

Stabilizer rank and higher-order Fourier analysis

Farrokh Labib

CWI, QuSoft, Science Park 123, 1098 XG Amsterdam, Netherlands. Supported by the Gravitation-grant NETWORKS-024.002.003 from the Dutch Research Council (NWO).

We establish a link between stabilizer states, stabilizer rank and higher-order Fourier analysis—a still-developing area of mathematics that grew out of Gowers’s celebrated Fourier-analytic proof of Szemerédi’s theorem [10]. We observe that n -qudit stabilizer states are so-called *nonclassical quadratic phase functions* (defined on affine subspaces of \mathbb{F}_p^n where p is the dimension of the qudit) which are fundamental objects in higher-order Fourier analysis. This allows us to import tools from this theory to analyze the stabilizer rank of quantum states. Quite recently, in [20] it was shown that the n -qubit magic state has stabilizer rank $\Omega(n)$. Here we show that the qudit analogue of the n -qubit magic state has stabilizer rank $\Omega(n)$, generalizing their result to qudits of any prime dimension. Our proof techniques use explicitly tools from higher-order Fourier analysis. We believe this example motivates the further exploration of applications of higher-order Fourier analysis in quantum information theory.

1 Introduction

The Gottesman-Knill Theorem [9, 18] states that any quantum circuit consisting of Clifford gates can be efficiently classically simulated. The Clifford group on n qubits is generated by the Hadamard gate H , the $\pi/4$ phase gate S and the entangling CNOT gate. In particular, this means that circuits consisting only of Clifford gates cannot provide computational advantage over classical computers. We can promote such circuits to universal quantum computers by having access to a non-Clifford gate or (equivalently) a “magic state” [3]. It is widely believed that universal quantum computers cannot be efficiently simulated by classical computers: state-of-the-art simulators using modern day supercomputers are only able to simulate a few dozens of qubits [6, 12, 19, 22]. So it has to be this magic state that fuels the computational hardness of simulation by classical computers. It is therefore important to understand how much this resource costs in terms of free (efficiently simulatable) resources. These costs are quantified by “measures of magic” [16] an example of which is *stabilizer rank*, first introduced in [4]. Here, the free resources are states obtained from the canonical all-zero state by applying only Clifford operations, which are the well-known stabilizer states. To increase our understanding of non-stabilizerness, or the amount of “magic” a quantum state has, a valid approach might be to find a different characterization of these objects. This might introduce new techniques in analyzing measures of magic. It is well known that stabilizer states are quadratic forms defined on affine subspaces [7, 11, 14]. Here we observe that these objects are so-called *nonclassical quadratic phase functions* defined on affine subspaces which are well-studied objects in

Farrokh Labib: farrokhlabib@gmail.com

higher-order Fourier analysis.

Higher-order Fourier analysis, a still nascent area of mathematics, grew out of a Fourier-analytic proof of Szemerédi’s Theorem [23] by Gowers [10]. Whereas in Fourier analysis one studies how functions correlate with characters, in higher-order Fourier analysis one studies correlations with functions that resemble polynomials (where characters correspond to linear functions). These polynomial-like functions are known as *polynomial phase functions*.

It turns out that Boolean functions giving the (unnormalised) amplitudes of graph states are examples of quadratic phase functions. In general, quadratic phase functions can be defined using “multiplicative derivatives”: for $h \in \mathbb{F}_2^n$, the multiplicative derivative of $f: \mathbb{F}_2^n \rightarrow \mathbb{C}$ in direction h is

$$\Delta_h f(x) := f(x+h)\overline{f(x)}.$$

Nonclassical polynomial phase functions of degree d are those functions that are constant after taking $d+1$ multiplicative derivatives. It is not difficult to check that graph states, whose amplitude function always has the form $f(x) = (-1)^{q(x)}$ where q is a quadratic polynomial, satisfies this property with $d=2$. These are referred to as the *classical* quadratic phase functions. However, the nonclassical quadratic phase functions are not exhausted by these examples. It turns out that stabilizer states correspond to functions in this broader class. This establishes a surprising link between higher-order Fourier analysis and quantum information theory. It was shown in [7] (see also [2]) that stabilizer states are *quadratic forms* taking values in \mathbb{Z}_8 defined on affine subspaces. We will see that they are nonclassical quadratic phase function on affine subspaces.

Let p be an odd prime and consider qudits of dimension p . Then, the amplitudes of n -qudit stabilizer states are also quadratic phase functions defined on affine subspaces of \mathbb{F}_p^n [14], see also [11]. It is interesting to note that for primes $p > 2$ the n -qudit stabilizer states are given by classical quadratic polynomials while there are no nonclassical polynomials of degree two, contrary to the case $p=2$.

Stabilizer rank. *Stabilizer rank* is a measure of magic which was recently extensively analysed by Bravyi et al. [5]. The stabilizer rank of a quantum state $|\psi\rangle$, denoted $\chi(|\psi\rangle)$, is the minimal number r such that $|\psi\rangle$ can be written as a linear combination of r stabilizer states. As is well known, any circuit \mathcal{C} consisting of Clifford gates and n copies of the T -gate, given by $|0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$, can be implemented using Clifford operations on the n -qubit magic state $|T\rangle^{\otimes n}$, where $|T\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$. Then, the stabilizer rank of $|T\rangle^{\otimes n}$ upper bounds the simulation cost of the circuit \mathcal{C} . Bravyi, Smith and Smolin [4] showed that the stabilizer rank of the n -qubit magic state is $\Omega(\sqrt{n})$. Very recently Peleg, Shpilka and Volk [20] showed a lower bound of $\Omega(n)$ for the stabilizer rank of the n -qubit magic state, which is a quadratic improvement. Here we give the same lower bound but generalize to qudits of any prime dimension.

Adding any non-Clifford gate to the Clifford gate set could in principle promote it to universal quantum computation. However, we use the generalization of the T gate for qudits from [15]. Let us call this gate U and define $|+\rangle := \frac{|0\rangle + |1\rangle + \dots + |p-1\rangle}{\sqrt{p}}$. Then, the single qudit magic state over \mathbb{F}_p is defined to be

$$|\psi_U\rangle = U|+\rangle.$$

Our main result is the following.

