lipschitz. Additionally, observe that $\mathbf{E}[f] = 0$ over the Haar measure because exactly half of the eigenvalues of W_x are 1 and the other half are -1. Then the corollary follows from Lemma 19. ◀

▶ **Corollary 22.**

$$\underset{|\psi\rangle\sim\mu_{\text{Haar}}}{\boldsymbol{Pr}}\left[\exists x \neq 0 : |\langle\psi|W_x|\psi\rangle| \geq \varepsilon\right] \leq 2^{2n+1}\exp\left(-\frac{2^n\varepsilon^2}{36\pi^3}\right).$$

Proof. This follows from Corollary 21 and a union bound over all 2^{2n} possible Weyl operators. ◀

Note that if $\varepsilon \geq \frac{1}{\text{poly}(n)}$, then the probability bound in Corollary 22 is doubly-exponentially small.

We have shown that, with high probability, all Weyl measurements (except $W_x = I$) are close to 0. We use this to complete the proof of Lemma 15.

Proof of second part of Lemma 15. Suppose $|\psi\rangle$ is a Haar-random state. By Corollary 22, for all $W_x \neq I$, $|\langle\psi|W_x|\psi\rangle|^2 = 2^n p(x) \leq \varepsilon^2$ with probability $1-2^{2n+1}\exp\left(-\frac{2^n\varepsilon^2}{36\pi^3}\right)$. Therefore by Fact 16 and Proposition 17,

$$\begin{aligned}\underset{x\sim q_\psi}{\mathbf{E}}\left[|\langle\psi|W_x|\psi\rangle|^2\right] &= 32^n \sum_{x,y\in\mathbb{F}_2^n} \widehat{p}(x,y)^3\\ &= 4^n \sum_{w,v\in\mathbb{F}_2^n} p(v,w)^3\\ &= 4^n\left(\frac{1}{8^n} + \sum_{\substack{w,v\in\mathbb{F}_2^n\\ w,v\neq 0}} p(v,w)^3\right)\\ &\leq \frac{1+(4^n-1)\varepsilon^6}{2^n},\end{aligned}$$

with probability at least $1-2^{2n+1}\exp\left(-\frac{2^n\varepsilon^2}{36\pi^3}\right)$. By setting $\epsilon^2 = \frac{1}{2^{n/6}}\left(\frac{2^n-2^{n/2}}{4^n-1}\right)^{1/3}$, we get

$$\underset{x\sim q_\psi}{\mathbf{E}}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \leq \frac{1}{2^{n/2}}$$

with probability at least $1 - 2^{2n+1}\exp\left(-\frac{2^{5n/6}}{36\pi^3}\left(\frac{2^n-2^{n/2}}{4^n-1}\right)^{1/3}\right)$, which is at least $1-\exp\left(-2^{n/2-15}\right)$ for $n \geq 33$. ◀

4 Algorithm and Sample Complexity Analysis

We are now ready to state and analyze our algorithm that distinguishes between Haar-random states and states with low stabilizer complexity. Our algorithm uses the fact that we can efficiently sample from q_ψ (via Bell difference sampling) and efficiently estimate $|\langle\psi|W_x|\psi\rangle|^2$ for any given $x \in \mathbb{F}_2^{2n}$, using quantum measurements. By combining these subroutines, we construct an unbiased estimator for $\mathbf{E}_{x\sim q}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$. Motivated by Lemma 15, if our estimator exceeds a certain threshold we determine that the input state has low stabilizer complexity; otherwise, we determine that the state is Haar-random. For the remainder of this section, $\eta := \mathbf{E}_{x\sim q}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$.

