Quadratic Lower Bounds on the Approximate Stabilizer Rank: A Probabilistic Approach

Saeed Mehraban
Tufts University
Medford, USA
saeed.mehraban@tufts.edu

Mehrdad Tahmasbi
University of Illinois Urbana-Champaign
Urbana, USA
mehrdad@illinois.edu

ABSTRACT

The approximate stabilizer rank of a quantum state is the minimum number of terms in any approximate decomposition of that state into stabilizer states. Bravyi and Gosset showed that the approximate stabilizer rank of a so-called "magic" state like $|T\rangle^{\otimes n}$, up to polynomial factors, is an upper bound on the number of classical operations required to simulate an arbitrary quantum circuit with Clifford gates and n number of T gates. As a result, an exponential lower bound on this quantity seems inevitable. Despite this intuition, several attempts using various techniques could not lead to a better than a linear lower bound on the "exact" rank of $|T\rangle^{\otimes n}$, meaning the minimal size of a decomposition that *exactly* produces the state. For the "approximate" rank, which is more realistically related to the cost of simulating quantum circuits, no lower bound better than $\tilde{\Omega}(\sqrt{n})$ has been known. In this paper, we improve the lower bound on the approximate rank to $\tilde{\Omega}(n^2)$ for a wide range of the approximation parameters. An immediate corollary of our result is the existence of polynomial time computable functions which require a super-linear number of terms in any decomposition into exponentials of quadratic forms over $\mathbb{F}_2$, resolving a question by Williams. Our approach is based on a strong lower bound on the approximate rank of a quantum state sampled from the Haar measure, a step-by-step analysis of the approximate rank of a magic-state teleportation protocol to sample from the Haar measure, and a result about trading Clifford operations with T gates.

CCS CONCEPTS

• **Theory of computation** → **Quantum complexity theory**.

KEYWORDS

Quantum computing, Stabilizer rank, Haar measure

ACM Reference Format:
Saeed Mehraban and Mehrdad Tahmasbi. 2024. Quadratic Lower Bounds on the Approximate Stabilizer Rank: A Probabilistic Approach. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC '24), June 24–28, 2024, Vancouver, BC, Canada.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3618260.3649733

STOC '24, June 24–28, 2024, Vancouver, BC, Canada

ACM ISBN 979-8-4007-0383-6/24/06
https://doi.org/10.1145/3618260.3649733

1 INTRODUCTION

Is there an efficient classical algorithm to simulate arbitrary quantum physical systems? This fundamental question plays a vital role in numerous science and engineering disciplines. For instance, in quantum chemistry, one may translate this question into the ability to measure the structural properties of molecules or design new materials [34]. Alternatively, in condensed matter theory, it is pertinent to our ability to predict the phases of quantum materials or sampling from thermal distributions [6]. Interestingly, this question also plays a non-trivial role in seemingly unrelated fields, such as theoretical computer science, cryptography, or number theory [21, 27, 44, 46].

In theoretical computer science, this question is formulated as the relationship between two complexity classes known as "bounded-error quantum polynomial time" (**BQP**) and "bounded-error classical polynomial time" (**BPP**). Since the early days of quantum mechanics, it was observed that many-body quantum systems have exponentially large phase spaces with counter-intuitive dynamics and unexpected features such as the duality of wave and particle aspects of subatomic systems (see [52] for some of the historical remarks). They furthermore demonstrate non-classical correlations known as entanglement [15]. Hence, the popular belief is that simulation of quantum systems requires exponential classical resources. This observation indeed motivated the development of quantum computing initiated by researcher such as Feynman in the 1980s [16]. Subsequently, a breakthrough result by Shor demonstrated that an efficient classical algorithm to simulate arbitrary quantum computations would also efficiently factor large numbers. This problem is crucial to the security of encryption schemes like RSA, for which no polynomial-time classical algorithm has been discovered despite centuries of research. It is thus natural to conjecture that **BPP** ≠ **BQP**. However, rigorous proof for this statement seems unlikely with current complexity theoretic tools since, for example, a proof of this statement will readily yield a separation of complexity classes such as "polynomial time" **P** and "polynomial space" **PSPACE**, which has been open beside an extensive amount of research over the past few decades.

Since an unconditional separation of **BPP** and **BQP** seems out-of-reach, it is insightful to ask the question from a complementary angle: are there restricted but non-trivial family of quantum systems that can be efficiently simulated classical computers. It turns out that there are several examples of classically simulable quantum circuits. For instance, if the amount of quantum entanglement at every step of a quantum circuit is limited, the system can be simulated efficiently [50]. Examples of such circuits include log-depth one-dimensional quantum circuits. Other classically simulable circuits based on constrained architecture include constant depth 2D

random quantum circuits on two-dimensional architectures [37] or adiabatic computations with large spectral gaps [39]. There is, however, an important class of quantum circuits known as Clifford circuits, which can generate maximal entanglement and have large circuit depth but admits efficient classical simulations through a well-known theorem due to Gottesmann and Knill [18]. This theorem works by considering quantum states "stabilized" by particular subgroups of the Pauli group; these states, also known as stabilizer states, were first introduced in the context of error-correcting codes [13] and subsequently found applications in several areas in quantum information science [29, 41]. The Clifford operations normalize the Pauli group, meaning they keep the group unchanged under conjugation, and hence, they map stabilizer states to stabilizer states. Starting from a stabilizer state, Gottesman-Knill's algorithm keeps track of generators of the stabilizer subgroup corresponding to the quantum state under simulation. This method leads to a strong simulation of Clifford circuits acting on stabilizer states on a classical computer, meaning that the output amplitudes of such computations can be computed exactly. Note that several classically simulable gate sets, such as match gates or the infinite-dimensional Gaussian gates, generate large amounts of entanglement and can be simulated classically efficiently. These simulation algorithms, however, capture variants of the Gottesman-Knill theorem for different physical particles known as Bosons [5] or Fermions [48]. In other words, the idea behind the Gottesman-Knill theorem is fundamental to all of these simulation techniques.

The Clifford gate set can only approximate a restricted family of quantum operations. However, this gate set becomes universal if we augment this gate set with an additional non-Clifford gate known as T, or $\pi/4$ phase shift. In the context of this universal gate set, the mentioned **BPP** vs. **BQP** question translates to characterizing the cost of classical simulation in terms of the number of T gates in an arbitrary quantum computation compiled into Clifford and T gates. Building on the Gottesman and Knill theorem, several works [10, 11] provided upper bounds on this classical simulation cost by developing classical simulation algorithms for quantum circuits dominated by Clifford gates. In particular, Bravi and Gosset [10] demonstrated that for a constant $c < 1$, a classical computer could simulate a quantum circuit with n qubits, $\text{poly}(n)$ Clifford gates, and m number of T gates in time $\text{poly}(n) \cdot 2^{cm}$. In their approach, they first consider teleportation of the so-called (non-stabilizer) magic state $|T\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$ to simulate the effect of a T gate at the middle of the circuit using Clifford gates and measurement in the computational basis. This operation converts a quantum circuit consisting of Clifford and T gates to a Clifford circuit with measurements and inputs $|T\rangle^{\otimes m}$ followed by some zero states. Then, they decompose $|T\rangle^{\otimes m}$ as a linear combination of $2^{c\cdot m}$ stabilizer states and use the Gottesman-Knill algorithm for each stabilizer state in this linear combination in time $\text{poly}(n)$. By the linearity of quantum mechanics, they can find the output of the circuit when the input is $|T\rangle^{\otimes m}$ in time $\text{poly}(n) \cdot 2^{c\cdot m}$. In this approach, a crucial quantity is the minimum number r such that there exist stabilizer states $|s_1\rangle, \ldots, |s_r\rangle$ and complex numbers $c_1, \ldots, c_r$ such that $|T\rangle^{\otimes m} = c_1|s_1\rangle + \ldots + c_r|s_r\rangle$. We call this quantity the stabilizer rank of $|T\rangle^{\otimes m}$ and denote it by $\chi(|T\rangle^{\otimes m})$. If we are interested in the minimum number of stabilizer states that approximate the $|T\rangle^{\otimes m}$ state within δ 2-norm, we arrive at the definition of the approximate rank, which we denote by $\chi_\delta(|T\rangle^{\otimes m})$. For an arbitrary state $|\psi\rangle$, we denote its approximate stabilizer rank with the approximation parameter $0 \le \delta \le 1$ by $\chi_\delta(|\psi\rangle)$.

In this paper, we study lower bounds on the number of steps the above simulation technique based on decomposing magic states into stabilizer states requires. In other words, our goal is to prove a lower bound on the stabilizer rank for the magic state $|T\rangle^{\otimes m}$. This question is essential in many ways. First, it gives significant insight into the relationship between **BQP** and **BPP** and why quantum computations obtain speedup over classical computations by studying a lower bound on **BQP** against a canonical class of simulation method on **BPP**. Similar questions have arisen in computational complexity, for instance, in the context of the **P** v.s. **NP** question, we know that specific restricted subclasses of **P** known as monotone circuits require an exponential lower bound to solve **NP**-hard problems [4, 42, 43].

Secondly, this question is conceptually an intriguing one. The complexity of classical simulation for quantum circuits is about counting the minimal number of computational steps that successfully simulate an "exponentially-sized" family of problems. In contrast, the problem of computing the stabilizer rank is "one counting problem" about "one" functional structure. It is counter-intuitive that the latter, which can be viewed as a question in functional analysis, would give non-trivial information about the former. Third, as we will highlight in Section 1.3, a lower bound on the (approximate) stabilizer rank organically connects with several interesting structural questions about complexity classes. For instance, we can show that if the exact rank is r, then $\mathbf{P}^{\#\mathbf{P}} \subseteq \text{TIME}(\text{poly}(n) \cdot r)/r$; here $\text{TIME}(\text{poly}(n) \cdot r)/r$ means a computation which runs in time $\text{poly}(n) \cdot r$ and has access to $O(r)$ bits of advice providing the description of the stabilizer decomposition. One of the immediate implications of the result of Bravyi and Gosset [10] is that assuming a polynomial upper bound on the approximate rank with approximation parameter δ implies that sampling within total variation distance $O(\delta)$ from arbitrary quantum circuits can be done in **BPP**; recent progress in quantum complexity theory has demonstrated that assuming plausible conjectures about the average-case hardness of specific approximate counting problems, sampling within total variation distance from quantum computers using **BPP** implies the collapse of the polynomial hierarchy (see for example [1, 7, 12]).

1.1 Overview of the Main Results

Even though we expect the exact stabilizer rank $\chi(|T\rangle^{\otimes m})$ to grow exponentially with m, the best-known lower bound has been $\tilde{\Omega}(m)$ due to three different groups [30, 32, 40]. As we will explain in Section 1.4, these three results use three different proof techniques, but they all stop at a linear lower bound. The situation with approximate stabilizer rank is slightly worse because the best-known lower bound for this quantity is $\sqrt{m}$ up to poly-logarithmic factors. An immediate conjecture is whether we can prove a super-linear lower bound on either the exact or approximate ranks.