Theorem 1.1. *Let p be any prime and let $|\psi_U\rangle^{\otimes n}$ be the n -qudit magic state over \mathbb{F}_p . We have that $\chi(|\psi_U\rangle^{\otimes n}) \geq \Omega(n)$.*

This result generalizes [20], but our techniques are completely different and use explicitly tools from higher-order Fourier analysis. Roughly speaking, we show that the function giving the amplitudes of the n -qudit magic state is a cubic nonclassical polynomial phase function for which the polynomial “in the phase” has high rank (see Definition 3.9). We then prove that the lower bound for this rank is also a lower bound for the stabilizer rank. In this step we use a lemma from [20] (Claim 3.3 in that paper) to get a handle on the affine subspaces that appear from the stabilizer states. Apart from this lemma, the techniques are different.

We think that the techniques used here might pave the way to super-linear lower bounds for decompositions in terms of stabilizer states defined on the full space \mathbb{F}_p^n .

Higher-order Fourier analysis and quantum information theory. We believe that the application we found motivate the further study of tools in higher-order Fourier analysis in quantum information theory. A work that connected to this area is [1], where the “Gowers Inverse Theorem” is utilised to analyze certain Bell inequalities. This current work is yet another example.

Higher-order Fourier analysis has already found many applications in classical theoretical computer science, such as in property testing, coding theory and complexity theory [13]. In analogy with analysis of Boolean functions, we hope that higher-order Fourier analysis proves equally useful in quantum information theory.

Acknowledgements I would like to thank Jop Briët for his guidance and many fruitful discussions in this project. Also thanks to Michael Walter for the fruitful discussions on stabilizer and magic states in odd prime dimension.

2 Preliminaries

For a finite non-empty set S , we write $\mathbb{E}_{s \in S}$ to mean $\frac{1}{|S|} \sum_{s \in S}$. Let p be a prime. We denote by \mathbb{F}_p the field of p elements, $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and \mathbb{Z}_n is the ring of integers mod n .

Let $|\cdot|: \mathbb{F}_p \rightarrow \{0, 1, \dots, p-1\}$ be the natural map. This map has the property that for $a, b \in \mathbb{F}_2$,

$$|a + b| = |a| + |b| - 2|ab|. \quad (1)$$

And for $a, b \in \mathbb{F}_3$,

$$|a + b| = |a| + |b| + 3(|a^2b| + |ab^2|) - 6|ab| \pmod{9}. \quad (2)$$

We also define $|\cdot|: \mathbb{F}_p^n \rightarrow \mathbb{Z}_{\geq 0} : x \mapsto |x_1| + \dots + |x_n|$, this is an abuse of notation, but it should be clear from context what the domain of the map $|\cdot|$ is. Define ι to be the map given by

$$\iota: \mathbb{F}_p \rightarrow \mathbb{T}: x \mapsto |x|/p \pmod{1}.$$

The exponential map $e: \mathbb{T} \rightarrow \mathbb{C}$ is defined $e(t) := e^{2\pi it}$.

For an affine subspace $H \subset \mathbb{F}_p^n$, we write $H = L(H) + v$ for some vector $v \in \mathbb{F}_p^n$ and a linear subspace $L(H)$. The vector v is not unique, but $L(H)$ is uniquely determined by H , namely $L(H) = \{x - y: x, y \in H\}$.

Let G be an abelian group, $H \subset \mathbb{F}_p^n$ an affine subspace and $P: H \rightarrow G$ a map. The additive derivative Δ_h is defined to be $\Delta_h P(x) := P(x+h) - P(x)$, where $h \in L(H)$ and $x \in H$.

For a subset $A \subset \mathbb{F}_p^n$, write $1_A: \mathbb{F}_p^n \rightarrow \{0,1\}$ for the indicator function of A , i.e. $1_A(x) = 1$ if $x \in A$ and 0 otherwise.

We also need some basic definitions for the Fourier transform. Let $\omega_p := e^{2\pi i/p}$. For functions $f, g: \mathbb{F}_p^n \rightarrow \mathbb{C}$, their inner product is defined by

$$\langle f, g \rangle := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \overline{g(x)} = p^{-n} \sum_{x \in \mathbb{F}_p^n} f(x) \overline{g(x)}.$$

Denote by \hat{f} the Fourier transform of f , i.e.

$$\hat{f}(\alpha) = \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \omega_p^{\langle \alpha, x \rangle}, \quad \alpha \in \mathbb{F}_p^n.$$

The inner product for the Fourier transforms is defined by

$$\langle \hat{f}, \hat{g} \rangle = \sum_{\alpha \in \mathbb{F}_p^n} \hat{f}(\alpha) \overline{\hat{g}(\alpha)}.$$

Using this definition, Parseval's theorem becomes

$$\langle f, g \rangle = \langle \hat{f}, \hat{g} \rangle.$$

3 Techniques

In this section, we introduce all the definitions necessary for the proof of our main result. Our main result generalizes the recent result of [20], but we use completely different techniques that we explain here as well.

3.1 Stabilizer states

In [2], a succinct representation of an n -qubit stabilizer states is given in terms of quadratic forms on affine subspaces of \mathbb{F}_2^n . For this, they introduced the following definition.

Definition 3.1. *For an affine subspace $H \subset \mathbb{F}_2^n$, a map $Q: H \rightarrow \frac{1}{8}\mathbb{Z}/\mathbb{Z}$ is called a quadratic form if $\Delta_{h_1} \Delta_{h_2} Q(x)$ is independent of $x \in H$ for all $h_1, h_2 \in L(H)$.*

Theorem 3.2 ([2]). *For any n -qubit stabilizer state $|\phi\rangle$, there exists a unique affine subspace $H \subset \mathbb{F}_2^n$ and a quadratic form $Q: H \rightarrow \frac{1}{8}\mathbb{Z}/\mathbb{Z}$ such that*

$$|\phi\rangle = 2^{-\dim H/2} \sum_{x \in H} e(Q(x)) |x\rangle. \quad (3)$$

In [2] quadratic forms are considered that are maps $Q: H \rightarrow \frac{1}{8}\mathbb{Z}/\mathbb{Z}$. We will show that the only way that such a map has the property $\Delta_{h_1} \Delta_{h_2} Q(x)$ being independent of $x \in H$ for all $h_1, h_2 \in L(H)$, is if Q actually take values in $\frac{1}{4}\mathbb{Z}/\mathbb{Z} \subset \frac{1}{8}\mathbb{Z}/\mathbb{Z}$. We will also see that such functions are known as *nonclassical* polynomials of degree two in the literature of higher-order Fourier analysis. Making this explicit link with higher-order Fourier analysis allows us to import tools from that theory to use in lower bounding the stabilizer rank of quantum states.