Algorithm 1 Distinguishing Low-Stabilizer-Complexity States from Haar-Random.

```
Input: Black-box access to copies of $|\psi\rangle$
Promise: $|\psi\rangle$ is Haar-random or has stabilizer fidelity at least $\frac{1}{k}$
Output: 1 if $|\psi\rangle$ has stabilizer fidelity at least $\frac{1}{k}$ and 0 if $|\psi\rangle$ is Haar-random
Let $m = 60k^{12} \ln(1/\delta)$.
repeat $m$ times
    Perform Bell difference sampling to obtain $W_x \sim q_\psi$.
    Perform the measurement $W_x^{\otimes 2}$ on $|\psi\rangle^{\otimes 2}$. Let $X_i \in \{\pm 1\}$ denote the
      measurement outcome.
Set $\widehat{\eta} = \frac{1}{m}\sum_i X_i$. Return 1 if $\widehat{\eta} \geq \frac{2}{3k^6}$, and 0 otherwise.
```

▶ **Theorem 23.** *Let $|\psi\rangle$ be an unknown n-qubit pure state for some $n \geq 33$, and let $k \leq \frac{4}{5}2^{n/12}$. Algorithm 1 distinguishes whether $|\psi\rangle$ is Haar-random or a state with stabilizer fidelity at least $\frac{1}{k}$, promised that one of these is the case. The algorithm uses $O\left(k^{12}\log(1/\delta)\right)$ copies of $|\psi\rangle$ and $O(nk^{12}\log(1/\delta))$ time, and distinguishes the two cases with success probability at least $1-\delta$.*

Proof. Following the notation in Algorithm 1, X_i is the outcome of the measurement on the ith iteration of the algorithm loop. Observe that for any X_i,

$$\mathop{\mathbf{E}}_{\substack{x\sim q_\psi,\\ \text{meas. by } W_x^{\otimes 2}}}[X_i] = \mathop{\mathbf{E}}_{x\sim q_\psi} \langle \psi^{\otimes 2}|\, W_x^{\otimes 2}\, |\psi^{\otimes 2}\rangle = \mathop{\mathbf{E}}_{x\sim q_\psi} |\langle \psi|W_x|\psi\rangle|^2 = \eta.$$

Therefore, $\widehat{\eta} = \frac{1}{m}\sum_i X_i$ is an unbiased estimator of η (i.e., $\mathbf{E}[\widehat{\eta}] = \eta$).

Suppose $|\psi\rangle$ has stabilizer fidelity at least $\frac{1}{k}$. Then, our algorithm fails when $\widehat{\eta} < \frac{2}{3k^6}$. Hence,

$$\mathbf{Pr}[\text{Algorithm 1 fails}] = \mathbf{Pr}\left[\widehat{\eta} < \frac{2}{3k^6}\right] = \mathbf{Pr}\left[\widehat{\eta} - \eta < \frac{2}{3k^6} - \eta\right] \leq \mathbf{Pr}\left[\widehat{\eta} - \eta \leq -\frac{1}{3k^6}\right],$$

where the last inequality follows from Lemma 15. By Hoeffding's inequality,

$$\mathbf{Pr}\left[\widehat{\eta} - \eta \leq -\frac{1}{3k^6}\right] \leq \exp\left(-\frac{m}{18k^{12}}\right).$$

Therefore, $m \geq 18k^{12}\ln(15) = 49k^{12}$ samples suffice for the failure probability to be at most $\frac{1}{15}$.

Now suppose $|\psi\rangle$ is Haar-random. Then, our algorithm fails when $\widehat{\eta} \geq \frac{2}{3k^6}$. By Lemma 15, $\eta \leq 2^{-n/2}$ with probability at least $1 - \exp\left(-2^{n/2-15}\right) >= 1 - e^{-2\sqrt{2}}$ for $n \geq 33$. Assuming that $\eta \leq 2^{-n/2}$,

$$\begin{aligned}\mathbf{Pr}[\text{Algorithm 1 fails}] &= \mathbf{Pr}\left[\widehat{\eta} \geq \frac{2}{3k^6}\right]\\ &= \mathbf{Pr}\left[\widehat{\eta} - \eta \geq \frac{2}{3k^6} - \eta\right]\\ &\leq \mathbf{Pr}\left[\widehat{\eta} - \eta \geq \frac{1}{2k^6} - 2^{-n/2}\right].\end{aligned}$$