In this paper, we resolve this conjecture by proving a nearly quadratic lower bound for the $|T\rangle^{\otimes m}$ state.

Theorem 1.1 (Informal statement of the main result). *Let $0 < \delta < 1$, then $\chi_\delta(|T\rangle^{\otimes m}) = \frac{\Omega(m^2)}{\text{poly}\log m}$.*

As the above theorem indicates, our result works for a wide range of error parameters. The T state a magic state in the second level of the Clifford hierarchy, meaning the group of operators that preserve the Clifford under conjugation; the third level is the group of operations that preserve the second level, and so on. Obviously, our result holds for quantum states that are Clifford equivalent to the T state but does not hold for arbitrary magic states. We remark that for $\delta = 0$, our result holds for any magic state.

Proof Sketch. Our method is a probabilistic one and has three main steps. As the first step, we show that for a random quantum state $|\phi\rangle$ with n qubits sampled from the Haar measure, the approximate rank satisfies the following strong concentration bound

$$Pr[\chi_\delta(|\phi\rangle) \leq M] \leq e^{n^2 M - \Omega(2^n)} \tag{1}$$

for any $\delta < 1$. As a result, we conclude that for all quantum states except for an exponentially small measure, the rank is at least $2^{n-o(1)}$.

Second, we show we can sample from the Haar measure with exponentially small error using $|T\rangle^{\otimes m}$ for $m \approx n2^{n/2}$ and m adaptive measurement. We know that arbitrary quantum states can be implemented using $\tilde{O}(2^n)$ number of T gates. However, by adding extra ancilla states initially in zeros and trading T gates with Clifford operations, we can implement arbitrary quantum states using $\tilde{O}(2^{n/2})$; this result is due to [33]. The third step is to show that the adaptive measurements do not increase the approximate rank of the T states. We remark that this step of the analysis, in its current form, relies critically on the structure of the state and works only for the T state due to its balanced structure, i.e., $|\langle 0|T\rangle|^2 = |\langle 1|T\rangle|^2$, and not arbitrary magic states. Putting these three steps together, and by rescaling $m = n2^{n/2}$, we obtain $\frac{\Omega(m^2)}{\text{polylog}(m)}$ lower bound on the approximate rank of $|T\rangle^{\otimes m}$.

The main bottleneck for going beyond the quadratic lower bound is that we need at least $\tilde{\Omega}(2^{n/2})$ T states to sample with high precision from the Haar measure; see [33] to see why this lower bound holds. We may wonder if we can use, instead of the Haar measure, pseudo-random quantum states such as approximate t-designs, which approximate the first t moments of the Haar measure and use $\ll 2^{n/2}$ T gates. It turns out the bound in Equation 1 relies on almost all moments of the Haar measure. For instance, the main strength of this bound is due to the 2^n factor in the tail. For t-designs we only get tails like $e^{n^2 M - \Omega(t)}$.

□

Next, we study the relationship between circuit complexity and approximate stabilizer rank. As shown above, we obtain a quadratic lower bound on the approximate rank of a simple state like $|T\rangle^{\otimes m}$, which has linear circuit complexity. More generally, our result implies the following

Theorem 1.2 (Stabilizer rank and circuit complexity). *For any number d there exists a quantum state with circuit complexity at most $n^d \text{poly}\log(n)$ and stabilizer rank at least n^d.*

We note that based on [8, 22] except for an exponentially small fraction, almost all quantum states from random quantum circuits of size s may not have circuit complexity less than $s^{1/5}$. This gives insight into why proving an exponential lower bound on the stabilizer rank of $|T\rangle^{\otimes n}$ might be a difficult task; likely $|T\rangle^{\otimes n}$ appears as one of the rare states whose circuit complexity may be compressed and the probabilistic method may not work anymore. As we will show in Section 4 a weaker version of this result can be deduced from the properties of t designs. In particular, we show that a quantum state of circuit complexity at most $O(n^{5d})$ and stabilizer rank at least n^d exists. However, if the dependency on the number of T gates used in [23] is improved to linear, we obtain exactly the result of Theorem 1.2. Alternatively, this result can be obtained from constructions of unitary t-designs based on random quantum circuits in time $O(t^{5+o(1)})\text{poly}(n)$ in [8, 22]. As indicated in [26], the bound on t can likely be improved to linear. In that case, we again obtain Theorem 1.2.

We raise the following conjecture:

Conjecture 1.3 (Stabilizer rank and circuit complexity). *For any constants $d \leq d'$, there exists a quantum state with circuit complexity at most n^d and stabilizer rank at least $n^{d'}$.*

1.2 Complexity Theoretic Implications

While proving unconditional separations between complexity classes is difficult, a simpler milestone is finding complexity-theoretic lower bounds against specific families of simple functions. For instance, we can consider the problem of representing Boolean functions in a specific complexity class such as **NP** as a linear combination of simple functions. For example, the so-called quadratic uncertainty principle [17] is the conjecture that in any exact decomposition of the AND function into

$$\sum_{j=1}^{r} c_j (-1)^{Q_j(x_1,\ldots,x_n)} \tag{2}$$

we need $r \geq 2^{\Omega(n)}$, where Q_j are quadratic polynomials over $\mathbb{F}_2$, and $c_j \in \mathbb{C}$. The best lower bound on this problem is linear due to Williams [53]. As observed by [40] Eq. (2) is exactly the overlap of sums of stabilizer states with bit strings. Because the AND function is itself a stabilizer function, it has a stabilizer rank of 1, and we do not hope to improve this bound based on a stabilizer lower bound approach. Williams furthermore showed that for any $k > 0$ there exists a function $f_k \in$**NP** such that $r \geq \Omega(n^k)$ for any decomposition of f_k into linear combination $\sum_{i=1}^{r} \alpha_i (-1)^{Q_i}$ for quadratic polynomials $Q_1, \cdots, Q_r$. An open problem is whether the same is true for functions in **P**; specifically, it is an open question whether there exists a function in **P** with super-linear r. As an immediate corollary of our result, we resolve this question by proving a (nearly) quadratic lower bound on the "approximate" rank r for the function defined in the following corollary (We remark that while the work of Williams [53] concerns exact decompositions, Chen and Williams [14] managed to extend some of the results in [53] to hold for the approximate decompositions as well).

Theorem 1.4. *Let $M : \{0,1\}^n \to \{0,1\}$ be such that $M(x_1, \ldots, x_n) = 1$ iff $x_1 + \ldots + x_n = 0 \mod 8$. Then any "approximate" decomposition*

of M into a decomposition $S_r(x)$ like Eq. (2) such that $\frac{1}{2^n}\sum_x |M(x) - S_r(x)|^2 \le \delta$ requires $r = \tilde{\Omega}(n^2)$.

Proof. Our proof is inspired by an observation made in [40] which implied a "linear" lower bound on the "exact" decomposition of M into quadratic phases. We use our main result (Theorem 1.1) to prove a (nearly) "quadratic" lower bound on the number of terms in any "approximate" decompositions of the Boolean function M into quadratic phases.

Define $T(x_1, \dots, x_n) = 2^{n/2}\langle x_1 \dots x_n | T\rangle = e^{i2\pi(|x|)/8}$, where $|x|$ is the Hamming weight of x. Let $\mathcal{Q} \subseteq \mathrm{Stab}_n$ be the set of all stabilizer states of the form $\frac{1}{\sqrt{2^n}}\sum_x (-1)^{Q(x)} |x\rangle$ for a quadratic polynomial $Q : \mathbb{F}_2^n \to \mathbb{F}_2$. With slight modification, the (nearly) quadratic lower bound in Theorem 1.2 also applies when we define the notion of rank with respect to the set $\mathcal{Q}$ instead of Stab_n. As a result, for any string $x \in \mathbb{F}_2^n$ and for any decomposition satisfying $\frac{1}{2^n}\sum_x |T(x) - \sum_{j=1}^{r_n}(-1)^{Q(x)}|^2 \le \delta$, we have $r_n = \tilde{\Omega}(n^2)$, where δ is a constant fixed in advance. T depends only on $|x| \mod 8$ and therefore can be written as $T(x) = \sum_{j=0}^{7} e^{2\pi i \frac{j}{8}} M_j(x)$ such that $M_j(x) = 1$ iff $|x| = j \mod 8$. Therefore, using the triangle inequality, there exists $j \in \{0, 1, \dots, 7\}$ such that any decomposition S_r with r terms that satisfies $\frac{1}{2^n}\sum_x |M_j(x) - S_r(x)|^2 \le \delta/7$ implies $r = \tilde{\Omega}(n^2)$. If $j = 0$, we are done. If $j \neq 0$ we use the following reduction:

$$M_0(\underbrace{1, \dots, 1}_{j}, x_1, \dots, x_n) = M_j(x_1, \dots, x_n).$$

Suppose there exists a decomposition with r terms S_r such that $\frac{1}{2^{n+j}}\sum_{y,x} |M_0(y_1, \dots, y_j, x_1, \dots, x_n) - S(y_1, \dots, y_j, x_1, \dots, x_n)|^2 \le \lambda$ therefore $S'_r(x_1, \dots, x_n) = S(y_1 = 1, \dots, y_j = 1, x_1, \dots, x_n)$ which has $\le r$ terms satisfies $\frac{1}{2^n}\sum_x |M_j(x) - S'_r(x)|^2 \le 2^j\lambda$. By choosing $\lambda = \delta/(7 \cdot 2^j)$ we conclude the proof. □

Remark 1.5. *This result can be viewed as a lower bound for a classical problem from an upper bound for a quantum synthesis problem, i.e., minimizing the number of T gates.*

1.3 Conditional Lower Bounds on the Exact Rank

Proving an unconditional exponential lower bound on the approximate stabilizer rank seems to be a difficult task. Can we prove this statement assuming plausible conjectures? [9] observed that for suitably small δ (and $\delta = 0$ in particular) a polynomial upper-bound on $\chi_\delta(|T\rangle^{\otimes m})$ would imply collapse of complexity classes such as **P** = **NP** or **BQP** = **BPP**. In this section, we show that a polynomial upper bound for $\delta = 0$ has the following stronger implication.