Next, qudit stabilizer states where the dimension of the qudit is an odd prime p are somewhat simpler as they are given by quadratic polynomials taking values in \mathbb{F}_p on affine subspaces in \mathbb{F}_p^n . Let $\omega_p = e^{2\pi i/p}$ be a p -th root of unity. A map $Q: H \rightarrow \mathbb{F}_p$ is a quadratic polynomial on an affine subspace $H \subset \mathbb{F}_p^n$ if $\Delta_{h_1}\Delta_{h_2}Q(x)$ is independent of $x \in H$ for all $h_1, h_2 \in L(H)$.

Theorem 3.3 ([14], see also [11]). *Let p be an odd prime and $|\phi\rangle$ an n -qudit stabilizer state where the dimension of the qudit is p . Then, there is an affine subspace $H \subset \mathbb{F}_p^n$ and a quadratic polynomial $Q: H \rightarrow \mathbb{F}_p$ such that*

$$|\phi\rangle = p^{-\dim(H)/2} \sum_{x \in H} \omega_p^{Q(x)} |x\rangle. \quad (4)$$

Definition 3.4. *For an n -qudit quantum state $|\psi\rangle$ define its stabilizer rank, denoted $\chi(|\psi\rangle)$, to be the minimal number r needed to write $|\psi\rangle$ as a linear combination of r stabilizer states.*

3.2 Nonclassical polynomials

We will now define what *nonclassical* polynomials are. First, let $P \in \mathbb{F}_p[x_1, \dots, x_n]$ be a ‘‘classical’’ polynomial of degree $d \geq 1$. One can show that $\Delta_h P(x) = P(x+h) - P(x)$ is again a polynomial but of degree at most $d-1$. So after taking $d+1$ derivatives, the resulting polynomial will be the zero polynomial. Using this observation, we can define a broader class of polynomials as functions that take values in \mathbb{T} and satisfy a condition on its derivatives.

Definition 3.5. *For an integer $d \geq 1$, a map $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ is a nonclassical polynomial of degree at most d if for all $h_1, \dots, h_{d+1} \in \mathbb{F}_p^n$ we have*

$$\Delta_{h_{d+1}} \cdots \Delta_{h_1} P(x) = 0. \quad (5)$$

The degree of P is the smallest such d .

Using the map $\iota: \mathbb{F}_p \rightarrow \mathbb{T}: x \mapsto |x|/p$, one can view a polynomial $P \in \mathbb{F}_p[x_1, \dots, x_n]$ as a map $\iota(P): \mathbb{F}_p^n \rightarrow \mathbb{T}$. Nonclassical polynomials that arise in this way are called classical polynomials and they are a subset of the nonclassical polynomials. Note that they take values in $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$. This confusing terminology has unfortunately become standard in the literature. Below, all polynomials are assumed to be nonclassical if it is not explicitly stated. The following example shows that this containment of classical polynomials in the set of nonclassical polynomials is indeed proper.

Example 3.6. Let $p = 2$ and consider $P: \mathbb{F}_2^n \rightarrow \mathbb{T}$ be given by $x \mapsto |x|/4$. This is a nonclassical polynomial of degree two. To show this, we take derivatives:

$$|x+h|/4 - |x|/4 = |x|/4 + |h|/4 - |x \circ h|/2 - |x|/4 = |h|/4 - |x \circ h|/2 \pmod{1},$$

where \circ is entry-wise product of vectors. In the first equality we used the property in (1). Taking one more derivative

$$\Delta_{h'} \Delta_h P(x) = -|x \circ h + h' \circ h|/2 + |x \circ h|/2 = -|h' \circ h|/2 \pmod{1}.$$

Indeed, $P(x) = |x|/4$ is a nonclassical polynomial of degree two. Note that it is *not* a classical polynomial since it takes values in $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$.

In general, the polynomial $P(x) = |x|/2^k$ is a nonclassical polynomial of degree k . We will see later (Section 4.1) that for $k = 3$, this polynomial corresponds to the n -qubit magic state.

Let $p = 3$ and consider the polynomial $P: \mathbb{F}_3^n \rightarrow \mathbb{T}: x \rightarrow |x|/9$. This is a nonclassical polynomial of degree three: let $h \in \mathbb{F}_3^n$, then by the property in (2)

$$\Delta_h P(x) = |x + h|/9 - |x|/9 = |h|/9 + (|x^2 \circ h| + |x \circ h^2|)/3 - 2|x \circ h|/3 \pmod{1}.$$

Here $x^2 = x \circ x$, i.e. the entry-wise product of x with itself. The above is (up to a shift) a classical polynomial of degree two, hence P is cubic. We will see in Section 4.1 that this polynomial P corresponds to the n -qudit magic state where the qudit has dimension three.

The above is a local definition of nonclassical polynomials. A global definition of classical polynomials of degree at most d is that they take the form $\sum_{i_1 + \dots + i_n \leq d} c_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$. Similarly, nonclassical polynomials have the following global description.

Proposition 3.7 ([24]). *$P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ is a nonclassical polynomial of degree at most d if and only if it has a representation of the form*

$$P(x_1, \dots, x_n) = \alpha + \sum_{\substack{0 \leq i_1, \dots, i_n \leq p-1; j \geq 0: \\ 0 < i_1 + \dots + i_n \leq d - j(p-1)}} \frac{c_{i_1, \dots, i_n, j} |x_1|^{i_1} \cdots |x_n|^{i_n}}{p^{j+1}}, \quad (6)$$

for some coefficients $c_{i_1, \dots, i_n, j} \in \{0, 1, \dots, p-1\}$ and $\alpha \in \mathbb{T}$, these coefficients are unique. The maximal j in this decomposition is called the depth of P .

Note that the depth of a nonclassical polynomial is always at most $\lceil d/(p-1) \rceil - 1$ since at least one of the indices i_1, \dots, i_n must be positive. Using this proposition, one quickly sees that the polynomial $x \mapsto |x|/4$ for $x \in \mathbb{F}_2^n$ from the example above has degree two and depth 1. The polynomial $x \mapsto |x|/2^k$ has degree k and depth $k-1$.

Let $H \subset \mathbb{F}_p^n$ be an affine subspace and $Q: H \rightarrow \mathbb{T}$ a map. Let $A: \mathbb{F}_p^{\dim(H)} \rightarrow \mathbb{F}_p^n$ be an affine linear transformation such that A maps surjectively on H . We can view Q in its “local coordinate system”: for $y \in \mathbb{F}_p^{\dim(H)}$ define $Q'(y) = Q(A(y))$.

Let $p = 2$. If Q is a quadratic form (Definition 3.1), then Q' is a nonclassical polynomial of degree at most two. Proposition 3.7 implies that its depth is at most 1. In other words, Q' takes values in $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$ and so does Q .