Once again, by Hoeffding's inequality,

$$\mathbf{Pr}\left[\widehat{\eta}-\eta \geq \frac{1}{2k^6}-2^{-n/2}\right] \leq \exp\left(-\frac{m}{2}\left(\frac{2}{3k^6}-2^{-n/2}\right)^2\right)$$
$$\leq \exp\left(-\frac{m}{2}\left(\frac{2}{3k^6}-\frac{1}{3k^6}\right)^2\right)$$
$$\leq \exp\left(-\frac{m}{18k^{12}}\right).$$

Therefore, $m \geq -18k^{12}\ln\left(\frac{1}{15}-e^{-2\sqrt{2}}\right) \geq 88k^{12}$ samples suffice for the failure probability to be at most $\frac{1}{15}-e^{-2\sqrt{2}}$. By the union bound, the failure probability is at most $\frac{1}{15}$, where the randomness is over both the Haar measure and the quantum measurements.

We have shown that in either case we output the correct answer with probability at least $\frac{14}{15}$. Using the Chernoff-Hoeffding theorem, the success probability can be boosted from $\frac{14}{15}$ to at least $1-\delta$ by doing $\frac{2}{3}\ln(1/\delta)$ repetitions of Algorithm 1 and taking the majority answer. Since each iteration of the algorithm loop uses 6 copies of $|\psi\rangle$, Algorithm 1 consumes $O\left(k^{12}\log(1/\delta)\right)$ copies in total. Finally, Bell difference sampling and performing the measurement $W_x^{\otimes 2}$ takes $O(n)$ time, so the total runtime is $O\left(nk^{12}\log(1/\delta)\right)$. ◀

All of these results also apply to states with stabilizer extent at most k, since by Claim 6, such states have stabilizer fidelity at least $\frac{1}{k}$.

▶ **Corollary 24.** *Let $|\psi\rangle$ be an unknown n-qubit pure state for $n \geq 33$, and let $k \leq \frac{4}{5}2^{n/12}$. Algorithm 1 distinguishes whether $|\psi\rangle$ is Haar-random or a state with stabilizer extent at most k, promised that one of these is the case. The algorithm uses $O\left(k^{12}\log(1/\delta)\right)$ copies of $|\psi\rangle$ and distinguishes the two cases with success probability at least $1-\delta$.*

The above result immediately implies that output states of Clifford+T circuits with few T-gates cannot be computationally pseudorandom.

▶ **Corollary 25.** *Any family of Clifford+T circuits that produces an ensemble of n-qubit computationally pseudorandom quantum states must use at least $\omega(\log n)$ T-gates.*

Proof. Consider any ensemble of states wherein each state in the ensemble is the output of some Clifford+T circuit with at most $K\log n$ T-gates. By Lemma 8, the stabilizer extent of any such state $|\psi\rangle$ is at most $n^{\alpha K}$ for $\alpha \leq 0.7716$. By Corollary 24, on input copies of $|\psi\rangle$, Algorithm 1 takes $O(n^{12\alpha K+1}) \leq \mathsf{poly}(n)$ time and outputs 1 with probability at least 2/3. On the other hand, if $|\psi\rangle$ is a Haar-random state then the same algorithm outputs 1 with probability at most $\frac{1}{3}$. As such, the algorithm's distinguishing advantage between the ensemble and the Haar measure is non-negligible. This is to say that the ensemble cannot be pseudorandom under the definition of [18]. ◀

5 Open Problems

An immediate direction for future work is to improve the sample complexity of our algorithm, or to prove sample complexity lower bounds. One can also endeavour to improve other features of our algorithm: Is it possible to remove the need for entangled measurements?[2] Or, is it possible to show that entangled measurements are in any sense necessary? Are there quantum measurements that allow us to sample from p_ψ directly (rather than q_ψ)?