Theorem 1.6. *The exact rank of the magic state $|T\rangle^{\otimes m}$ is super-polynomial unless the permanent has polynomial circuits.*

Proof sketch. Here we provide a sketch of the proof. For further details, visit [35]. We show that if $\chi(|T\rangle^{\otimes m}) = \mathrm{poly}(m)$, there exists a polynomial-time algorithm with polynomial advice (and therefore a polynomial-size circuit) for the problem of computing the gap of a polynomial-size classical circuit and hence a polynomial-size circuit for the permanent. In particular, given a polynomial-size function $f : \{0,1\}^n \to \{0,1\}$, we print a polynomial-size quantum circuit with $m = \mathrm{poly}(n)$ many T gates U_f such that $\alpha\langle 0^{n+1}|U_f|0^{n+1}\rangle = gap(f)$, where α only depends on n ($\sqrt{2}2^n$ in particular). Using [9, Eq. (16)], we obtain we can replace T gates with T states and Clifford operations. In particular, there exists a polynomial-size Clifford circuit C_f such that

$$gap(f) = \beta\langle 0^{n+m+1}|C_f|0^{n+1}\rangle \otimes |T\rangle^{\otimes m} \tag{3}$$

where $\beta = \sqrt{2}2^n 2^{m/2}$. Consider a minimal decomposition of $|T\rangle^{\otimes m}$:

$$|T\rangle^{\otimes m} = \sum_{i=1}^{r} c_i |s_i\rangle \tag{4}$$

for $r = \chi(|T\rangle^{\otimes m})$ and stabilizer states $|s_1\rangle, \cdots, |s_r\rangle$. We show that if r is at most polynomially large in m (and hence in n), then we can use polynomial in n number bits of advice to represent $c_1, \dots, c_r$. It is not immediately clear that polynomial bits of advice that keep a $2^{-m^{O(1)}}$ precision for c_is is sufficient; we prove this in [35]. We then use polynomial bits of advice storing the variables in equation 4 to expand the expression in 3 and compute each term exactly using the Gottesman Knill theorem.

□

1.4 Related Works

As we mentioned before, there have been several results achieving lower bounds on the stabilizer rank prior to this work. Here, we briefly review some of these results. The first work in this line of research was [11] where the authors proved a lower bound of $\Omega(\sqrt{n})$ on the exact stabilizer rank of magic state with proof techniques similar to ours. More precisely, they constructed an arbitrary n-qubit quantum state with exact stabilizer rank $\Omega(n)$, which can be prepared by $O(n^2)$ T gates and Clifford gates. Then, they used the quantum teleportation idea to show that the exact stabilizer rank of $O(n^2)$ magic states is at least $\Omega(n)$. The authors of [9] established an exponential lower bound in a restricted setting in which we only consider stabilizer states that are tensor products of $|0\rangle$ and $|+\rangle$ states. They used ultra-metric matrices machinery to characterize the Gram matrix of such stabilizer states.

In [40] the authors proved a linear lower bound on the exact stabilizer rank by carefully investigating coefficients in the computational basis of any linear combination of $o(n)$ stabilizer states. In particular, they showed that there are two vectors in computation basis $|x\rangle$ and $|x'\rangle$ such that the number of ones in x and x' is different, but their corresponding coefficients are the same, so it cannot be associated with appropriate magic states. As a part of the same study, they also proved a lower bound of $\tilde{\Omega}(\sqrt{n})$ on the approximate stabilizer rank of magic states using tools from the polynomial method and an analysis of Boolean functions.

Labib in [30] proved a linear lower bound on exact rank using tools from higher-order Fourier analysis. He showed that $|T\rangle^{\otimes n}$ has an exponentially small correlation with a class of functions, so-called "quadratic non-classical phases" defined in higher-order Fourier analysis, and are inherently connected to stabilizer states. Then, he showed that any function written as $o(n)$ of such functions cannot have such a small correlation with all quadratic non-classical phases. Finally, among other contributions, the authors of [32] almost re-derived the results of [40] using a modified version of a result in number theory on the subset-sum representation of a

sequence of numbers with exponentially increasing subsequence. However, their lower bound on exact rank was $O(n/\log n)$ instead of $O(n)$, they handled both exact and approximate using similar approaches.

1.5 Discussions and Open Questions

(1) **Strengthening the bounds:** In this work, we provided a lower bound of $\frac{\Omega(n^2)}{\text{poly}\log n}$ on the approximate stabilizer rank of $|T\rangle^{\otimes n}$ or any state in the second Clifford hierarchy. We suspect that with more careful analysis, one can remove the $\text{poly}\log(m)$ factor from our lower bound. We may also be able to strengthen our result to hold for the approximate rank of all magic states; right now, the bound works only for the $|T\rangle$ state (and its Clifford equivalents) and/or exact rank. Nevertheless, obtaining a super-quadratic lower bound using our approach would be much more challenging. Indeed, with our proof technique, any deterministic or randomized construction of quantum states with low "non-Clifford complexity" (defined in Definition 2.1) but high approximate stabilizer rank is of interest (See also Conjecture 1.3). However, at least for two natural classes of probability distributions over quantum states, i.e., the Haar measure and t-designs, it seems that the non-Clifford complexity of a "typical" quantum state grows at least quadratically with approximate stabilizer rank.

(2) **Proving an exponential lower bound:** In our approach, we realize that the instances corresponding to states with high stabilizer rank and low circuit complexity correspond to an exponentially small fraction of quantum states. As a result, we believe that one needs to probe the structure of the stabilizer states more closely in order to make progress on this result. Building on the work of Labib [30], we suggest the following sufficient condition to improve the bound on stabilizer rank to exponential.

Conjecture 1.7. *Let $|\psi\rangle$ be a quantum state with stabilizer rank r, such that $F(|\psi\rangle) := \max_{s\in\text{Stab}_n} |\langle s|\psi\rangle|^2 < 1/e^{\Omega(n)}$, then there exists a stabilizer state $|s\rangle$ such that $|\langle s|T\rangle^{\otimes n}|^2 \geq \frac{1}{\text{poly}(r)}$.*

For instance, we know that $F(|T\rangle^n) = \cos(\pi/8)^{2n}$ [9]; however, the best bound we can prove for the largest overlap is $1/4^r$, which fails at giving a super-linear lower bound. Our intuition is that to improve this bound, we need to find sharp bounds on the geometry of stabilizer states, e.g., given a stabilizer state, find how many stabilizer states there are that have at least $1-\epsilon$ fidelity with that stabilizer state.
Another venue for going beyond quadratic lower bounds is by lower bounding the stabilizer rank of $|\psi\rangle \otimes |\phi\rangle$ when $|\psi\rangle$ and $|\phi\rangle$ are $n/2$ qubit states sampled from the Haar measure. In particular, if we can show that $\chi_\delta(|\psi\rangle \otimes |\phi\rangle) > (\chi_\delta(|\psi\rangle)\chi_\delta(|\phi\rangle))^{1/2+c}$ for some constant $c > 0$ and $\delta = 1/2^{\text{poly}(n)}$, then we can improve the quadratic lower bound on the stabilizer rank to possibly even exponential. The intuition is that in order to prepare $|\psi\rangle \otimes |\phi\rangle$ we quadratically have fewer number of $|T\rangle$ states than a n qubit state sampled from the Haar measure. We note that we can show $\chi_\delta(|\psi\rangle \otimes |\phi\rangle) \approx \chi_\delta(|\psi\rangle)\chi_\delta(|\phi\rangle)$ for $\delta = 1/2^{2^{\Omega(n)}}$ which is not sufficient for our purpose.

(3) **Strong lower bounds on exact rank from weak lower bounds on approximate ranks:** Another interesting question is whether our lower bound on approximate stabilizer rank has any implications for exact stabilizer rank. Lemma A.5 shows that in general, we cannot get a super-quadratic lower bound on exact stabilizer rank from only knowing that the approximate stabilizer rank is $\Omega(m^2/\text{poly}\log(m))$. However, we might be able to use some additional structures of magic states to improve the lower bound.

(4) **Complexity theoretic connections:** A natural open question is whether either of the ideas used in this paper can be utilized to prove the quadratic uncertainty principle for the AND function; see Section 1.2. Our main theorem implies a lower bound on the decomposition of the Boolean function $M(x) = 1$ iff $|x| = 0 \mod 8$. Rather surprisingly, this result can be viewed as a lower bound on a classical problem from an upper bound on a quantum state synthesis problem. Understanding the full capabilities of this approach for classical problems is an interesting future direction.
Can we strengthen Theorem 1.6? Sampling one bit from the output distribution of stabilizer circuits is complete for the complexity class $\oplus\mathbf{L}$ [3], which is the class of problems that are solvable on a non-deterministic logspace machine which the even parity of a non-deterministic path is an indication of acceptance. Hence, we suspect that the full power of $\mathbf{P}$ is not necessary to prove Theorem 4.3 and we might be able to replace $\mathbf{P}$ with a weaker class such as $\oplus\mathbf{L}$. However, to show this, we need to show that strong simulation of stabilizer circuits is also possible in $\oplus\mathbf{L}$. More realistically, we suspect a strong simulation of Clifford circuits is possible in gap$\mathbf{L}$ = $\mathbf{DET}$, the same way a strong simulation of $\mathbf{BQP}$ is possible in gap$\mathbf{P}$. How about approximate rank? A polynomial upper bound of on the δ approximate rank of the magic states implies sampling within total variation distance $O(\delta)$ from quantum circuits in polynomial time. Assuming conjectures about hardness of approximate counting for specific functions implies a super-polynomial lower bound on the approximate rank assuming the collapse of polynomial hierarchy [1, 7, 12]. Can we improve this result by basing the lower bound merely on the non-collapse of the polynomial hierarchy? We remark that unlike results such as [1, 2, 7, 12], we can allow any structured circuit (which, e.g., would permit error correction).

2 PRELIMINARIES

Let $\mathbb{F}_2$ be the finite field of order two. $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$. An affine subspace of $\mathbb{F}_2^n$ is a linear subspace shifted by an arbitrary vector. A quadratic function over $\mathbb{F}_2^n$ is of the form $x \mapsto x^T Ax + a^T x$ where T is an $n \times n$ matrix and $a \in \mathbb{F}_2^n$. The Hilbert space corresponding to an n-qubit system is $(\mathbb{C}^2)^{\otimes n}$. We identify the computational basis for this Hilbert space by elements of $x \in \mathbb{F}_2^n$. Let I_2 be the identity function on $\mathbb{C}^2$. Let $\mathcal{H}$ be a finite-dimensional Hilbert space in the following definitions. Let $U(\mathcal{H})$ denote all unitaries acting on $\mathcal{H}$. Let $\text{Proj}(\mathcal{H}, M)$ denote all the orthogonal

projections acting on $\mathcal{H}$ and rank at most M. For a linear operator $A : \mathcal{H} \to \mathcal{H}$, $\|A\|$ denotes the operator norm of A defined as

$$\|A\| \coloneqq \sup_{|\phi\rangle \in \mathcal{H} \setminus \{0\}} \frac{\|A|\phi\rangle\|}{\||\phi\rangle\|}. \tag{5}$$

Is the largest singular value of A and is the same as the infinite Schatten norm. Here, by $\| |v\rangle \|$ we mean the 2-norm of the vector $|v\rangle$. We also denote the trace-norm of A by $\|A\|_1 = \operatorname{tr}\sqrt{AA^\dagger}$. A *quantum channel* is a linear super-operator that is trace-preserving and completely positive. The diamond distance between two quantum channels Φ and Ψ for a Hilbert space $\mathcal{H}$ is defined as

$$\sup_{d \geq 0} \sup_{X \in \mathcal{H} \otimes \mathbb{C}^d} \frac{\|(\Phi \otimes \mathrm{id}_d(X) - \Psi \otimes \mathrm{id}_d(X))\|_1}{\|X\|_1}, \tag{6}$$

where id_d is the identity channel on $\mathbb{C}^d$.

