Tolerant Testing of Stabilizer States with a Polynomial Gap via a Generalized Uncertainty Relation

Zongbo Bao
CWI
Amsterdam, Netherlands
QuSoft
Amsterdam, Netherlands
Zongbo.Bao@cwi.nl

Philippe van Dordrecht
University of Amsterdam
Amsterdam, Netherlands
QuSoft
Amsterdam, Netherlands
philippevdord@gmail.com

Jonas Helsen
CWI
Amsterdam, Netherlands
QuSoft
Amsterdam, Netherlands
jonas@cwi.nl

Abstract

We prove a conjecture of Arunachalam & Dutt [3] on the existence of a tolerant stabilizer testing algorithm, and achieve an *exponential* improvement in the parameters of the tester. Key to our argument is a generalized uncertainty relation for sets of Pauli operators, based on the Lovász theta function.

CCS Concepts

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

Keywords

Quantum computing, Stabilizer state, Tolerant testing, Uncertainty relation, Lovász theta function

ACM Reference Format:
Zongbo Bao, Philippe van Dordrecht, and Jonas Helsen. 2025. Tolerant Testing of Stabilizer States with a Polynomial Gap via a Generalized Uncertainty Relation. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC '25), June 23–27, 2025, Prague, Czechia.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3717823.3718201

1 Introduction

We consider the problem of stabilizer testing: given copies of a state $|\psi\rangle$ with the promise that it is either ϵ_1-close to a stabilizer state (as measured by state fidelity) or ϵ_2-far away, decide which one is the case. This problem has garnered significant interest in recent years following the introduction of the Bell difference sampling algorithm in [12]. There it was proven that Bell difference sampling gives rise to a one-sided tester (i.e. setting $\epsilon_1 = 1$ and $\epsilon_2 < 1$). Their analysis was improved by [11], who proved that Bell difference sampling gives rise to a tester provided that $\epsilon_2 \leq C\epsilon_1^6$. However, they also required that ϵ_1 was larger than some critical threshold. This latter requirement was relaxed by [3], allowing for arbitrary ϵ_1 (this regime is called tolerant testing). However, their argument only obtained a weaker gap relation of the form $\epsilon_2 \leq \exp\left\{-O\left(1/\epsilon_1^c\right)\right\}$, and furthermore it turned out their argument relied on an unproven statement in additive combinatorics, making their ultimate result conjectural (see Conjecture 1.2 in [3][1]).

In this paper we both sidestep their need for a conjecture, and improve their gap relation to a *polynomial* one. This is the polynomial gap mentioned in the title. Concretely we prove the following result:

Theorem 1. *Let $\epsilon_1, \epsilon_2 \in [0, 1]$ and let $|\psi\rangle$ be a state with stabilizer fidelity*

$$\mathcal{F}_S(|\psi\rangle) := \max_{|S\rangle\in\mathrm{STAB_n}} |\langle\psi|S\rangle|^2, \tag{1}$$

either (1) larger than ϵ_1 or (2) smaller than ϵ_2. If $\epsilon_2 \leq C'\epsilon_1^{600}$ for some constant C', then $O\left(\epsilon_1^{-12}\right)$ rounds of Bell difference sampling can distinguish between case (1) and case (2) with probability greater than $2/3$.

The polynomial degree we achieve is likely highly suboptimal. We aim to improve it in future work. To achieve this result we build on the work of [3], combined with a generalized uncertainty relation involving the Lovász theta function, which we derive from a result on Hamiltonian optimization due to Hastings & O'Donnell [13], which we think may be of independent interest.

Remark: After we showed the authors of [3] a summary of our result, they derived their own version of our result based on an earlier note by Sergey Bravyi. Their argument, which uses different techniques, but proceeds essentially along the same lines, is given in [2]. A third, independent, proof of our result was also posted [18] shortly after we posted a first version of this paper on the arXiv. This argument proceeds along different lines from ours, achieving a slightly worse polynomial degree.

2 Preliminaries

In this section we quote some background facts on graph theory (in particular on the Lovász theta) and Bell difference sampling.