[2] The optimal algorithms for learning and testing stabilizer states use entangled measurements. So, a first step would be to understand how many separable measurements are required to separate stabilizer states from Haar-random.

Beyond that, can Bell difference sampling be used for learning and/or property testing stabilizer-extent-k states? For stabilizer states ($k = 1$), a 6-query property testing algorithm is given by [13] and a $\Theta(n)$-query learning algorithm is given by [22]. Both algorithms rely on Bell difference sampling and are asymptotically optimal. We ask if there are generalizations of these algorithms for states with higher stabilizer complexity, similar to the question that was raised in [2].

▶ **Question 26.** *Is there a* $\mathsf{poly}(k)$*-query algorithm for property testing stabilizer-extent-k states? Likewise, is there a* $\mathsf{poly}(n, k)$*-time algorithm for learning stabilizer-extent-k states?*

Our results on stabilizer extent are due to the fact that extent and fidelity are inversely related. Is it possible to relate *stabilizer rank* (a closely-related complexity measure, denoted by χ) and stabilizer fidelity? For instance, proving that, for all states $|\psi\rangle$,

$$F_{\mathcal{S}}(|\psi\rangle)^{-1} \leq \chi(|\psi\rangle)^c, \quad \text{for any constant } c,$$

would imply that our algorithm can distinguish low-stabilizer-rank states from Haar-random. However, proving such a relation for even $c < \frac{\alpha n}{\log n}$ for $\alpha \leq 0.2284$ would imply super-linear lower bounds on the stabilizer rank of Clifford magic states, a long-standing open problem.

One can also ask if the lower bound on the number of T-gates necessary for computationally pseudorandom states can be improved.

▶ **Question 27.** *How many T-gates are necessary for a family of Clifford+T circuits to produce an ensemble of n-qubit computationally pseudorandom states?*

We remark that any improvements to our $\log n$ lower bound would require techniques beyond the ones used in our paper. Indeed, in Appendix B we show that one can hope for at most a quadratic improvement in the relationship between η and stabilizer fidelity. Such an improvement would only yield constant-factor improvements on the number of T-gates necessary to prepare computationally pseudorandom states.

On the other hand, we are not aware of any attempts to optimize the T-gate count for plausible constructions of n-qubit pseudorandom states. The best upper bound we know of is the essentially trivial bound of $O(n)$, based on constructions of with $O(n)$ general gates. This is because pseudorandom states can be constructed from pseudorandom functions (PRFs) with constant overhead [4], and PRFs are believed to be constructible in linear time [17, 9].[3]

References

1 Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5), November 2004. doi:10.1103/physreva.70.052328.

2 Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal algorithms for learning quantum phase states, 2022. doi:10.48550/arxiv.2208.07851.

3 Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-Testing/Correcting with Applications to Numerical Problems. *J. Comput. Syst. Sci.*, 47(3):549–595, 1993. doi:10.1016/0022-0000(93)90044-W.

4 Zvika Brakerski and Omri Shmueli. (Pseudo) Random Quantum States with Binary Phase. In *Theory of Cryptography*, 2019. doi:10.1007/978-3-030-36030-6_10.

[3] Technically, we are not sure whether the PRFs constructed in [17, 9] are secure against quantum adversaries, which is necessary for instantiating [4]'s construction, but we consider it reasonable to conjecture that linear-time quantum-secure PRFs exist.

5 Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum Amplitude Amplification and Estimation, 2002. doi:10.1090/conm/305/05215.

6 Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. Simulation of quantum circuits by low-rank stabilizer decompositions. *Quantum*, 3:181, September 2019. doi:10.22331/q-2019-09-02-181.

7 Sergey Bravyi and David Gosset. Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates. *Phys. Rev. Lett.*, 116:250501, 2016. doi:10.1103/PhysRevLett.116.250501.