Similarly, for $p > 2$ a quadratic polynomial $Q: H \rightarrow \mathbb{F}_p$ on an affine subspace $H \subset \mathbb{F}_p^n$, is simply a quadratic polynomial in local coordinates, i.e. the map $Q': \mathbb{F}_p^{\dim(H)} \rightarrow \mathbb{F}_p$ is a polynomial of degree two in the $\dim(H)$ variables.

The following is a simple observation that we will need later, it follows directly from Proposition 3.7.

Lemma 3.8. *Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be a nonclassical polynomial of degree at most one. Then P is classical (up to some shift).*

3.3 Rank of nonclassical polynomials

In this section we introduce a notion of rank for nonclassical polynomials. The main reference is again [13].

Definition 3.9. Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be a nonclassical polynomial. For an integer $d \geq 1$, we define the d -rank, denoted by $\text{rank}_d(P)$, to be the minimal number r such that there are nonclassical polynomials Q_1, \dots, Q_r all of degree at most $d - 1$ and a function $\Gamma: \mathbb{T}^r \rightarrow \mathbb{T}$ such that for all $x \in \mathbb{F}_p^n$

$$\Gamma(Q_1(x), \dots, Q_r(x)) = P(x).$$

If $d = 1$, the d -rank will be ∞ if P is non-constant and 0 otherwise. The rank of P , denoted $\text{rank}(P)$, is the $\deg(P)$ -rank of P .

The next result [13, Corollary 7.16] is a standard application of Fourier analysis and can be thought of as a kind of “inverse theorem”. We give the proof here for convenience.

Proposition 3.10. Let $d \geq 2$ and $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ a polynomial with $r := \text{rank}_d(P)$. Then there exists a polynomial Q of degree at most $d - 1$ such that

$$|\langle e(P), e(Q) \rangle| \geq p^{-(1 + \lceil (d-1)/(p-1) \rceil)r}.$$

Proof. Let $\Gamma: \mathbb{T}^r \rightarrow \mathbb{T}$ be a map and Q_1, \dots, Q_r be polynomials of degree at most $d - 1$ such that

$$P(x) = \Gamma(Q_1(x), \dots, Q_r(x)).$$

We can assume that Γ is a map with domain $G := \prod_{i=1}^r \frac{1}{p^{k_i+1}} \mathbb{Z}/\mathbb{Z}$, where k_i is the depth of Q_i . Let $\hat{G} = \prod_{i=1}^r \mathbb{Z}_{p^{k_i+1}}$ be the dual of G , so that the Fourier decomposition of $e(\Gamma)$ becomes

$$e(\Gamma(z)) = \sum_{\alpha \in \hat{G}} \hat{\Gamma}_\alpha e(\langle \alpha, z \rangle).$$

The Fourier decomposition of $e(\Gamma)$ gives a “higher-order” Fourier decomposition of $e(P)$: for $\alpha \in \hat{G}$ define $Q_\alpha(x) := \sum_{i=1}^r \alpha_i Q_i(x)$, then

$$e(P(x)) = \sum_{\alpha \in \hat{G}} \hat{\Gamma}_\alpha e(Q_\alpha(x)).$$

So

$$1 = |\langle e(P), e(P) \rangle| \leq \sum_{\alpha \in \hat{G}} |\langle e(P), e(Q_\alpha) \rangle|.$$

Indeed, there is an α^* such that

$$|\langle e(P), e(Q_{\alpha^*}) \rangle| \geq |\hat{G}|^{-1}.$$

Since the degree of the polynomials Q_i is at most $d - 1$, it follows that $k_i(p - 1) \leq d - 1$. This implies that

$$|\hat{G}| = p^{k_1+1+\dots+k_r+1} \leq p^{(1 + \lceil (d-1)/(p-1) \rceil)r}.$$

□

The next lemma [13, Lemma 7.2] tells us how the rank changes if we restrict a polynomial to an affine subspace.

Lemma 3.11. *Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be a polynomial of degree $d \geq 2$ and $r := \text{rank}(P)$. Let $U \subset \mathbb{F}_p^n$ be an affine subspace of codimension k and define P' to be the restriction of P to U . If $r > pk + 1$ then P' is a polynomial of degree d and $\text{rank}(P') \geq r - pk$.*

Proof. We will prove the statement for $k = 1$. The general case will follow after repeated application of the proof for $k = 1$.

Since rank and degree do not change under invertible affine linear transformations, we can assume without loss of generality that $U = \{x \in \mathbb{F}_p^n : x_n = 0\}$. Let $\pi: \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ be the projection onto U , so $\pi(x_1, \dots, x_n) = (x_1, \dots, x_{n-1}, 0)$. Define $P'' = P - P' \circ \pi$. For $x \in U$ we have $P''(x) = 0$. Let $a \in \mathbb{F}_p \setminus \{0\}$ and $h_a = (0, \dots, 0, a) \in \mathbb{F}_p^n$. We have that $\Delta_{h_a} P''$ has degree at most $d - 1$ and that $\Delta_{h_a} P''(y) = P''(y + h)$ for all $y \in U$. So P'' agrees with a polynomial Q_a of degree at most $d - 1$ on $U + h_a$. This implies there is a function $\Gamma: \mathbb{T}^{p+1} \rightarrow \mathbb{T}$ such that $P(x) = \Gamma(|x_n|/p, P'(x), Q_1(x), \dots, Q_{p-1}(x))$.

Now, if P' has degree at most $d - 1$, then $\text{rank}(P) \leq p + 1 < r$, which is a contradiction. If P' has $\text{rank} < r - p$, we get that $\text{rank}(P) < r$ which is again a contradiction. \square

Next, we define the *Fourier rank* of a function which is a new notion of rank for functions and prove straightforward properties of it.

Definition 3.12. *Let $f: \mathbb{F}_p^n \rightarrow \mathbb{C}$ be a function and $d \geq 1$. The degree- d Fourier rank of f , denoted $\text{frank}_d(f)$, is the minimal r such that there are polynomials Q_1, \dots, Q_r of degree at most $d - 1$ such that for all $x \in \mathbb{F}_p^n$*

$$f(x) = \sum_{i=1}^r c_i e(Q_i(x)). \quad (7)$$

The degree-2 Fourier rank of a function f is also known as the *Fourier sparsity* of f . The following lemma relates the notion of rank of a polynomial and its Fourier rank.