2.1 Graph Theoretic Notions

Notations: Given a (simple) graph $\Gamma = (V(\Gamma), E(\Gamma))$ we denote its vertex set by $V(\Gamma)$ and its edge set by $E(\Gamma)$. We use K_n to denote the complete graph on n vertices and $\overline{\Gamma}$ to represent the complement graph of Γ, which shares the same vertex set of Γ, but has complementary edges, i.e. $E\left(\overline{\Gamma}\right) \cap E(\Gamma) = \emptyset$ and $E\left(\overline{\Gamma}\right) \cup E(\Gamma) = E\left(K_{|V(\Gamma)|}\right)$. For graphs Γ_1 and Γ_2, say $\Gamma_1 \subseteq \Gamma_2$ if and only if $V(\Gamma_1) = V(\Gamma_2)$ and

[1] More specifically the second version currently on the arXiv. The first version (lemma 4.17) contains contains a misstatement of a result from [21], leading to the requirement of Conjecture 1.2 in the second version.

STOC '25, Prague, Czechia

ACM ISBN 979-8-4007-1510-5/25/06
https://doi.org/10.1145/3717823.3718201

$E(\Gamma_1) \subseteq E(\Gamma_2)$.

Disjoint union: Graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$, have a disjoint union, denoted by $\Gamma_1 \sqcup \Gamma_2$. It is defined as the graph with $V(\Gamma_1 \sqcup \Gamma_2) = V_1 \cup V_2$, where we assume V_1 and V_2 are disjoint and $E(\Gamma_1 \sqcup \Gamma_2) = E(\Gamma_1) \cup E(\Gamma_2)$.

Strong product: Graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$, have a *strong product*, denoted by $\Gamma_1 \boxtimes \Gamma_2$. It is defined as a graph with vertex set $V(\Gamma_1 \boxtimes \Gamma_2) = V_1 \times V_2$. Distinct vertices $(u_1, v_1), (u_2, v_2) \in V_1 \times V_2$ are connected by an edge if and only if:

(1) $u_1 = u_2$ and v_1 is connected with v_2 in Γ_2, or
(2) $v_1 = v_2$ and u_1 is connected with u_2 in Γ_1, or
(3) u_1 is connected with u_2 in Γ_1 and v_1 is connected with v_2 in Γ_2.

Lovász theta function: Lovász [17] introduced the following graph parameter in the context of classical Shannon theory:

Definition 2 (Lovász theta function)**.** For any graph $\Gamma = ([n], E)$, the Lovász theta is the number

$$\vartheta(\Gamma) = \max_{\rho \in \mathbb{R}^{n\times n}} \left\{ \mathrm{Tr}(\rho \mathbb{J}) \,\middle|\, \rho \geq 0, \mathrm{Tr}(\rho) = 1, \rho_{jk} = 0 \ \forall j, k \in E \right\}, \quad (2)$$

where $\mathbb{J}$ denotes the all-1's matrix.

We will not need anything particularly sophisticated regarding the Lovász theta function in our proofs, merely the following facts:

Fact 3 (Theorem 7 of [17])**.** *For graphs Γ_1 and Γ_2, $\vartheta(\Gamma_1 \boxtimes \Gamma_2) = \vartheta(\Gamma_1) \cdot \vartheta(\Gamma_2)$.*

Fact 4 (Section 18 of [15])**.** *For graphs Γ_1 and Γ_2, $\vartheta(\Gamma_1 \sqcup \Gamma_2) = \vartheta(\Gamma_1) + \vartheta(\Gamma_2)$.*

Fact 5 (Monotonicity of Lovász theta function)**.** *For graphs Γ_1 and Γ_2 such that $\Gamma_1 \subseteq \Gamma_2$, we have that $\vartheta(\Gamma_1) \geq \vartheta(\Gamma_2)$.*

The last fact follows directly from the definition, as more edges will result in more constraints in the maximization.

2.2 Weyl Operators and Distributions

We recall some standard concepts related to stabilizer states and stabilizer testing. We will consistently refer to Hermitian (unsigned) n-qubit Pauli operators as Weyl operators:

Definition 6 (Weyl operator)**.** For $x = (x_1, x_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n = \mathbb{F}_2^{2n}$, the Weyl operator W_x is defined as

$$W_x = i^{x_1 \cdot x_2} \bigotimes_{i=1}^{n} X^{x_{1,i}} Z^{x_{2,i}}. \quad (3)$$

We will occasionally intentionally identify (i.e. confuse) binary vector spaces and sets of Weyl operators.