2.1 Quantum Circuits

A quantum circuit on n qubits is a unitary operation over $(\mathbb{C}^2)^{\otimes n}$. In most cases, we represent a quantum circuit as a product of m unitaries $V_1, \cdots, V_m$ where each V_i is a unitary acting on a subset of qubits (typically of size one, two, or three). The unitaries acting on a smaller number of qubits are called quantum gates, and the set of all allowed gates is called a gate set. A gate set is *universal* if one can approximate any unitary on n qubits within an arbitrary error using a sequence of gates from the gate set. We know that the gate set $\{H, CNOT, S, T\}$ is universal where

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},$$
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \tag{7}$$

Finally, we define a notion of "non-Clifford complexity," quantifying how many non-Clifford resources we need to prepare a quantum state.

Definition 2.1. *Let $|\phi\rangle$ be an n qubit state. $\tau_\epsilon(|\phi\rangle)$ is the smallest k such that there exists a quantum circuit V, acting on $n + \lambda$ qubits for $\lambda > 0$, consisting of arbitrary number of Clifford gates and k number of T gates such that $\||\phi\rangle \left|0^\lambda\right\rangle - V(|0^n\rangle \left|0^\lambda\right\rangle)\| \leq \epsilon$.*

2.2 Stabilizer Formalism

We briefly review stabilizer formalism here (see [38] for details). Let $\mathcal{P}_n$ be the Pauli group acting on n qubits. The Clifford group on n qubits, denoted by C_n, is the normalizer of $\mathcal{P}_n$ in the unitary group modulo a phase. We denote by Stab_n the set of all stabilizer states, which can be written of the form [49]

$$\frac{1}{\sqrt{|A|}} \sum_{x \in A} i^{\ell(x)} (-1)^{Q(x)} |x\rangle, \tag{8}$$

where $A \subset \mathbb{F}_2^n$ is an affine subspace of $\mathbb{F}_2^n$ ($A = \{Ly + v : y \in \mathbb{F}_2^m\}$, where $L \in \mathbb{F}_2^{n \times m}$, $V \in \mathbb{F}_2^n$), $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$ is a linear function, and $Q : \mathbb{F}_2^n \to \mathbb{F}_2$ is a quadratic function. Here are some known facts about stabilizer states.

Lemma 2.2. *The following are true*

(1) For any Clifford unitrary $C \in C_n$ and any stabilizer state $|s\rangle \in \mathrm{Stab}_n$, we have $C|s\rangle \in \mathrm{Stab}_n$.
(2) Let $|s\rangle$ be an n-qubit stabilizer state and $b \in \mathbb{F}_2$. Then, $I_2^{\otimes n-1} \otimes \langle b| |s\rangle$ is either zero or proportional to a state in Stab_{n-1}.
(3) $|\mathrm{Stab}_n| \leq e^{0.54n^2}$ for $n \geq 6$ [31].

We next define the (approximate) stabilizer rank of a quantum state. Let $|\phi\rangle$ be an n-qubit state. We denote by $\chi(|\phi\rangle)$ the stabilizer rank of $|\phi\rangle$ defined as the minimum $M > 0$ such that there exists $c_1, \cdots, c_M \in \mathbb{C}$ and $|s_1\rangle, \cdots, |s_M\rangle \in \mathrm{Stab}_n$ such that $|\phi\rangle = \sum_{i=1}^M c_i |s_i\rangle$. We also define $\chi_\delta(|\phi\rangle)$ as

$$\min_{|\psi\rangle : \||\phi\rangle - |\psi\rangle\| \leq \delta} \chi(|\psi\rangle), \tag{9}$$

where $|\psi\rangle$ does not need to be normalized. We remark that the stabilizer rank is operationally relevant to the cost of classical simulation. We may choose other measures of closeness to the set of stabilizer states which we will review in Appendix A.

2.3 Haar Measure and t-Designs

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. The Haar measure over $\mathcal{H}$ is the unique probability distribution on the unit vectors in $\mathcal{H}$ invariant under the action of any unitary in $U(\mathcal{H})$. We shall use the following concentration of measure result for the Haar measure over finite-dimensional Hilbert spaces known as Lévy's theorem [51, Theorem 7.37].

Theorem 2.3 (Lévy's concentration)**.** *Let $\mathcal{H}$ be a d-dimensional Hilbert space and $|\phi\rangle$ be distributed according to the Haar measure in $\mathcal{H}$. For any κ-Lipschitz function f from the unit sphere in $\mathcal{H}$ to $\mathbb{R}$ and $\epsilon > 0$, we have*

$$\Pr[f(|\phi\rangle) - \mathrm{E}[f(|\phi\rangle)] \geq \epsilon] \leq 2e^{-\frac{\epsilon^2 d}{25\pi\kappa^2}} \tag{10}$$

A function is κ-Lipschitz if $|f(|\phi\rangle) - f(|\psi\rangle)| \leq \kappa \| |\psi\rangle - |\phi\rangle \|$. We use the following property of Haar measure, whose proof is similar to that of [51, Lemma 7.2].

Lemma 2.4. *Let $\mathcal{H}$ be a d-dimensional Hilbert space and P be a projection on $\mathcal{H}$ of rank M. Let $|\phi\rangle$ be distributed according to the Haar measure in $\mathcal{H}$. Then,*

$$\operatorname{tr}(P^{\otimes t} \mathrm{E}\left[(|\phi\rangle\langle\phi|)^{\otimes t}\right]) = \frac{\binom{M+t-1}{t}}{\binom{d+t-1}{t}} = \frac{(M+t-1)\cdots(M+1)M}{(d+t-1)\cdots(d+1)d}. \tag{11}$$

The Haar measure over $U(\mathcal{H})$ is the unique probability distribution invariant under left or right multiplication by any unitary in $U(\mathcal{H})$. While preparing a unitary according to the Haar measure requires an exponential amount of resources [28], unitary t-designs, which we formally define here, mimic the Haar measure up to the t-th moment and can be efficiently prepared for t small enough.

Definition 2.5. *Denote for a distribution ν over $U(\mathcal{H})$*

$$M_t^\nu(\rho) \coloneqq \int U^{\otimes t} \rho (U^\dagger)^{\otimes t} d\nu, \tag{12}$$

which is a quantum channel. We call ν an ϵ-approximate t-design if $\|M_t^\nu - M_t^{\mathrm{Haar}}\|_\diamond \leq \epsilon$.

There are several constructions of approximate t-designs [8, 22–24, 36]. We state here two constructions: one that has a close connection to stabilizer formalism and one using random circuits.

Theorem 2.6 ([23]). *There exists constant C_1 and C_2 such that for all ϵ, n, and t with $n \geq C_2 t^2$ the following holds. There exists an ϵ-approximate t-design ν such that any unitary in the support of ν consists of Clifford gates and at most $C_1 \log^2(t)(t^4 + t\log(1/\epsilon))$ number of T gates.*

Theorem 2.7 ([22]). *For $n \geq 2\log(4t) + 1.5\sqrt{\log(4t)}$, there exists an ϵ-approximate t-design for n qubits such that each unitary in the support of ν is composed of $Cn\ln^5(t)t^{4+3\frac{1}{\sqrt{\log(t)}}}(2nt + \log(1/\epsilon))$ two-qubit gates for absolute constant $C > 0$.*

We also state a conjecture on the optimal number of non-Clifford gates in any t-design when t scales with n. The intuition behind this conjecture is that by [8, Proposition 8], we need $\tilde{\Omega}(nt)$ gates to get a t-design for n-qubits, and we expect that most of these gates should be non-Clifford.

Conjecture 2.8. *Let ν be a distribution supported on quantum circuits with an arbitrary number of Clifford gates and k number of T gates. If ν is an ϵ-approximate t-design for $t = \omega(1)$, then $k = \Omega(t)$.*

3 LOWER BOUNDS ON APPROXIMATE STABILIZER RANK OF MAGIC STATES

In this section, we state and prove our main result, which is a lower bound on the approximate stabilizer rank of $|T\rangle^{\otimes n}$.

Theorem 3.1. *Let $1 > \delta > 0$. We have*

$$\chi_\delta(|T\rangle^{\otimes m}) = \Omega\left(\frac{(1-\delta^2)^2 m^2}{\text{poly}\log(m)}\right). \tag{13}$$

We prove the above result using three ingredients.

(1) In Section 3.1, we show that for each n and δ there exists an arbitrary n-qubit quantum state with an approximate stabilizer rank $\Omega(2^n/n^2)$ (Lemma 3.2). To prove this result, we consider the approximate stabilizer rank of a random n-qubit state distributed according to the Haar measure. For each choice of $\Omega(2^n/n^2)$ number of stabilizer states, we obtain a doubly exponential upper bound on the probability that we can estimate the random state as a linear combination of those stabilizer states. We then use the union bound to obtain an upper bound on the probability that a random state has approximate stabilizer rank $\Omega(2^n/n^2)$.
(2) In Section 3.2, we state a result of [33] that shows every n-qubit state can be approximated using Clifford gates and at most $O(\text{poly}(n2^{n/2})$ number of T gates and many ancilla qubits (Lemma 3.5).
(3) In Section 3.3, we finally use the ideas in gadget-based implementation of T gates to show that the approximate stabilizer rank of the output of state is upper bounded by stabilizer rank of $|T\rangle^{\otimes m}$ (Lemma 3.6).

Having these ingredients, we prove Theorem 3.1 in Section 3.4, but provide the high-level argument here. Fixing m, we choose n such that $\text{poly}(n)2^{n/2} \approx m$, which implies that $n \approx 2\log m$ and $2^{n/2} \approx m/\text{poly}\log(m)$. We then choose quantum state $|\phi\rangle$ with n qubits and approximate stabilizer rank $\Omega((1-\delta^2)^2 2^n/n^2) = \Omega((1-\delta^2)^2 m/\text{poly}\log(m))$ according to the first ingredient. Let V be the quantum circuit according to the second ingredient, i.e., $V|0^n\rangle \approx |\phi\rangle$ and V contains Clifford gates and $m = \text{poly}(n)2^{n/2}$ number of T gates. Then, using the last ingredient, we obtain

$$\begin{aligned}\Omega((1-\delta^2)^2 m^2/\text{poly}\log(m)) = \chi_\delta(|\phi\rangle) &\approx \chi_\delta(V(|0^n\rangle|0^\lambda\rangle)) \\ &\leq \chi_\delta(|T\rangle^{\otimes \text{poly}(n)2^{n/2}}) \approx \chi_\delta(|T\rangle^{\otimes m}).\end{aligned} \tag{14}$$

See Section 3.4 for details.