8 A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996. doi:10.1103/PhysRevA.54.1098.

9 Zhiyuan Fan, Jiatu Li, and Tianqi Yang. The Exact Complexity of Pseudorandom Functions and the Black-Box Natural Proof Barrier for Bootstrapping Results in Computational Complexity. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, pages 962–975, 2022. doi:10.1145/3519935.3520010.

10 Manuel Gerken. Measure concentration: Levy's Lemma, 2013.

11 Daniel Gottesman. Stabilizer Codes and Quantum Error Correction, 1997. doi:10.48550/arxiv.quant-ph/9705052.

12 Daniel Gottesman. The Heisenberg Representation of Quantum Computers, 1998. doi:10.48550/arXiv.quant-ph/9807006.

13 David Gross, Sepehr Nezami, and Michael Walter. Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations. *Communications in Mathematical Physics*, 385(3):1325–1393, 2021. doi:10.1007/s00220-021-04118-7.

14 Jonas Haferkamp, Felipe Montealegre-Mora, Markus Heinrich, Jens Eisert, David Gross, and Ingo Roth. Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates, 2020. doi:10.48550/arxiv.2002.09524.

15 Marcel Hinsche, Marios Ioannou, Alexander Nietner, Jonas Haferkamp, Yihui Quek, Dominik Hangleiter, Jean-Pierre Seifert, Jens Eisert, and Ryan Sweke. A single t-gate makes distribution learning hard, 2022. doi:10.48550/arxiv.2207.03140.

16 Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020. doi:10.1038/s41567-020-0932-7.

17 Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with Constant Computational Overhead. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 433–442, 2008. doi:10.1145/1374376.1374438.

18 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom Quantum States. In *Advances in Cryptology – CRYPTO 2018*. Springer International Publishing, 2018. doi:10.1007/978-3-319-96878-0_5.

19 E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. *Physical Review A*, 77(1), 2008. doi:10.1103/physreva.77.012307.

20 Richard Kueng and David Gross. Qubit stabilizer states are complex projective 3-designs, 2015. doi:10.48550/arXiv.1510.02767.

21 Ching-Yi Lai and Hao-Chung Cheng. Learning Quantum Circuits of Some T Gates. *IEEE Transactions on Information Theory*, 68(6):3951–3964, 2022. doi:10.1109/TIT.2022.3151760.

22 Ashley Montanaro. Learning stabilizer states by Bell sampling. *arXiv preprint arXiv:1707.04012*, 2017. doi:10.48550/arXiv.1707.04012.

23 Michael A. Nielsen and Isaac Chuang. Quantum Computation and Quantum Information, 2002. doi:10.1017/CBO9780511976667.

24 Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. doi:10.1017/CBO9781139814782.

25 Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. Estimating Outcome Probabilities of Quantum Circuits Using Quasiprobabilities. *Phys. Rev. Lett.*, 115:070501, 2015. doi:10.1103/PhysRevLett.115.070501.

26 Patrick Rall, Daniel Liang, Jeremy Cook, and William Kretschmer. Simulation of qubit quantum circuits via Pauli propagation. *Phys. Rev. A*, 99:062337, 2019. doi:10.1103/PhysRevA.99.062337.

27 Robert Raussendorf and Hans J. Briegel. Quantum computing via measurements only, 2000. doi:10.48550/arxiv.quant-ph/0010033.

28 Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, 1995. doi:10.1103/PhysRevA.52.R2493.

29 Zak Webb. The Clifford Group Forms a Unitary 3-Design. *Quantum Info. Comput.*, 16(15–16):1379–1400, 2016.

30 Huangjun Zhu, Richard Kueng, Markus Grassl, and David Gross. The Clifford group fails gracefully to be a unitary 4-design, 2016. arXiv:1609.08172.

A Algorithm Improvements via State Preparation Unitary

When given access to a state preparation unitary for $|\psi\rangle$ (and its inverse), denoted by U and $U^\dagger$, we can improve the sample and time complexities of our algorithm to $O\left(k^3 \log(1/\delta)\right)$ and $O\left(nk^3 \log(1/\delta)\right)$, respectively, at the cost of $O\left(k^3 \log(1/\delta)\right)$ queries to U and $U^\dagger$.