If we want to know whether two Weyl operators commute, we calculate their symplectic inner product (which is a genuine symplectic form on $\mathbb{F}_2^{2n}$):

Definition 7. The *symplectic inner product* between two vectors $x, y \in \mathbb{F}_2^{2n}$ is the bilinear form

$$[x, y] = \langle x_1, y_2 \rangle + \langle x_2, y_1 \rangle, \quad (4)$$

where $x = (x_1, x_2), y = (y_1, y_2)$ and $x_1, x_2, y_1, y_2 \in \mathbb{F}_2^n$

The following fact is easily verified:

Proposition 8. *For $x, y \in \mathbb{F}_2^{2n}$,*

$$W_x W_y = (-1)^{[x,y]} W_y W_x. \quad (5)$$

Definition 9. An isotropic subspace of $\mathbb{F}_2^{2n}$ is a subspace V of $\mathbb{F}_2^{2n}$ such that for all $x, y \in V$, $[x, y] = 0$. If in addition $|V| = 2^n$, we call the subspace *Lagrangian.*

Lagrangian subspaces (which can be directly identified with the stabilizer groups of stabilizer states) are of importance to us, because they allow us to lower bound the stabilizer fidelity:

Proposition 10 (Proof of Theorem 3.3 of [12], Corollary 7.4 of [11])**.** *Let V be a Lagrangian subspace of $\mathbb{F}_2^{2n}$. Then,*

$$\mathcal{F}_S(|\psi\rangle) \geq \sum_{x \in V} p_\psi(x). \quad (6)$$

where $p_\psi(x) = 2^{-n} |\langle \psi | W_x | \psi \rangle|^2$ is the characteristic distribution of $|\psi\rangle$ (see below).

For completeness, we give a proof of this proposition in Appendix B.

2.3 Bell Difference Sampling

In this section we briefly discuss Bell difference sampling. The key objects are the *characteristic* and *Weyl* distributions of a state $|\psi\rangle$:

Definition 11 (Characteristic and Weyl distributions)**.** We define the characteristic distribution of $|\psi\rangle$ as

$$p_\psi(x) = 2^{-n} |\langle \psi | W_x | \psi \rangle|^2. \quad (7)$$

Furthermore, we define the Weyl distribution q_ψ as

$$q_\psi(x) = 4^n (p_\psi * p_\psi)(x) = \sum_{y \in \mathbb{F}_2^{2n}} p_\psi(y) p_\psi(x + y). \quad (8)$$

We gather some properties of these distributions in the following proposition. Two of these are straightforward, and the third is a core result of [3] (lemma 3.3):

Proposition 12 (Properties of p_ψ)**.** *The characteristic distribution p_ψ has the following properties:*

- $\sum_{x \in \mathbb{F}_2^{2n}} p_\psi(x) = 1$,
- *For all $x \in \mathbb{F}_2^{2n}$, $p_\psi(x) \leq 2^{-n}$,*
- $\mathbb{E}_{x \sim p_\psi} [2^n p_\psi(x)] \geq \mathbb{E}_{x \sim q_\psi} [2^n p_\psi(x)] \geq \left(\mathbb{E}_{x \sim p_\psi} [2^n p_\psi(x)] \right)^2$.

Finally we briefly discuss Bell difference sampling. Bell difference sampling is a surprisingly straightforward procedure that allows us to estimate $\mathbb{E}_{x \sim q_\psi} [|\langle \psi | W_x | \psi \rangle|^2]$ in the following way [12]:

(1) Measure $|\psi\rangle^{\otimes 2}$ in the Bell basis twice. This gives us two independent samples x, y from p_ψ. We set $a = x + y$.
(2) Measure the Weyl operator W_a twice. We accept the sample a if the measurements agree, and reject otherwise.

Repeating this many times and calculating the average number of accepts we can compute the expectation value $\mathbb{E}_{x \sim q_\psi} [|\langle \psi | W_x | \psi \rangle|^2]$. In particular (as can be seen in the proof of Theorem 3.3 in [12]), the probability of acceptance p_{accept} is equal to

$$\frac{1}{2} \sum_a q_\psi(a) \left(1 + |\langle \psi | W_a | \psi \rangle|^2 \right) = \frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{x \sim q_\psi} \left[|\langle \psi | \, W_x \, | \psi \rangle|^2 \right]. \quad (9)$$

This expectation value is the core quantity in stabilizer testing. It provides an upper bound for the stabilizer fidelity as follows:

Fact 13 (Lemma 3.1 of [10]). *Let $|\psi\rangle$ be an n-qubit pure quantum state. Then,*

$$\mathcal{F}_S(|\psi\rangle) \leq \left(\mathop{\mathbb{E}}_{x\sim q_\psi}\left[|\langle\psi| W_x |\psi\rangle|^2\right]\right)^{1/6}. \tag{10}$$

This upper bound is enough to prove that Bell difference sampling provides a one-sided stabilizer tester. The rest of this note is concerned with providing a corresponding lower bound.