3.1 Existence of Quantum States with Large Approximate Stabilizer Rank

The following lemma provides an upper bound on the likelihood that a Haar random state of n qubits has a small approximate stabilizer rank.

Lemma 3.2. *Let $|\phi\rangle$ be a random n-qubit state distributed according to Haar measure with $n \geq 6$. Let M be a positive integer and $0 < \delta < 1$ be such that $1 - \delta^2 - \frac{M}{2^n} > 0$. We have*

$$\Pr[\chi_\delta(|\phi\rangle) \leq M] \leq 2e^{0.54n^2 M - \frac{(1-\delta^2 - M/2^n)^2 2^n}{100\pi}} \tag{15}$$

In particular, for $n \geq 2\log\frac{1}{1-\delta^2} + 9$, there exists an n-qubit state $|\phi\rangle$ with $\chi_\delta(|\phi\rangle) \geq C\frac{(1-\delta^2)^2 2^n}{n^2}$ for an absolute constant $C \geq \frac{1}{1000}$.

Remark 3.3. *A random state distributed according to Haar measure with probability zero lies inside the span of any $2^n - 1$ stabilizer states. Therefore, by union bound,*

$$\Pr\left[\chi(|\phi\rangle) = 2^n\right] = 1. \tag{16}$$

Lemma 3.2 states a robust version of this observation.

To prove the above lemma, we first introduce a necessary condition for the approximate stabilizer rank of an arbitrary state to be less than M in the following lemma.

Lemma 3.4. *Let $|\phi\rangle$ be an n-qubit state. If $\chi_\delta(\phi) \leq M$, then*

$$\max_{S\subset \text{Stab}_n : |S| = M} \|P_S|\phi\rangle\|^2 \geq 1 - \delta^2$$

where P_S denotes the orthogonal projection onto the subspace spanned by the elements of S.

Proof. Assume that $\chi_\delta(\phi) \leq M$. It means that there exist complex numbers $c_1, \cdots, c_M$ and $S = \{|s_1\rangle, \cdots, |s_M\rangle\} \subset \text{Stab}_n$ such that $\left\||\phi\rangle - \sum_{i=1}^M c_i|s_i\rangle\right\| \leq \delta$. We also know that

$$\begin{aligned}1 = \||\phi\rangle\|^2 &\overset{(a)}{=} \||\phi\rangle - P_S|\phi\rangle\|^2 + \|P_S|\phi\rangle\|^2 \\ &\overset{(b)}{\leq} \left\||\phi\rangle - \sum_{i=1}^M c_i|s_i\rangle\right\|^2 + \|P_S|\phi\rangle\|^2 \leq \delta^2 + \|P_S|\phi\rangle\|^2\end{aligned} \tag{17}$$

where (a) follows from Pythagoras Theorem in Hilbert Spaces, and (b) follows since $P_S|\phi\rangle$ is the closest point to $|\phi\rangle$ in the subspace spanned by elements of S. Therefore, $\|P_S|\phi\rangle\|^2 \geq 1 - \delta^2$ as desired. □

Proof of Lemma 3.2. Before delving into the technical proof, we sketch the main ideas. Lemma 3.4 helps us to upper bound the probability that the approximate stabilizer rank of a random state is less than M in terms of the norm of the projection of the

random state into several subspaces. We use union bound and Lévy's theorem (Theorem 2.3) to upper bound that probability.

Note that

$$\Pr[\chi_\delta(|\phi\rangle) \le M] \overset{(a)}{\le} \Pr\left[\max_{S\subset \mathrm{Stab}_n:|S|=M} \|P_S|\phi\rangle\|^2 \ge 1-\delta^2\right] \tag{18}$$

$$\overset{(b)}{\le} \sum_{S\subset \mathrm{Stab}_n:|S|=M} \Pr\left[\|P_S|\phi\rangle\|^2 \ge 1-\delta^2\right] \tag{19}$$

$$\le \binom{|\mathrm{Stab}_n|}{M} \sup_{\substack{P\in\\ \mathrm{Proj}((\mathbb{C}^2)^{\otimes n},M)}} \Pr\left[\|P|\phi\rangle\|^2 \ge 1-\delta^2\right] \tag{20}$$

$$\le |\mathrm{Stab}_n|^M \sup_{\substack{P\in\\ \mathrm{Proj}((\mathbb{C}^2)^{\otimes n},M)}} \Pr\left[\|P|\phi\rangle\|^2 \ge 1-\delta^2\right] \tag{21}$$

$$\overset{(c)}{\le} e^{0.54n^2M} \sup_{\substack{P\in\\ \mathrm{Proj}((\mathbb{C}^2)^{\otimes n},M)}} \Pr\left[\|P|\phi\rangle\|^2 \ge 1-\delta^2\right] \tag{22}$$

where (a) follows from Lemma 3.4, (b) follows from the union bound, and (c) follows from Lemma 2.2. We now upper bound $\Pr\left[\|P|\phi\rangle\|^2 \ge 1-\delta^2\right]$ for $P \in \mathrm{Proj}((\mathbb{C}^2)^{\otimes n}, M)$ using Lévy's theorem (Theorem 2.3).

We take $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ and $f(|\phi\rangle) = \|P|\phi\rangle\|^2$ and show that f is 2-Lipschitz and $\mathrm{E}[f(|\phi\rangle)] \le \frac{M}{2^n}$. First note that for arbitrary unit vectors $|\phi\rangle$ and $|\psi\rangle$, we have

$$|f(|\phi\rangle) - f(|\psi\rangle)| = |\|P|\phi\rangle\|^2 - \|P|\psi\rangle\|^2| \tag{23}$$

$$= |\|P|\phi\rangle\| - \|P|\psi\rangle\||(\|P|\phi\rangle\| + \|P|\psi\rangle\|) \tag{24}$$

$$\le \|P|\phi\rangle - P|\psi\rangle\|(\|P|\phi\rangle\| + \|P|\psi\rangle\|) \tag{25}$$

$$\le \||\phi\rangle - |\psi\rangle\|(\||\phi\rangle\| + \||\psi\rangle\|) \tag{26}$$

$$= 2\||\phi\rangle - |\psi\rangle\|, \tag{27}$$

which means that f is 2-Lipschitz. By Lemma 2.4, we also have $\mathrm{E}[f(|\phi\rangle)] = \frac{\mathrm{rank}P}{2^n} \le \frac{M}{2^n}$. Applying Lèvy's theorem, we obtain

$$\Pr\left[\|P|\phi\rangle\|^2 \ge 1-\delta^2\right] \le 2e^{-\frac{(1-\delta^2-M/2^n)^2 2^n}{100\pi}}. \tag{28}$$

Combining (22) and (28) yields the first part of Lemma 3.2.

To prove the second part, it is enough to show that for $n \ge 2\log\frac{1}{1-\delta^2} + 9$ and $M = \frac{(1-\delta^2)^2 2^n}{1000n^2}$, $\Pr[\chi_\delta(|\phi\rangle) \le M] < 1$.

By the first part of the lemma, it is enough to show that $0.54n^2M - \frac{(1-\delta^2-M/2^n)^2 2^n}{100\pi} \le -1$.

We have by direct calculation

$$1-\delta^2-\frac{M}{2^n} = 1-\delta^2-\frac{(1-\delta^2)^2}{1000n^2} \ge (1-\delta^2)\left(1-\frac{1}{1000}\right). \tag{29}$$

and therefore

$$0.54n^2M - \frac{(1-\delta^2-M/2^n)^2 2^n}{100\pi} \le 0.54n^2M - \frac{(1-\delta^2)^2(0.999)^2 2^n}{100\pi}$$

$$= (1-\delta^2)^2 2^n (.00054 - \frac{0.999^2}{100\pi}) \le -0.0026(1-\delta^2)^2 2^n, \tag{30}$$

which is less than -1 for $n \ge 2\log\frac{1}{1-\delta^2} + 9$. □

3.2 Trading T Gates for Clifford Operations

In the previous section, we showed that, except for an exponentially small fraction, Haar random quantum states have exponentially large approximate ranks. Our strategy is to translate this lower into a lower bound on the approximate stabilizer rank of $|T\rangle^{\otimes n}$. As an intermediate step toward this goal, we need to find an upper bound on the number of T gates necessary to sample from the Haar measure. This section finds an upper bound on the number of T gates to construct arbitrary quantum states. One might expect that an arbitrary quantum state would require $\Omega(2^n)$ numbers of T gates to prepare. It turns out that by allowing ancilla qubits, arbitrary quantum states may be prepared using $\tilde{O}(2^{n/2})$ number of T gates and $\tilde{O}(2^{n/2})$ ancillae.

Lemma 3.5 (Trading T gates with Clifford operations [33]). *Let $|\phi\rangle$ be an arbitrary n-qubit quantum state then $\tau_{4^{-n}}(|\phi\rangle) = 2^{n/2}O(n)$ where τ_ϵ is defined in Definition 2.1.*

This lemma makes a nontrivial use of anciallae to provide a quadratic saving on the number of T gates. This nontrivial result enables us to cross the linear lower-bound barrier on the stabilizer rank and obtain a quadratic lower bound.

3.3 Approximate Stabilizer Rank and Quantum Circuits

Lemma 3.6. *Let V be a quantum circuit consisting of Clifford gates and k T gates. Then, $\chi_\delta(V|0\rangle) \le \chi_\delta(|T\rangle^{\otimes k})$.*

The proof is based on the idea of teleportation of each T gate using a magic $|T\rangle$ state. We need the following two technical results for the measurement required in the teleportation of T gate. We first show that under certain conditions, the measurement output has a uniform distribution. This result is implicitly assumed in the literature, but we provide proof for completeness.

Lemma 3.7. *Let $|\psi\rangle$ be an n-qubit quantum state. Apply controlled-not gate on the last qubit of $|\psi\rangle \otimes |T\rangle$ controlled on one of the qubits in $|\psi\rangle$ and then measure the last qubit in the computational basis. Then, the output of the measurement has a uniform distribution.*

Proof. Write $|\psi\rangle = \sum_{x\in\mathbb{F}_2^n} \alpha_x |x\rangle$. Without loss of generality, we assume that the CNOT is controlled on the first qubit. The state after applying CNOT is $\sum_{x\in\mathbb{F}_2^n} \alpha_x |x\rangle \otimes \frac{|x_1\rangle + e^{i\pi/4}|1-x_1\rangle}{\sqrt{2}}$. Hence, the probability that we obtain zero after measuring the last qubit is

$$\left\|(I_2^{\otimes n} \otimes \langle 0|) \sum_{x\in\mathbb{F}_2^n} \alpha_x |x\rangle \otimes \frac{|x_1\rangle + e^{i\pi/4}|1-x_1\rangle}{\sqrt{2}}\right\|^2$$

$$= \frac{1}{2}\left\|\sum_{x\in\mathbb{F}_2^n} e^{x_1 i\pi/4}\alpha_x |x\rangle\right\|^2 = \frac{1}{2}\|\psi\|^2 = \frac{1}{2}, \tag{31}$$

as desired. □

The next lemma states that performing a "balance" measurement on one of the qubits does not increase the approximate stabilizer rank for at least one outcome.