Lemma 3.13. *Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be a polynomial and $d \geq 2$. Then $\text{frank}_d(e(P)) \geq \text{rank}_d(P)$.*

Proof. Denote by r' the degree d Fourier rank of $e(P)$. So there are polynomials $Q_1, \dots, Q_{r'}$ of degree at most $d - 1$ such that we have a decomposition

$$e(P(x)) = \sum_{i=1}^{r'} c_i e(Q_i(x)). \quad (8)$$

We will now define a function $\Gamma: \mathbb{T}^{r'} \rightarrow \mathbb{T}$ as follows. Let $Q: \mathbb{F}_p^n \rightarrow \mathbb{T}^{r'}$ be defined by $Q(x) = (Q_1(x), \dots, Q_{r'}(x))$. The map Γ on the image of Q is defined by

$$e(\Gamma(Q_1(x), \dots, Q_{r'}(x))) = \sum_{i=1}^{r'} c_i e(Q_i(x)).$$

For a point z in the complement of the image of Q , we simply set $\Gamma(z) = 0$ or any other constant value would do. But the Γ we just defined has the property that $\Gamma(Q_1(x), \dots, Q_{r'}(x)) = P(x)$ by (8). Hence $r' \geq r$, proving the statement. \square

For $d = 2$, Sanyal [21] shows that $\text{frank}_2(e(P)) \geq \text{rank}_2(P)^2$. This is quadratically better than the above lemma. See Section 6 for a discussion for the case $d > 2$.

In the other direction, we have the following lemma.

Lemma 3.14. *Let $d \geq 2$ and $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ a polynomial. Then*

$$\text{frank}_d(e(P)) \leq p^{(1 + \lceil (d-1)/(p-1) \rceil) \text{rank}_d(P)}.$$

Proof. Let $r := \text{rank}_d(P)$. Then there is a function $\Gamma: \mathbb{T}^r \rightarrow \mathbb{T}$ and polynomials Q_1, \dots, Q_r of degree at most $d - 1$ such that $\Gamma(Q_1(x), \dots, Q_r(x)) = P(x)$. The Fourier expansion of Γ gives us a degree $d - 1$ Fourier expansion of P , namely

$$\begin{aligned} e(\Gamma(Q_1(x), \dots, Q_r(x))) &= \sum_{\alpha \in \widehat{G}} \widehat{\Gamma}(\alpha) e(Q_\alpha(x)) \\ &= e(P(x)), \end{aligned}$$

where $Q_\alpha(x) = \sum_{i=1}^r \alpha_i Q_i(x)$ and $\widehat{G} = \prod_{i=1}^r \mathbb{Z}_{p^{k_i+1}}$ is the dual of the group $G = \prod_{i=1}^r \frac{1}{p^{k_i+1}} \mathbb{Z}/\mathbb{Z}$ and k_i is the depth of Q_i . Since there are at most

$$|\widehat{G}| \leq p^{(1+\lceil (d-1)/(p-1) \rceil)r}$$

Fourier coefficients in the above expression, the result follows. \square

4 Magic states in prime dimension

In this section we will give the explicit form of the magic state that we obtain by using the generalization of the T gate in odd prime dimensions [15]. We will then proceed to show that these magic states have exponentially small correlation with quadratic phase functions.

4.1 Generalization of the T gate

The generalization of the T gate, and hence the corresponding magic state, curiously enough depends on whether the prime dimension p is equal to three or $p > 3$.

- But first, let us consider the case $p = 2$. In this case, the T -gate is given by $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ and the corresponding single qubit magic state is given by $T|+\rangle = |T\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$, hence the n -qubit magic state is

$$|T\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} e(|x|/8)|x\rangle. \quad (9)$$

Here, the polynomial $P: \mathbb{F}_2^n \rightarrow \mathbb{T}: x \mapsto |x|/8$ is a nonclassical polynomial of degree exactly three. This follows immediately from Proposition 3.7, see also Example 3.6. We will see a similar phenomenon in other prime dimensions.

- In the case that $p = 3$, let $\xi = e^{2\pi i/9}$ be a ninth-root of unity. The generalization of the T -gate for $p = 3$, denoted by U , is given by

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix}.$$

The corresponding single qudit magic state is then

$$|\psi_U\rangle = U|+\rangle = \frac{|0\rangle + \xi|1\rangle + \xi^2|3\rangle}{\sqrt{3}}.$$

The n -qudit magic state in this case is

$$|\psi_U\rangle^{\otimes n} = \frac{1}{3^{n/2}} \sum_{x \in \mathbb{F}_3^n} e(|x|/9)|x\rangle. \quad (10)$$

The polynomial $P: \mathbb{F}_3^n \rightarrow \mathbb{T}: x \mapsto |x|/9$ is again a nonclassical polynomial of degree three which follows from Proposition 3.7, see also Example 3.6.

- The case $p > 3$ are all similar, but different from the previous two cases. In this case, let $\omega_p = e^{2\pi i/p}$ be a p -th root of unity and $P: \mathbb{F}_p \rightarrow \mathbb{F}_p$ a classical polynomial of degree three. Define

$$U := \sum_{x \in \mathbb{F}_p} \omega_p^{P(x)} |x\rangle\langle x|.$$

This gate is then a non-clifford gate [15] and could serve as a generalization of the T gate. The condition that P has degree three is important: if P has degree two, then U is a Clifford gate. The corresponding n -qudit magic state is then

$$|\psi_U\rangle^{\otimes n} = \frac{1}{p^{n/2}} \sum_{x \in \mathbb{F}_p^n} \omega_p^{P_n(x)} |x\rangle, \quad (11)$$

where $P_n(x) = \sum_{i=1}^n P(x_i)$. Unlike the $p = 2, 3$ case, the polynomial P_n is a *classical* polynomial of degree three. Coincidentally, there are no cubic nonclassical polynomials for $p > 3$.

4.2 Correlation with quadratic phase functions

We will now show that for the n -qudit magic states defined as above, the correlation with quantum states whose amplitudes are given by a quadratic phase functions is exponentially small. We need the following basic lemma, see [17]. We will state and prove it here for convenience.

Lemma 4.1. *For any two functions $f, g: \mathbb{F}_p^n \rightarrow \mathbb{T}$, we have*

$$|\langle e(f), e(g) \rangle|^4 \leq \mathbb{E}_{h \in \mathbb{F}_p^n} |\langle e(\Delta_h f), e(\Delta_h g) \rangle|^2.$$

Proof. By the Cauchy-Schwarz inequality,

$$\begin{aligned} \sqrt{\mathbb{E}_h |\langle e(\Delta_h f), e(\Delta_h g) \rangle|^2} &\geq |\mathbb{E}_h \langle e(\Delta_h f), e(\Delta_h g) \rangle| \\ &= |\mathbb{E}_{x, h} e(f(x+h) - f(x) - (g(x+h) - g(x)))| \\ &= |\langle e(f), e(g) \rangle|^2. \end{aligned}$$

□

In other words, we can compute the correlation between two phase functions by computing the correlations between their derivatives and taking their average. If the derivatives are easier to work with, this will become useful.