Access to U and $U^\dagger$ allows us to run quantum amplitude estimation (QAE) as a subroutine in our algorithm. Recall the well-known result of Brassard, Høyer, Mosca, and Tapp:

▶ **Theorem 28** (Quantum Amplitude Estimation (Theorem 12 in [5])). *Let Π be a projector and $|\psi\rangle$ be an n-qubit pure state such that $\langle\psi|\Pi|\psi\rangle = \eta$. Given access to the unitary transformations $R_\Pi = 2\Pi - I$ and $R_\psi = 2|\psi\rangle\langle\psi| - I$, there exists a quantum algorithm that outputs $\widehat{\eta}$ such that*

$$|\widehat{\eta} - \eta| \leq \frac{2\pi\sqrt{\eta(1-\eta)}}{m} + \frac{\pi^2}{m^2}$$

with probability at least $\frac{8}{\pi^2}$. The algorithm makes m calls to R_Π and R_ψ.

▶ **Corollary 29.** *Let Π, $|\psi\rangle$, R_Π, and R_ψ be the same as in Theorem 28. There exists a quantum algorithm that outputs $\widehat{\eta}$ such that*

$$|\widehat{\eta} - \eta| \leq \varepsilon$$

with probability at least $\frac{8}{\pi^2}$. The algorithm makes no more than

$$\pi\frac{\sqrt{\eta(1-\eta)+\varepsilon}}{\varepsilon}$$

calls to R_Π and R_ψ.

Proof. By Theorem 28, this will require m queries, where m is a solution to the following quadratic equation:

$$\frac{2\pi\sqrt{\eta(1-\eta)}}{m} + \frac{\pi^2}{m^2} \leq \varepsilon \Rightarrow m \geq \pi\frac{\sqrt{\eta(1-\eta)+\varepsilon}}{\varepsilon} \geq \pi\frac{\sqrt{\eta(1-\eta)} + \sqrt{\eta(1-\eta)+\varepsilon}}{2\varepsilon}. \qquad ◀$$

With that, we are ready to explain the modifications to Algorithm 1 that achieves a quartic speedup in the dependency on k.

▶ **Theorem 30.** *Let $|\psi\rangle$ be an unknown n-qubit pure state prepared by a unitary U for $n \geq 33$, and let $k \leq \frac{4}{5}2^{n/12}$. There exists a quantum algorithm that distinguishes whether $|\psi\rangle$ is Haar-random or a state with stabilizer fidelity at least $\frac{1}{k}$, promised that one of these is The case. The algorithm uses $O\left(k^3 \log(1/\delta)\right)$ applications of either U or $U^\dagger$ and time $O\left(nk^3 \log(1/\delta)\right)$, and distinguishes the two cases with success probability at least $1-\delta$.*

Proof. We first define the *Bell difference sampling projector* on x as

$$\Pi_x \coloneqq \sum_{y \in \mathbb{F}_2^{2n}} |W_y\rangle\langle W_y| \otimes |W_{x+y}\rangle\langle W_{x+y}| .$$

Note that this is simply a compact way of writing the Bell difference sampling procedure: the probability of sampling x is $q_\psi(x) = \|\Pi_x |\psi^{\otimes 4}\rangle\|$.[4] We can also perform the projective measurement $P_{\psi,x} \coloneqq W_x |\psi\rangle\langle\psi| W_x = W_x U |0\rangle\langle 0| U^\dagger W_x$, where this measurement is performed by applying W_x, $U^\dagger$, and then measuring in the computational basis. We can entangle Π_x and $P_{\psi,x}$ to form the following projector:

$$M = \sum_{x \in \mathbb{F}_2^{2n}} \Pi_x \otimes P_{\psi,x}.$$

Building M involves controlled applications of W_x according to the Bell difference sampling outcome. Observe that

$$\langle\psi^{\otimes 5}|M|\psi^{\otimes 5}\rangle = \sum_{x \in \mathbb{F}_2^{2n}} \langle\psi^{\otimes 4}|\Pi_x|\psi^{\otimes 4}\rangle \cdot \langle\psi|P_{\psi,x}|\psi\rangle = \mathop{\mathbf{E}}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right].$$

Hence, we can run QAE with the input projector M and the input state $|\psi^{\otimes 5}\rangle$, and the output will be an estimate of η whose accuracy depends on m, the number of total calls to R_Π and R_ψ.