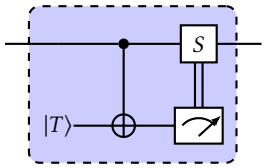

Figure 1: Gadget for implementing T gate

Lemma 3.8. *Consider measuring the last qubit in an n-qubit state $|\phi\rangle$ in the computational basis. Let p_b be the probability that the measurement output is b and $\left|\widetilde{\phi_b}\right\rangle$ be the post-measurement state when the output is b. If $p_0 = p_1$, then $\min_{b=0,1} \chi_\delta(\left|\widetilde{\phi_b}\right\rangle) \leq \chi_\delta(|\phi\rangle)$.*

Proof. Let $\chi_\delta(|\phi\rangle) = M$ and consider $c_1, \cdots, c_M \in \mathbb{C}$ and $|s_1\rangle, \cdots, |s_M\rangle \in \mathrm{Stab}_n$ such that $\left\||\phi\rangle - \sum_{i=1}^M c_i |s_i\rangle\right\| \leq \delta$. We also define $|\psi\rangle = \sum_{i=1}^M c_i |s_i\rangle$ and decompose $|\phi\rangle = |\psi_0\rangle \otimes |0\rangle + |\phi_1\rangle \otimes |1\rangle$ and $|\psi\rangle = |\psi_0\rangle \otimes |0\rangle + |\psi_1\rangle \otimes |1\rangle$. Since $|0\rangle$ and $|1\rangle$ are orthogonal, we have $\||\phi_0\rangle - |\psi_0\rangle\|^2 + \||\phi_1\rangle - |\psi_1\rangle\|^2 \leq \delta^2$. Hence, $\min_{b=0,1} \||\phi_b\rangle - |\psi_b\rangle\| \leq \frac{\delta}{\sqrt{2}}$. Without loss of generality, assume that the minimum is achieved for $b = 0$. Since the post-measurement state on the first $n-1$ qubits is $\sqrt{2}|\phi_0\rangle$ and $\left\|\left|\widetilde{\phi_0}\right\rangle - \sqrt{2}|\psi_0\rangle\right\| \leq \delta$. Finally, we note that $\sqrt{2}|\psi_0\rangle = (I_2^{\otimes n-1} \otimes \langle 0|)|\psi\rangle = \sum_{i=1}^M c_i (I_2^{\otimes n-1} \otimes \langle 0|)|s_i\rangle$, which is a linear combination of at most M stabilizer states. This proves that $\chi_\delta(\left|\widetilde{\phi_0}\right\rangle) \leq M$ as desired. □

Proof of Lemma 3.6. We replace each T gate in the circuit with the gadget introduced in [19] as in Fig. 1. We index $n+k-i+1$ the second qubit in the gadget corresponding to the i^{th} T gate in V and denote by $x_i \in \{0,1\}$ the output of the measurement in that gadget. We note that $x = (x_1, \cdots, x_k)$ has uniform distribution over $\{0,1\}^k$ by Lemma 3.7. We can formally express the equivalence of gadget-based implementation of as

$$V|0^n\rangle = 2^{k/2} C_k^{x_k} (I_2^{\otimes n} \otimes \langle x_k|) C_{k-1}^{x_{k-1}} (I_2^{\otimes n+1} \otimes \langle x_{k-1}|) \cdots C_1^{x_1} (I_2^{\otimes n+k-1} \otimes \langle x_1|) C_0 |0^n\rangle \otimes |T\rangle^{\otimes k}. \tag{32}$$

where C_i^b is a Clifford circuit acting on $n+k-i$ first qubits for all $b \in \{0,1\}$ and $i \in [n]$. In the beginning, $\chi_\delta(|0^n\rangle \otimes |T\rangle^{\otimes k}) = \chi_\delta(|T\rangle^{\otimes k})$. By Lemma 3.8, at each measurement, the approximate stabilizer rank does not increase for one output. As approximate stabilizer rank is invariant under Clifford operations, we conclude that for one particular choice of $x_1, \cdots, x_n$

$$\begin{aligned}\chi_\delta(|T\rangle^{\otimes k}) &\geq \chi_\delta(2^{k/2} C_k^{x_k} (I_2^{\otimes n} \otimes \langle x_k|) C_{k-1}^{x_{k-1}} (I_2^{\otimes n+1} \otimes \langle x_{k-1}|) \cdots \\ &\quad \cdots C_1^{x_1} (I^{\otimes n+k-1} \otimes \langle x_1|) C_0 |0^n\rangle \otimes |T\rangle^{\otimes k}) \\ &= \chi_\delta(V|0^n\rangle).\end{aligned} \tag{33}$$

□

3.4 Concluding the Proof of Theorem 3.1

Let cn for constant $c > 0$ be the linear term in the statement of Lemma 3.5 and C be the constant in the statement of Lemma 3.2. Given a positive integer m, we choose the largest n such that $cn2^{n/2} \leq m$. By Lemma 3.2, there exists n-qubit state $|\phi\rangle$ with $\chi_{\delta+4^{-n}}(|\phi\rangle) \geq C\frac{(1-(\delta+4^{-n})^2)^2 2^n}{n^2}$ when $n \geq 2\log\frac{1}{1-(\delta+4^{-n})^2} + 9 = O(1)$. According to Lemma 3.5 and our assumption that $cn2^{n/2} \leq m$, there exists a quantum circuit consisting of Clifford gates and at most m number of T gates such that $\||\phi\rangle|0^\lambda\rangle - V(|0^n\rangle|0^\lambda\rangle)\| \leq 4^{-n}$ for some $\lambda > 0$. Using Lemma 3.6, we have

$$\chi_\delta(|T\rangle^{\otimes m}) \geq \chi_\delta(V|0^{n+\lambda}\rangle) \geq \chi_{\delta+4^{-n}}(|\phi\rangle) \geq C\frac{(1-(\delta+4^{-n})^2)^2 2^n}{n^2}. \tag{34}$$

Since n was largest integer such that $cn2^{n/2} \leq m$, we have $m < \sqrt{2}c(n+1)2^{n/2}$. Furthermore, we have $2^{n/2} \leq cn2^{n/2} \leq m$ and therefore $n \leq 2\log(m)$. Combining these two inequalities, we obtain that $2^n > \frac{m}{\sqrt{2}c(2\log m+1)}$. Hence, substituting n and 2^n, we get

$$C\frac{(1-(\delta+4^{-n})^2)^2 2^n}{n^2} > C\frac{(1-(\delta+\frac{4c^4(1+2\log m)}{m^2})^2)^2}{8c^2(1+2\log m)^2\log^2 m} m^2 \tag{35}$$

$$= \Omega\left(\frac{(1-\delta^2)^2 m^2}{\log^4 m}\right). \tag{36}$$

Remark 3.9. *We proved the result for a fixed δ. However, we highlight the proof works for a sequence $\{\delta_m\}_{m\geq 1}$ where $\delta_m \to 1$ slowing enough (e.g., $\delta_m = 1 - O(\frac{\log m}{m})$ is enough). More precisely, as long as our constraint $n \geq 2\log\frac{1}{1-(\delta_m+4^{-n})^2} + 9$ is consistent with our other constraint that $cn2^{n/2} \leq m$, our argument goes through.*

We conclude this section by stating a corollary of our proof techniques on the existence of quantum states with low circuit complexity but high approximate stabilizer rank.

Corollary 3.10. *Let δ, n, and M be fixed such that $M = O((1-\delta^2)^2 2^n n^{-2})$. Then, there exists a quantum circuit V consisting of $M\mathrm{poly}\log(M)$ gates such that $\chi_\delta(V|0^n\rangle) \geq M$.*

Proof. Let C be the constant in Lemma 3.2. We choose k the smallest integer such that $C(1-\delta^2)^2\frac{2^k}{k^2} \geq M$. By Lemma 3.2, there exists k qubit state $|\psi\rangle$ such that $\chi_\delta(|\psi\rangle) \geq M$. By [28, Theorem 3.3], there exists a quantum circuit V consisting of $O(k2^k) = M\mathrm{poly}\log(M)$ two-qubit gates such that $V|0^k\rangle = |\psi\rangle$. Then, $V \otimes I_2^{\otimes n-k}$ has the desired properties. □

4 APPROXIMATE STABILIZER RANK OF t-DESIGNS

This section discusses what happens if we replace the Haar measure in Lemma 3.2 with a t-design. Initially, we discuss whether we can expect a bound on the approximate stabilizer rank for t-designs. The following proposition shatters any such hope for $t = O(1)$. We omit the proofs; for detailed proofs, please refer to [35].

Proposition 4.1. *There exist absolute constants $C_1 > 0$ and $C_2 > 0$ such that for all t, $n \geq C_2 t^2$, and $1 > \epsilon > 0$, there exists an ϵ-approximate unitray t-design for n-qubits where the following holds. Then, $\chi_\delta(U|0^n\rangle) \leq 2^{C_1\log^2(t)(t^4+t\log(\frac{1}{\epsilon}))}$ with probability one, if U is sampled according to the t-design.*

This proposition together with Lemma 3.2 imply that when $t = O(1)$, the approximate stabilizer rank of a t-design can range from $O(1)$ to $\Omega(n^{-2}2^n)$. However, we provide a lower bound on the approximate rank when t grows with n using a similar approach as in the proof of Lemma 3.2.

Lemma 4.2. *If U is distributed according to an n-qubit ϵ-approximate t-design, then* $\Pr[\chi_\delta(U|0^n\rangle) \le M] \le e^{0.54n^2M}\frac{\left(\frac{M+t-1}{2^n+t-1}\right)^t+\epsilon}{(1-\delta^2)^t}$.

Next, we provide an upper bound on how many gates we need to get a state with approximate stabilizer rank $\mathrm{poly}(n)$. Perhaps surprisingly, the bound we obtain using t-designs is weaker than what we obtain from the Haar measure in Corollary 3.10.

Proposition 4.3. *Let $d \ge 1$ and $1 > \delta > 0$. There exists a quantum circuit V with $O(\log^5(n)n^{3+5d+\frac{3\sqrt{(d+1)}}{\sqrt{\log n}}})$ gates and $\chi_\delta(V|0^n\rangle) \ge n^d$.*

We finally comment on the possibility of using t-design to improve the lower bound on the approximate stabilizer of $|T\rangle^{\otimes m}$. Using Lemma 4.2, we should take $t = \Omega(Mn)$ for a state with approximate stabilizer state M. Assuming that Conjecture 2.8 is true, we need at least $\Omega(Mn)$ T-gates to construct such t-design. Therefore, using our approach, one cannot expect to get a lower bound better than linear on $\chi_\delta(|T\rangle^{\otimes m})$.