Proposition 4.2. *Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be the polynomial in the phase of the amplitudes in either Equation (9), (10) or (11). Then, for any nonclassical polynomial $Q: \mathbb{F}_p^n \rightarrow \mathbb{T}$ of degree at most two,*

$$|\langle e(P), e(Q) \rangle| \leq 2^{-cn},$$

for some $c > 0$ depending on p .

Proof. We will only prove it for the case $p = 2$, since the other case $p > 2$ is very similar. We will show that the polynomial phase function $e(|x|/8)$, giving the amplitudes of the n -qubit magic state (see (9)), has exponentially small correlation with quadratic phase functions. First we compute the derivative of P ; let $h \in \mathbb{F}_2^n$. Then

$$\begin{aligned} P(x+h) - P(x) &= |x+h|/8 - |x|/8 = \sum_i |x_i + h_i|/8 - |x|/8 \\ &= \sum_i (|x_i| + |h_i| - 2|x_i||h_i|)/8 - |x|/8 \\ &= |h|/8 - |x \circ h|/4. \end{aligned}$$

In the second line, we used the property (1). Let $f: x \mapsto e(|x \circ h|/4)$. We need the magnitudes of the Fourier coefficients of f ; we have for $\alpha \in \mathbb{F}_2^n$

$$\hat{f}(\alpha) = \mathbb{E}_x e^{i\pi(|x \circ h| - 2|\alpha \circ x|)/2},$$

so

$$\begin{aligned} |\hat{f}(\alpha)|^2 &= \mathbb{E}_{x,y} e^{i\pi(|x \circ h| - |y \circ h| - 2|\alpha \circ x| + 2|\alpha \circ y|)/2} \\ &= \mathbb{E}_{y,z} e^{i\pi(|y \circ h| + |z \circ h| - 2|y \circ z \circ h| - |y \circ h| - 2|\alpha \circ z|)/2} \\ &= \mathbb{E}_{y,z} e^{i\pi(|z \circ h| - 2|y \circ z \circ h| - 2|\alpha \circ z|)/2} \\ &= \mathbb{E}_z e^{i\pi(|z \circ h| - 2|\alpha \circ z|)/2} \mathbb{E}_y (-1)^{|y \circ z \circ h|}. \end{aligned}$$

In the second line we used a change of variables $x = y + z$ and the property in (1) so that

$$\begin{aligned} |x \circ h| &= |(y+z) \circ h| = |y \circ h + z \circ h| = |y \circ h| + |z \circ h| - 2|(y \circ h) \circ (z \circ h)| \\ &= |y \circ h| + |z \circ h| - 2|y \circ z \circ h|. \end{aligned}$$

The expectation over y is 0 unless $h_i = 1 \Rightarrow z_i = 0$ in which case it is equal to 1. So continuing where we left off

$$\begin{aligned} &= \frac{1}{2^n} \sum_{z: h_i=1 \Rightarrow z_i=0} e^{i\pi(|z \circ h| - 2|\alpha \circ z|)/2} \\ &= \frac{1}{2^n} \sum_{z: h_i=1 \Rightarrow z_i=0} (-1)^{|\alpha \circ z|} \end{aligned}$$

which is 0 unless $h_i = 0 \Rightarrow \alpha_i = 0$, in which case it equals $2^{-|h|}$. So the non-zero Fourier coefficients of f are at those $\alpha \in \mathbb{F}_2^n$ for which it holds that $h_i = 0 \Rightarrow \alpha_i = 0$.

We will now show that there is exponentially small correlation between $e(P)$ and any nonclassical polynomial phase function $e(Q)$ of degree two. By Lemma 4.1 and Parseval, we have that

$$\begin{aligned}
|\langle e(P), e(Q) \rangle|^4 &\leq \mathbb{E}_h |\langle e(\Delta_h P), e(\Delta_h Q) \rangle|^2 \\
&= \mathbb{E}_h |\langle e(\widehat{\Delta_h P}), e(\widehat{\Delta_h Q}) \rangle|^2 \\
&\leq \mathbb{E}_h 2^{-|h|} \\
&= \frac{1}{2^n} \sum_{k=0}^n 2^{-k} |\{h \in \mathbb{F}_2^n : |h| = k\}| \\
&= \left(\frac{3}{4}\right)^n.
\end{aligned}$$

In the third line, we used that $\Delta_h Q$ is a degree one classical polynomial (using Lemma 3.8), which means that $e(\Delta_h Q)$ has only one non-zero Fourier coefficient and that the magnitude of all the Fourier coefficients of $e(\Delta_h(P))$ is at most $2^{-|h|/2}$, see the computation of $|\hat{f}(\alpha)|^2$ above where $f(x) = e(|h|/8)e(-\Delta_h P(x))$.

For $p = 3$, the cubic phase function giving the amplitudes of the n -qudit magic states is given by (10). One follows the same strategy by first computing the derivative of the polynomial $x \mapsto |x|/9$ using the property (2) and computing the magnitude of the Fourier coefficients of its associated phase function and concluding with a use of Lemma 4.1. The case $p > 3$ is simpler as it does not require any property of the map $|\cdot|$, since the polynomial in the phase of (11) is a classical polynomial. \square

5 Stabilizer rank of the n -qudit magic state

Here we prove Theorem 1.1, our main result.

The following claim from [20] is needed to get a handle on the affine subspaces that appear with the stabilizer states in a stabilizer decomposition.