Proving the sample complexity bound will mimic Theorem 23. Suppose $|\psi\rangle$ is a state with stabilizer fidelity at least $\frac{1}{k}$. Define $\eta_{min} \coloneqq \frac{1}{k^6}$, and note that for any state with stabilizer fidelity at least $\frac{1}{k}$, $\eta \geq \eta_{min}$ due to Lemma 15. For our algorithm to succeed, recall from the proof of Theorem 23 that we need

$$|\widehat{\eta} - \eta| \leq |\frac{2}{3k^6} - \eta|.$$

Therefore, we can run QAE with a fixed value of m (to be specified later) for an estimate of η whose accuracy is within $\pm\left(\eta - \frac{2}{3k^6}\right)$. By Corollary 29,

$$m \geq \pi \frac{\sqrt{\eta(1-\eta) + \eta - \frac{2}{3k^6}}}{\eta - \frac{2}{3k^6}} \tag{2}$$

queries suffice. The chosen value of m must work for all $\eta \in [\frac{1}{k^6}, 1]$. Note that Equation (2) is monotonically decreasing for $\eta \in [\frac{2}{3k^6}, 1)$, and is therefore maximized by η_{min} for $\eta \in [\frac{1}{k^6}, 1]$. To succeed with probability at least $\frac{8}{\pi^2}$,

$$m \geq 4\pi k^3 \geq \pi\sqrt{12k^6 - 9} = \pi \frac{\sqrt{\eta_{min}(1-\eta_{min}) + \eta_{min} - \frac{2}{3k^6}}}{\eta_{min} - \frac{2}{3k^6}}$$

calls to R_Π and R_ψ suffices.

[4] Indeed, this is the way Gross, Nezami, and Walter [13] introduce Bell difference sampling.

Now suppose $|\psi\rangle$ is a Haar-random state. Again, by Lemma 15, we know that $\eta \leq 2^{-n/2}$ with probability $1 - e^{-2\sqrt{2}}$ for $n \geq 33$. Assuming $\eta \leq 2^{-n/2}$ and using Corollary 29, as long as we have

$$m \geq \sqrt{6}\pi k^3 \geq \pi \frac{\sqrt{2^{-n/2}(1-2^{-n/2}) + \frac{2}{3k^6} - 2^{-n/2}}}{\frac{2}{3k^6} - 2^{-n/2}} \geq \pi \frac{\sqrt{\eta(1-\eta) + \frac{2}{3k^6} - \eta}}{\frac{2}{3k^6} - \eta}$$

queries to R_Π and R_ψ, we obtain the correct answer with probability at least $\frac{8}{\pi^2}$. In the inequalities above we use similar reasoning to the stabilizer fidelity $\frac{1}{k}$ case, combined with the fact that $2^{-n/2} \leq \frac{1}{3k^6}$.

Finally, since R_Π and R_ψ use a constant number of calls to U and $U^\dagger$, the total number of calls is $O(k^3)$. Chernoff-Hoeffding can be used to bring the success probability from $3/4$ to $1 - \delta$ using $6\ln(1/\delta)$ repetitions. The runtime includes an extra factor of $O(n)$, due to the linear cost of both preparing W_x and the Bell difference sampling projector, giving a $O\left(nk^3 \log(1/\delta)\right)$ time complexity. ◀

B On the Tightness of Our Analysis

We argue that the first part of Lemma 15 is polynomially-close to optimal. We begin by computing the stabilizer extent and stabilizer fidelity of Clifford magic states. The two technical ingredients involved in the computation are due to Bravyi et al. [6].