ACKNOWLEDGEMENTS

S. M. and M. T. acknowledge funding provided by NSF CCF-2013062. S. M. acknowledges funding by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NSF Grant PHY-1733907). We are grateful to Ryan Williams, Ulysse Chabaud, and Arsalan Motamedi for their insightful conversations. We thank the anonymous referee who spotted an error in Theorem 1.6, which was subsequently fixed.

A STABILIZERNESS MEASURES

Approximate and exact stabilizer ranks measure the closeness of a quantum state to the set of all stabilizer states. Other measures of stabilizerness have been studied in the literature that might be mathematically more tractable but are not operationally as relevant as stabilizer ranks. In this section, we review some of these measures and also suggest a novel one based on the Gowers norm [20] (See Definition A.1). Gowers norms are extensively studied in the context of higher-order Fourier analysis and have found several applications in different areas of mathematics and theoretical computer science [25, 47]. In particular, for a polynomial $P : \mathbb{F}_2^n \to \mathbb{F}_2$ of degree d, the Gowers norm of degree d of $(-1)^P$ is 1. Since stabilizer states are defined in terms of quadratic phases, the useful properties of Gowers norm could be exploited to study stabilizerness of arbitrary quantum states (See Remark A.2). Since some of these measures are easier to deal with, it is interesting to ask if a bound on one measure implies any bound on other measures. As an example, we prove a relation between stabilizer fidelity and stabilizer rank (Proposition A.3), which immediately implies a linear lower-bound on $\chi(|T\rangle^{\otimes n})$ using the results of [9] (Corollary A.4). We summarize other relations in Table 1 that exist in literature.

Definition A.1 (Stabilizerness measures)**.** *Consider the n-qubit state $|\phi\rangle = \frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n} f(x)|x\rangle$. We consider the following quantities.*

(1) Stabilizer fidelity: $F(|\phi\rangle) = \max_{|s\rangle\in\mathrm{Stab}_n}|\langle s|\phi\rangle|^2$

(2) Stabilizer extent:

$$\xi(\phi) = \inf\{\|c\|_1^2 : c \in \mathbb{C}^M : \exists\, |s_1\rangle, \cdots, |s_M\rangle \in \mathrm{Stab}_n : |\phi\rangle = \sum_{i=1}^M c_i|s_i\rangle\}. \tag{37}$$

(3) Stabilizer rank $\chi(|\phi\rangle)$ and approximate stabilizer rank $\chi_\delta(|\phi\rangle)$ as defined in Section 2.2.

(4) Gowers norm:

$$\||\phi\rangle\|_{U^3}^8 = \frac{1}{16^n}\sum_{x,h_1,h_2,h_3\in\mathbb{F}_2^n} f(x)\overline{f(x+h_1)f(x+h_2)f(x+h_3)} \times f(x+h_1+h_2)f(x+h_1+h_3)f(x+h_2+h_3)\overline{f(x+h_1+h_2+h_3)}. \tag{38}$$

Remark A.2. *We believe that Gowers norm $\||\phi\rangle\|_{U^3}$ is a relevant measure of stabilizerness because of its relation with the overlap of a function with quadratic phase functions [25, Theorem 5.3]. In particular, let $\||\phi\rangle\|_{U^3} = \delta$. Then, the direct part of [25, Theorem 5.3] implies that for any stabilizer state $|s\rangle$ such that $\langle s|x\rangle \ne 0$ for all $x \in \mathbb{F}_2^n$, we have $|\langle s|\phi\rangle| \le \delta$. Furthermore, the converse part of [25, Theorem 5.3] implies that there exists a stabilizer state $|s\rangle$ such that $|\langle s|\phi\rangle| \ge 2^{-c\log^4\frac{1}{\delta}}$ for a universal constant $c > 0$. While the direct and converse theorems do not match, $\||\phi\rangle\|_{U^3}$ has a closed expression unlike $F(|\phi\rangle)$.*

In the following proposition, we, establish a relation between $F(|\phi\rangle)$ and $\chi(|\phi\rangle)$. We closely follow the proof approach of [30], but we manage to avoid any tools from the higher-order Fourier analysis.

Proposition A.3. *For any n-qubit state $|\phi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{F}_2^n} f(x)|x\rangle$, we have $\chi(|\phi\rangle) \ge \frac{2}{3}\log\left(\frac{\alpha^2}{\beta\sqrt{F(|\phi\rangle)}}\right)$ where $\alpha := \min_{x\in\mathbb{F}_2^n}|f(x)|$ and $\beta := \max_{x\in\mathbb{F}_2^n}|f(x)|$.*

Before starting the proof, we briefly review the setup for (classical) Fourier analysis here. Let G be any finite Abelian group. A character for G is a function $\gamma : G \to \mathbb{C}$ such that $\gamma(g+h) = \gamma(g)\gamma(h)$. We denote the set of all characters by $\widehat{G}$, which is finite and of the same cardinality as G. For any function $f : G \to \mathbb{C}$, there exists a unique function $\widehat{f} : \widehat{G} \to \mathbb{C}$ such that $f = \sum_{\gamma\in\widehat{G}}\widehat{f}(\gamma)\gamma$. Using Parseval equality and Cauchy-Schwartz inequality, we have $\sum_{\gamma\in\widehat{G}}|\widehat{f}(\gamma)| \le \sqrt{|G|}\max_{g\in G}|f(g)|$.

Let G_1 and G_2 be two finite Abelian groups. We have $\widehat{G_1\times G_2} = \{\gamma_1\gamma_2 : \gamma_1 \in \widehat{G_1}, \gamma_2 \in \widehat{G_2}\}$. Finally, consider the group $G = \{\pm1, \pm i\}$ under multiplication. Then, $\widehat{G} \cong \mathbb{Z}_4$ and the characters are $x \mapsto x^i$ for $i \in \mathbb{Z}_4$.

Proof of Proposition A.3. We define the set of functions $\mathbb{F}_2^n \to \mathbb{C}$ of the form $x \mapsto i^{\ell(x)}(-1)^{Q(x)}$ for ℓ linear and Q quadratic as $\mathcal{Q}$, which is closed under function multiplication. Let $\chi_\delta(|\phi\rangle) = M$, i.e., there exist $c_1, \cdots, c_M \in \mathbb{C}$, $A_1, \cdots, A_M \subset \mathbb{F}_2^n$ affine subspaces, $Q_1, \cdots, Q_M \in \mathcal{Q}$ such that $f = \sum_{i=1}^M c_iQ_i1_{A_i}$. We recursively construct an affine subspace $U \subset \mathbb{F}_2^n$ with dimension at least $n-M$ such that 1_{A_i} is constant on U for all i. (This is a minor improvement to

Table 1: Known relations among measures of stabilizerness.

	$\xi(\|\phi\rangle)$	$\chi(\|\phi\rangle)$	$\chi_\delta(\phi)$	$\|\|\|\phi\rangle\|\|_{U_3}$
$F(\|\phi\rangle)$	$\zeta(\|\phi\rangle) = \sup_{\|\omega\rangle} \frac{\|\langle\phi\|\omega\rangle\|^2}{F(\|\omega\rangle)}$ [9, Theorem 4]	Proposition A.3 See also [30]	Open question	Remark A.2 [45]
$\xi(\|\phi\rangle)$		Open question	[9, Theorem 1]	Open question
$\chi(\|\phi\rangle)$	Open question		Lemma A.5 [32, Lemma 3.5]	Open question

Claim 3.3 in [40].). Start with $U_0 = \mathbb{F}_2^n$. For each $i \in [M]$ let U_{i-1} be given such that $1_{A_1}, \cdots, 1_{A_{i-1}}$ are constant on U_{i-1}. If $U_{i-1} \subset A_i$, then take $U_i = U_{i-1}$ and 1_{A_i} is one on U_i. Otherwise, there is a subspace U_i of U_{i-1} with codimension one such that $U_{i-1} \cap A_i =$, i.e., $\mathbb{1}_{A_i}$ is zero on U_i (and since $U_i \subset U_{i-1}$, $1_{A_1}, \cdots, 1_{A_{i-1}}$ are constant on U_i too). We take $U = U_M$, which has a dimension at least $n - M$ because the dimension of U_0 is n, and in each step, the dimension is decreased at most by one.

Upon defining $S \coloneqq \{i \in [M] : 1_{A_i}|_U = 1\}$, we have $f|_U = \sum_{i\in S} c_i Q_i|_U$. Define $G = \{\pm 1, \pm i\}$, which is a group under multiplication. We also define

$$h : U \to G^S \quad x \mapsto (Q_i(x))_{i\in S} \tag{39}$$

$$\Gamma : G^S \to \mathbb{C} \quad y \mapsto \begin{cases} \sum_{i\in S} c_i y_i & y \in \mathrm{Im}(h) \\ 0 & \text{Otherwise} \end{cases} \tag{40}$$

for which $f(x) = \Gamma(h(x))\ \forall x \in U$. Using our discussion before the proof about Fourier analysis of G^S, we can write $\Gamma = \sum_{\gamma\in\mathbb{Z}_4^S} \widehat{\Gamma}(\gamma)\gamma$ and $f(x) = \sum_{\gamma\in\mathbb{Z}_4^S} \widehat{\Gamma}(\gamma) Q_\gamma(x)$, $\forall x \in U$ where $Q_\gamma \coloneqq \prod_{i\in S} Q_i^{\gamma_i} \in \boldsymbol{Q}$. Therefore,

$$\frac{1}{|U|}\sum_{x\in U}|f(x)|^2 = \sum_{i\in S}\widehat{\Gamma}(\gamma)\frac{1}{|U|}\sum_{x\in U} Q_\gamma(x)\overline{f(x)}. \tag{41}$$

We consider the stabilizer state $|s_\gamma\rangle \coloneqq \frac{1}{\sqrt{|U|}}\sum_{x\in U} Q_\gamma(x)\,|x\rangle$. It holds that

$$\langle\phi|s_\gamma\rangle = \frac{1}{\sqrt{|U|2^n}}\sum_{x\in U} Q_\gamma(x)\overline{f(x)}. \tag{42}$$

Combining (41) and (42), we obtain

$$\frac{1}{|U|}\sum_x |f(x)|^2 = \sum_{i\in S}\widehat{\Gamma}(\gamma)\sqrt{\frac{2^n}{|U|}}\langle\phi|s_\gamma\rangle,$$

which we can upper bound by

$$\begin{aligned}(\sum_\gamma |\widehat{\Gamma}(\gamma)|)\sqrt{\frac{2^n F(|\phi\rangle)}{|U|}} &\le 2^{|S|}\max_{y\in G^S}|\Gamma(y)|\sqrt{\frac{2^n F(|\phi\rangle)}{|U|}} \\ &\le 2^{|S|}\beta\sqrt{\frac{2^n F(|\phi\rangle)}{|U|}} \le 2^M\beta\sqrt{\frac{F(|\phi\rangle)}{2^M}}.\end{aligned} \tag{43}$$

Combining the above inequality with $\frac{1}{|U|}\sum_x |f(x)|^2 \ge \alpha^2$ completes the proof. □

Proposition A.3 immediately implies a linear lower bound on exact stabilizer rank of $|T\rangle^{\otimes m}$ using $F(|T\rangle^{\otimes m}) = \cos(\frac{\pi}{8})^{2m}$ [9].