Claim 5.1 ([20]). *Let p be a prime and $H_1, \dots, H_r \subset \mathbb{F}_p^n$ be a collection of affine subspaces and assume $r \leq n/2$. Then there exists an affine subspace U of dimension at least $n - 2r$ and a subset $S \subset [r]$ such that for all $x \in U$*

$$1_{H_i}(x) = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $E: \mathbb{F}_p^n \rightarrow \{0, 1\}^r$ be the map given by $x \mapsto (1_{H_1}(x), \dots, 1_{H_r}(x))$. By the pigeonhole principle, there is $\alpha \in \{0, 1\}^r$ such that $|E^{-1}(\alpha)| \geq p^n 2^{-r} \geq p^{n-r}$. Denote by $S \subset [r]$ the set of indices i such that $\alpha_i = 1$. It is clear that $E^{-1}(\alpha) = \bigcap_{i \in S} H_i \setminus \bigcup_{i \notin S} H_i$ (if $S = \emptyset$, define $\bigcap_{i \in S} H_i = \mathbb{F}_p^n$). Now define $V = \bigcap_{i \in S} H_i$, this is an affine subspace of dimension at least $n - r$. Pick an arbitrary $x_0 \in E^{-1}(\alpha)$, so $x_0 \notin H_i$ for $i \notin S$. This implies that $\forall i \notin S$ there is an affine equation h_i such that $h_i(x_0) = 1$ but $h_i(x) = 0$ for all $x \in H_i$. The affine subspace we are looking for is

$$U := \{x \in V : \forall i \notin S \quad h_i(x) = 1\}.$$

Note that U is not empty since $x_0 \in U$. Since we only add at most r extra equations, the dimension of U is at least $n - 2r$. \square

Proof of Theorem 1.1 Let $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be the nonclassical polynomial of degree three given by the corresponding n -qudit magic state, depending on the prime p . For $p = 2$, $p = 3$ and $p > 3$ it is given by the (polynomials in the phase of the) amplitudes of Equation (9), (10) and (11) respectively. Let $|\psi\rangle$ be the corresponding n -qudit magic state, i.e.

$$|\psi\rangle = p^{-n/2} \sum_{x \in \mathbb{F}_p^n} e(P(x))|x\rangle.$$

Denote by r the stabilizer rank of $|\psi\rangle$, so there is a decomposition

$$|\psi\rangle = \sum_{i=1}^r c_i |\phi_i\rangle,$$

for some constants c_i and stabilizer states $|\phi_i\rangle$. Each such ϕ_i is defined on an affine subspace $H_i \subset \mathbb{F}_p^n$. Let $C > 0$ be a large enough constant¹. If $r > n/C$, we are done. So assume $r \leq n/C$. Then, we have that

$$\begin{aligned} e(P(x)) &= p^{n/2} \langle x | \psi \rangle = p^{n/2} \sum_{i=1}^r c_i \langle x | \phi_i \rangle \\ &= \sum_{i=1}^r c'_i e(Q_i(x)) 1_{H_i}(x), \end{aligned}$$

where Q_i is a quadratic polynomial on H_i and $c'_i = p^{(n-\dim(H_i))/2} c_i$. Then by Claim 5.1 (using $r \leq n/C$), there is an affine subspace U of dimension cn for some $c \geq 0.99$ and a non-empty subset $S \subset [r]$ such that $\forall x \in U$

$$1_{H_i}(x) = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise.} \end{cases}$$

Let $A: \mathbb{F}_p^{cn} \rightarrow \mathbb{F}_p^n$ be an affine linear map such that $U = \{A(y): y \in \mathbb{F}_p^{cn}\}$. Let $P': \mathbb{F}_p^{cn} \rightarrow \mathbb{T}$ be the polynomial given by $P'(y) = P(A(y))$. Then the restriction of the above decomposition of $e(P(x))$ to U implies that

$$e(P'(y)) = \sum_{i \in S} c'_i e(Q'_i(y)), \tag{12}$$

where $Q'_i(y) := Q_i(A(y))$ and we have that Q'_i is a nonclassical polynomial of degree at most two. By Proposition 4.2 and (the contrapositive of) 3.10 the polynomial P has high rank: $\text{rank}(P) \geq \Omega(n)$. By Lemma 3.11 it follows that P' is still cubic and we have $\text{rank}(P') \geq \Omega(n)$ (this uses that C is a large enough constant). But (12) is a decomposition in terms of nonclassical polynomial phase functions of degree at most two. By Lemma 3.13 we have $|S| \geq \Omega(n)$ so that $r \geq \Omega(n)$. \square

6 Discussion

From the above proof, we can immediately conclude that it is not possible to get super-linear lower bounds on the stabilizer rank of n -qudit magic states using these techniques. This is due to the use of Claim 5.1. However, there is no obvious obstruction to get super-linear lower bounds on the number of stabilizer states needed in a decomposition of n -qudit

¹Given the prime p and the constant c from Proposition 4.2, the constant C should satisfy $C > 2p/c$.

magic states where all the stabilizer states are defined on the full space \mathbb{F}_p^n . The graph states (classical quadratic polynomials) are for example in this set. The possibility of such a super-linear lower bound hinges on the relationship between the rank of a polynomial and its Fourier rank: the d -rank of a polynomial P on n variables is at most n , whereas the degree- d Fourier rank of a polynomial is at most p^n . Lemma 3.13 only shows that $\text{frank}_d(e(P)) \geq \text{rank}_d(P)$. Is this relation optimal, or can we expect much better?

Problem 6.1. *Let $d \geq 2$ and $P: \mathbb{F}_p^n \rightarrow \mathbb{T}$ be a polynomial. Is it true that*

$$\text{frank}_d(e(P)) \geq \omega(\text{rank}_d(P))?$$

A positive answer to this question would not only show that the n -qubit magic state needs super-linear many stabilizer states defined on the full space \mathbb{F}_p^n , but would also have implications in another field. For this, let us consider the case $p = 2$.

Let $\text{AND}(x) = |x_1 x_2 \cdots x_n|/2$ be the (classical) polynomial giving the AND function. The ‘‘quadratic uncertainty principle’’ [8] is a conjecture that states that any decomposition

$$e(\text{AND}(x)) = \sum_{i=1}^r c_i e(Q_i(x)), \quad (13)$$

where Q_i are classical quadratic polynomials, must have $r \geq 2^{\Omega(n)}$. Note that Definitions 3.9 and 3.12 of rank and frank are still valid if we only allow *classical* polynomials, which we will denote by rank' and frank' . The best known lower bound is $\text{frank}'_3(e(\text{AND})) \geq n/2$ [25]. The proof of this uses the Chevalley-Waring theorem in an elegant way. It shows, implicitly, that the 3-rank' of the AND function is at least $n/2$, i.e. near maximal rank. This way of looking at it fits very well with Lemma 3.13. What is actually shown in [25] is the same lower bound for the NOR function, i.e. $\text{NOR}(x) = |1 + x_1| \cdots |1 + x_n|/2$. Lower bounds on the NOR function imply the same lower bounds on the AND function (it is the same function in a different basis). The proof also works if we allow polynomials of degree at most a constant.