▶ **Fact 31** ([6, Proposition 2]). *Let $|\psi\rangle$ be a Clifford magic state. Then,* $\xi(|\psi\rangle) = F_{\mathcal{S}}(|\psi\rangle)^{-1}$.

▶ **Fact 32** ([6, Proposition 1]). *Let $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_L\rangle\}$ be any set of states such that each state $|\psi_j\rangle$ describes a system of at most 3 qubits. Then,*

$$\xi(|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_L\rangle) = \prod_i \xi(|\psi_i\rangle).$$

It is well known that the m-fold tensor product of $|T\rangle \coloneqq 2^{-1/2}(|0\rangle + e^{i\pi/4}|0\rangle)$ is a Clifford magic state. Using the facts above, we can compute the stabilizer extent and stabilizer fidelity of $|T^{\otimes m}\rangle$.

▶ **Fact 33.**

$$\xi(|T^{\otimes m}\rangle) = (\cos\pi/8)^{-2m} \quad \textit{and} \quad F_{\mathcal{S}_m}(|T^{\otimes m}\rangle) = (\cos\pi/8)^{2m}.$$

Proof. By Fact 32, the stabilizer extent of $|T^{\otimes m}\rangle$ is simply the stabilizer extent of $|T\rangle$ raised to the power m. By Fact 31, the stabilizer extent is the inverse of the stabilizer fidelity. Hence, the result follows simply by showing that the stabilizer fidelity of $|T\rangle$ is $\cos(\pi/8)^2$, which can be verified by explicit calculation over the 6 different 1-qubit stabilizer states. ◀

Next, we compute η for the state $|T^{\otimes m}\rangle$.

▷ Claim 34. Let $|\psi\rangle = |T^{\otimes m}\rangle$ and define $\eta \coloneqq \mathbf{E}_{x\sim q_\psi}[2^n p_\psi(x)]$. Then, $\eta = (5/8)^m$.

Proof. We begin by writing out $|T\rangle\!\langle T|$ as a sum of Pauli matrices. By definition,

$$|T\rangle\!\langle T| = \frac{1}{2}\left(I + \frac{1}{\sqrt{2}}X + \frac{1}{\sqrt{2}}Y\right).$$

We wish to compute $\sum_{x \in \mathbb{F}_2^{2m}} \widehat{p}_\psi(x)^3$. We know that every such Pauli with nonzero $\widehat{p}_\psi(x)$ is a tensor product combination of I, X, and Y, so we enumerate over the number of indices where an X or Y appear.

$$\sum_{x \in \mathbb{F}_2^{2m}} \widehat{p}_\psi(x)^3 = \frac{1}{2^{6m}} \sum_{k=0}^{m} \binom{m}{k} \frac{1}{2^{3k}} \cdot 2^k = \frac{1}{64^m} \sum_{k=0}^{m} \binom{m}{k} \frac{1}{4^k} = \left(\frac{5}{256}\right)^m .$$

Thus, by Fact 16,

$$\eta = 32^m \sum_{x \in \mathbb{F}_2^{2m}} \widehat{p}_\psi(x)^3 = \left(\frac{5}{8}\right)^m . \qquad \triangleleft$$

Combining Claim 34 with Lemma 15, we have

$$F_{\mathcal{S}}(|\psi\rangle) \leq \eta^{1/c} = \left(\frac{5}{8}\right)^{m/c}$$

for $c = 6$ (Lemma 15). But, from Fact 33, we know that $F_{\mathcal{S}}(|T^{\otimes m}\rangle) = (\cos \pi/8)^{2m}$. Combining the two statements gives

$$(\cos \pi/8)^{2m} \leq (5/8)^{m/c}.$$

$c \approx 2.97$ is the minimum c that does not violate this inequality. Hence, one cannot hope for much more than a quadratic improvement in our bound.