Corollary A.4. *We have* $\chi(|T\rangle^{\otimes m}) \ge \frac{2}{3}\log\left(\frac{1}{\cos(\frac{\pi}{8})}\right)m > 0.076m$.

The next lemma shows that we cannot, in general, control the gap between approximate and exact rank.

Lemma A.5. *Let* $1 > \delta > 0$, *n, and M be given such that* $1 \le M \le 2^n$. *Then, there are two n-qubit quantum states* $|\phi_1\rangle$ *and* $|\phi_2\rangle$ *such that* $\chi(|\phi_1\rangle) = \chi(|\phi_2\rangle) = \Theta(M)$, $\chi_\delta(|\phi_1\rangle) = \Omega\left(\frac{M}{\log^2 M}\right)$ *and* $\chi_\delta(|\phi_2\rangle) = O(1)$.

Proof. Let k be the smallest integer such that $2^k \ge M$. By Lemma 3.2, there exists a k qubit state $|\psi_1\rangle$ such that $\chi_\delta(|\psi_1\rangle) = \Omega(\frac{2^k}{k^2})$. Furthermore, by a probabilistic argument, we can further assume that $\chi_\delta(|\psi_1\rangle) = 2^k$. Taking $|\phi_1\rangle = |\psi_1\rangle\otimes|0\rangle^{\otimes n-k}$ has the desired property. Next, using the same argument and [32, Lemma 3.5] implies the existence of $|\phi_2\rangle$. □

REFERENCES

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

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

[3] Scott Aaronson and Daniel Gottesman. 2004. Improved simulation of stabilizer circuits. *Physical Review A* 70, 5 (2004), 052328.

[4] Noga Alon and Ravi B Boppana. 1987. The monotone circuit complexity of Boolean functions. *Combinatorica* 7 (1987), 1–22.

[5] Stephen D Bartlett, Barry C Sanders, Samuel L Braunstein, and Kae Nemoto. 2002. Efficient classical simulation of continuous variable quantum information processes. *Physical Review Letters* 88, 9 (2002), 097904.

[6] Bela Bauer, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Chan. 2020. Quantum Algorithms for Quantum Chemistry and Quantum Materials Science. *Chemical Reviews* 120, 22 (Nov 2020), 12685–12717. https://doi.org/10.1021/acs.chemrev.9b00829

[7] Adam Bouland, Joseph F Fitzsimons, and Dax Enshan Koh. 2017. Complexity classification of conjugated Clifford circuits. *arXiv preprint arXiv:1709.01805* (2017).

[8] Fernando G. S. L. Brandao, Aram W. Harrow, and Michal Horodecki. 2016. Local Random Quantum Circuits are Approximate Polynomial-Designs. *Communications in Mathematical Physics* 346, 2 (Sep 2016), 397–434. https://doi.org/10.1007/s00220-016-2706-8

[9] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. 2019. Simulation of quantum circuits by low-rank stabilizer decompositions. *Quantum* 3 (Sep 2019), 181. https://doi.org/10.22331/q-2019-09-02-181

[10] Sergey Bravyi and David Gosset. 2016. Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates. *Physical Review Letters* 116, 25 (Jun 2016), 250501. https://doi.org/10.1103/PhysRevLett.116.250501

[11] Sergey Bravyi, Graeme Smith, and John A. Smolin. 2016. Trading Classical and Quantum Computational Resources. *Physical Review X* 6, 2 (Jun 2016), 021043. https://doi.org/10.1103/PhysRevX.6.021043

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

[13] A Robert Calderbank and Peter W Shor. 1996. Good quantum error-correcting codes exist. *Physical Review A* 54, 2 (1996), 1098.

[14] Lijie Chen and R Ryan Williams. 2019. Stronger connections between circuit analysis and circuit lower bounds, via PCPs of proximity. In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[15] A. Einstein, B. Podolsky, and N. Rosen. 1935. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review* 47, 10 (May 1935), 777–780. https://doi.org/10.1103/PhysRev.47.777

[16] Richard P. Feynman. 1982. Simulating physics with computers. *International Journal of Theoretical Physics* 21, 6–7 (Jun 1982), 467–488. https://doi.org/10.1007/BF02650179

[17] Yuval Filmus, Hamed Hatami, Steven Heilman, Elchanan Mossel, Ryan O'Donnell, Sushant Sachdeva, Andrew Wan, and Karl Wimmer. 2014. Real analysis in computer science: A collection of open problems. *Preprint available at https://simons. berkeley. edu/sites/default/files/openprobsmerged. pdf* (2014).

[18] Daniel Gottesman. 1998. The Heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006* (1998).

[19] Daniel Gottesman and Isaac L. Chuang. 1999. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* 402, 6760 (Nov 1999), 390–393. https://doi.org/10.1038/46503

[20] W.T. Gowers. 2001. A new proof of Szemerédi's theorem. *GAFA Geometric And Functional Analysis* 11, 3 (Aug 2001), 465–588. https://doi.org/10.1007/s00039-001-0332-9

[21] Lov K. Grover. 1997. Quantum Computers Can Search Arbitrarily Large Databases by a Single Query. *Phys. Rev. Lett.* 79 (Dec 1997), 4709–4712. Issue 23. https://doi.org/10.1103/PhysRevLett.79.4709

[22] Jonas Haferkamp. 2022. Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$. *Quantum* 6 (Sept. 2022), 795. https://doi.org/10.22331/q-2022-09-08-795

[23] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth. 2023. Efficient Unitary Designs with a System-Size Independent Number of Non-Clifford Gates. *Communications in Mathematical Physics* 397, 3 (Feb 2023), 995–1041. https://doi.org/10.1007/s00220-022-04507-6

[24] Aram W. Harrow and Richard A. Low. 2009. Random Quantum Circuits are Approximate 2-designs. *Communications in Mathematical Physics* 291, 1 (Oct 2009), 257–302. https://doi.org/10.1007/s00220-009-0873-6

[25] Hamed Hatami, Pooya Hatami, Shachar Lovett, et al. 2019. Higher-order fourier analysis and applications. *Foundations and Trends® in Theoretical Computer Science* 13, 4 (2019), 247–448.

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

[27] R. Jozsa. 2001. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science & Engineering* 3, 2 (2001), 34–43. https://doi.org/10.1109/5992.909000

[28] E. Knill. 1995. Approximation by Quantum Circuits. arXiv:quant-ph/9508006 [quant-ph]

[29] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. 2008. Randomized benchmarking of quantum gates. *Phys. Rev. A* 77 (Jan 2008), 012307. Issue 1. https://doi.org/10.1103/PhysRevA.77.012307

[30] Farrokh Labib. 2022. Stabilizer rank and higher-order Fourier analysis. *Quantum* 6 (Feb. 2022), 645. https://doi.org/10.22331/q-2022-02-09-645

[31] Zi-Wen Liu and Andreas Winter. 2022. Many-Body Quantum Magic. *PRX Quantum* 3 (May 2022), 020333. Issue 2. https://doi.org/10.1103/PRXQuantum.3.020333

[32] Benjamin Lovitz and Vincent Steffan. 2022. New techniques for bounding stabilizer rank. *Quantum* 6 (April 2022), 692. https://doi.org/10.22331/q-2022-04-20-692

[33] Guang Hao Low, Vadym Kliuchnikov, and Luke Schaeffer. 2018. Trading T-gates for dirty qubits in state preparation and unitary synthesis. *arXiv preprint arXiv:1812.00954* (2018).

[34] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C. Benjamin, and Xiao Yuan. 2020. Quantum computational chemistry. *Rev. Mod. Phys.* 92 (Mar 2020), 015003. Issue 1. https://doi.org/10.1103/RevModPhys.92.015003

[35] Saeed Mehraban and Mehrdad Tahmasbi. 2023. Lower bounds on the approximate stabilizer rank: A probabilistic approach. *arXiv preprint arXiv:2305.10277* (2023).

[36] Yoshifumi Nakata, Christoph Hirche, Masato Koashi, and Andreas Winter. 2017. Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics. *Physical Review X* 7, 2 (Apr 2017), 021006. https://doi.org/10.1103/PhysRevX.7.021006

[37] John C Napp, Rolando L La Placa, Alexander M Dalzell, Fernando GSL Brandao, and Aram W Harrow. 2022. Efficient classical simulation of random shallow 2D quantum circuits. *Physical Review X* 12, 2 (2022), 021021.

[38] Michael A. Nielsen and Isaac L. Chuang. 2012. *Quantum Computation and Quantum Information*. Cambridge University Press. https://doi.org/10.1017/cbo9780511976667

[39] Tobias J Osborne. 2007. Simulating adiabatic evolution of gapped spin systems. *Physical review a* 75, 3 (2007), 032321.

[40] Shir Peleg, Amir Shpilka, and Ben Lee Volk. 2022. Lower Bounds on Stabilizer Rank. *Quantum* 6 (Feb. 2022), 652. https://doi.org/10.22331/q-2022-02-15-652

[41] Robert Raussendorf and Hans J. Briegel. 2000. Quantum computing via measurements only. arXiv:quant-ph/0010033 [quant-ph]

[42] AA Razborov. 1985. A lower bound on the monotone network complexity of the logical permanent Mat.

[43] Alexander Razborov. 1985. Lower bounds on the monotone complexity of some Boolean function. In *Soviet Math. Dokl.*, Vol. 31. 354–357.

[44] Oded Regev. 2009. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)* 56, 6 (2009), 1–40.

[45] Alex Samorodnitsky. 2007. Low-degree tests at large distances. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*. 506–515.

[46] Peter W Shor. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 41, 2 (1999), 303–332.

[47] Terence Tao. 2012. *Higher order Fourier analysis*. Vol. 142. American Mathematical Soc.

[48] Leslie G Valiant. 2001. Quantum computers that can be simulated classically in polynomial time. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. 114–123.

[49] M. Van Den Nest. 2010. Classical simulation of quantum computation, the gottesman-Knill theorem, and slightly beyond. *Quantum Information and Computation* 10, 3 & 4 (Mar 2010), 258–271. https://doi.org/10.26421/QIC10.3-4-6

[50] Guifré Vidal. 2008. Class of quantum many-body states that can be efficiently simulated. *Physical review letters* 101, 11 (2008), 110501.

[51] John Watrous. 2018. *The theory of quantum information*. Cambridge university press.

[52] Steven Weinberg. 2015. *Lectures on quantum mechanics*. Cambridge University Press.

[53] Richard Ryan Williams. 2018. Limits on representing boolean functions by linear combinations of simple functions: thresholds, reLUs, and low-degree polynomials. In *Proceedings of the 33rd Computational Complexity Conference*. 1–24.

Received 12-NOV-2023; accepted 2024-02-11