Theorem 6.2 ([25], generalized). *Let $\text{NOR}: \mathbb{F}_2^n \rightarrow \mathbb{T}$ be the function defined above and let $d \geq 3$ be an integer (constant). Then $\text{frank}'_d(e(\text{NOR})) \geq n/(d-1)$.*

Proof. We will show that $\text{rank}'_d(\text{NOR}) \geq n/(d-1)$. Having shown this, the result follows immediately from Lemma 3.13 (which also holds for rank' and frank').

Let $r = \text{rank}'_d(\text{NOR})$. So there are (classical) polynomials Q_1, \dots, Q_r of degree at most $d-1$ such that there is a function $\Gamma: \mathbb{T}^r \rightarrow \mathbb{T}$ such that

$$\text{NOR}(x) = \Gamma(Q_1(x), \dots, Q_r(x)).$$

We may assume without loss of generality that $Q_i(0) = 0$ for all $i = 1, \dots, r$ (since Γ can always add/subtract a constant to/from Q_i). Assume that $r < n/(d-1)$. By the Chevalley-Waring theorem, the polynomials Q_1, \dots, Q_r have another common root $x \neq (0, \dots, 0)$. This contradicts the fact that $\text{NOR}(x) = 1/2$ if and only if $x = (0, \dots, 0)$. \square

Since the NOR function has $\text{rank}'_3(\text{NOR}) \geq n/2$, a positive answer to Problem 6.1 would show that the number of quadratic polynomials needed in (13) is super-linear. As noted before, Sanyal [21] showed that $\text{frank}'_2(e(P)) \geq \text{rank}'_2(P)^2$. An analogue of this result for $d > 2$ would quadratically improve the best lower bound on $\text{frank}'_3(\text{NOR})$.

References

- [1] Tom Bannink, Jop Briët, Harry Buhrman, Farrokh Labib, and Troy Lee. Bounding quantum-classical separations for classes of nonlocal games. In *36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019)*, pages 12:1–12:11, March 2019. DOI: 10.4230/LIPIcs.STACS.2019.12.
- [2] Sergey Bravyi and David Gosset. Improved classical simulation of quantum circuits dominated by clifford gates. *Phys. Rev. Lett.*, 116:250501, Jun 2016. DOI: 10.1103/PhysRevLett.116.250501.
- [3] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005. DOI: 10.1103/PhysRevA.71.022316.
- [4] Sergey Bravyi, Graeme Smith, and John A. Smolin. Trading classical and quantum computational resources. *Phys. Rev. X*, 6:021043, Jun 2016. DOI: 10.1103/PhysRevX.6.021043.
- [5] 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.
- [6] Jianxin Chen, Fang Zhang, Cupjin Huang, Michael Newman, and Yaoyun Shi. Classical simulation of intermediate-size quantum circuits. *arXiv preprint arXiv:1805.01450*, 2018.
- [7] Jeroen Dehaene and Bart De Moor. Clifford group, stabilizer states, and linear and quadratic operations over $\text{gf}(2)$. *Phys. Rev. A*, 68:042318, Oct 2003. DOI: 10.1103/PhysRevA.68.042318.
- [8] Yuval Filmus, Hamed Hatami, Steven Heilman, Elchanan Mossel, Ryan O’Donnell, Sushant Sachdeva, Andrew Wan, and Karl Wimmer. Real analysis in computer science: A collection of open problems. *Preprint available at <https://simons.berkeley.edu/sites/default/files/openprobsmerged.pdf>*, 2014.
- [9] D Gottesman. The heisenberg representation of quantum computers. 6 1998. URL <https://www.osti.gov/biblio/319738>.
- [10] William Timothy Gowers. A new proof of szemerédi’s theorem for arithmetic progressions of length four. *Geometric & Functional Analysis GAFA*, 8(3):529–551, 1998.
- [11] D. Gross. Hudson’s theorem for finite-dimensional quantum systems. *Journal of Mathematical Physics*, 47(12):122107, 2006. DOI: 10.1063/1.2393152.
- [12] Thomas Häner and Damian S. Steiger. 0.5 petabyte simulation of a 45-qubit quantum circuit. In *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. ACM, 2017. DOI: 10.1145/3126908.3126947.
- [13] Hamed Hatami, Pooya Hatami, and Shachar Lovett. Higher-order fourier analysis and applications. *Foundations and Trends® in Theoretical Computer Science*, 13(4): 247–448, 2019. DOI: 10.1561/04000000064.
- [14] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic. *Physical Review A*, 71(4), apr 2005. DOI: 10.1103/physreva.71.042315.
- [15] Mark Howard and Jiri Vala. Qudit versions of the qubit $\pi/8$ gate. *Physical Review A*, 86(2):022316, 2012. DOI: 10.1103/PhysRevA.86.022316.
- [16] Zi-Wen Liu and Andreas Winter. Many-body quantum magic. *arXiv preprint arXiv:2010.13817*, 2020.
- [17] Shachar Lovett, Roy Meshulam, and Alex Samorodnitsky. Inverse conjecture for the

- gowers norm is false. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 547–556, 2008. DOI: 10.1145/1374376.1374454.
- [18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.
- [19] Edwin Pednault, John A Gunnels, Giacomo Nannicini, Lior Horesh, Thomas Magerlein, Edgar Solomonik, and Robert Wisnieff. Breaking the 49-qubit barrier in the simulation of quantum circuits. *arXiv preprint arXiv:1710.05867*, 15, 2017.
- [20] Shir Peleg, Ben Lee Volk, and Amir Shpilka. Lower Bounds on Stabilizer Rank. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 110:1–110:4. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. DOI: 10.4230/LIPIcs.ITCS.2022.110.
- [21] Swagato Sanyal. Fourier sparsity and dimension. *Theory of Computing*, 15(11):1–13, 2019. DOI: 10.4086/toc.2019.v015a011.
- [22] Mikhail Smelyanskiy, Nicolas PD Sawaya, and Alán Aspuru-Guzik. qhipster: The quantum high performance software testing environment. *arXiv preprint arXiv:1601.07195*, 2016.
- [23] Endre Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27(199-245):2, 1975. URL <http://eudml.org/doc/205339>.
- [24] Terence Tao and Tamar Ziegler. The inverse conjecture for the gowers norm over finite fields in low characteristic. *Annals of Combinatorics*, 16(1):121–188, 2012. DOI: 10.1007/s00026-011-0124-3.
- [25] Richard Ryan Williams. Limits on Representing Boolean Functions by Linear Combinations of Simple Functions: Thresholds, ReLUs, and Low-Degree Polynomials. In *33rd Computational Complexity Conference (CCC 2018)*, volume 102 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:24. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2018. DOI: 10.4230/LIPIcs.CCC.2018.6.