3 A Generalized Uncertainty Relation

In this section we introduce a generalized uncertainty relation, which we will use to prove our main result. Roughly speaking, we aim to generalize the following folklore relation for sets of mutually anti-commuting Weyl operators to arbitrary sets of Weyl operators:

Fact 14 (Folklore, Lemma 4.23 of [3]). *Let $\{A_i\}_{i=1}^M$ be a set of mutually anti-commuting Weyl operators. For any pure state $\psi = |\psi\rangle\langle\psi|$, we have that $\sum_{j=1}^M \operatorname{Tr}(\psi A_j)^2 \leq 1$.*

Let us now construct a generalization. Given an arbitrary set A of Weyl operators, define Γ_A as the *anti-commutation graph* of A. To be more specific, the vertex set of Γ_A is exactly A, and for any $A_i, A_j \in A$, they are connected by an edge if and only if A_i and A_j anti-commute.

Taking a slight detour, we can also define the set of "normalized Hamiltonians" associated with a set of Weyl operators A. We will be interested in the operator norm of these Hamiltonians, maximized over all possible Hamiltonians. For a set $A = \{A_i\}_{i=1}^M$ of Weyl operators, we define

$$\Psi_0(A) = \max_{a\in\mathbb{R}^M}\left\{\left\|H_A(a)^2\right\| \;\middle|\; H_A(a) = \sum_{i=1}^M a_i A_i, \|a\|_2 = 1\right\} \tag{11}$$

where $\left\|H_A(a)^2\right\| = \lambda_{\max}\left(H_A(a)^2\right)$, $\|a\|_2 = \left(\sum_{i=1}^M a_i^2\right)^{\frac{1}{2}}$. Our key observation is as follows:

Lemma 15. *Let $\{A_i\}_{i=1}^M$ be a set of Weyl operators. For any pure state $\psi = |\psi\rangle\langle\psi|$, we have that*

$$\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 \leq \Psi_0(A). \tag{12}$$

Proof. Consider the vector $w \in \mathbb{R}^M$ where $w_i := \operatorname{Tr}(\psi A_i) = \langle\psi| A_i |\psi\rangle$. Notice that

$$\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 = \sum_{i=1}^M \langle\psi| A_i |\psi\rangle\langle\psi| A_i |\psi\rangle = \langle\psi| \sum_{i=1}^M w_i A_i |\psi\rangle. \tag{13}$$

Let $H_A(w) = \sum_{i=1}^M w_i A_i$, we have

$$\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 = \langle\psi| \sum_{i=1}^M w_i A_i |\psi\rangle \leq \|H_A(w)\|. \tag{14}$$

Since $\|H_A(w)\| = \|w\|_2 \left\|H_A\left(\frac{w}{\|w\|_2}\right)\right\|$, we conclude that

$$\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 \leq \|w\|_2 \left\|H_A\left(\frac{w}{\|w\|_2}\right)\right\| \leq \|w\|_2 \sqrt{\Psi_0(A)}, \tag{15}$$

since $\|w/\|w\|_2\|_2 = 1$. Combining that $\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 = \|w\|_2^2$, we can rearrange and square the above to obtain the lemma statement. □

We note that this quantity was also studied by [1] under the name "commutation index". The uncertainty relation we are about to show was also discovered independently (and earlier) in [6]. Next, we want to relate the quantity $\Psi_0(A)$ to a property of the anti-commutation graph Γ_A. To do this, we leverage a result by Hastings & O'Donnell [13], derived in the context of fermionic Hamiltonian optimization. Concretely, we need the following definition and proposition.

Definition 16 (Definition 4.6 of [13]). For a graph $\Gamma = ([M], E)$, we define

$$\Psi(\Gamma) = \max_{a\in\mathbb{R}^M}\left\{\operatorname{Opt}\left(l^2\right) \;\middle|\; l = \sum_{i=1}^M a_i \chi_i \in \mathfrak{C}(\Gamma), \|a\|_2 = 1\right\}, \tag{16}$$

where $\|a\|_2 = \left(\sum_{i=1}^M a_i^2\right)^{\frac{1}{2}}$.

Here, $\mathfrak{C}(\Gamma)$ is any matrix representation of the anti-commutation relations encoded by the graph Γ. Note that in particular, any set of Weyl operators A is a representation of its anti-commutation graph Γ_A (this is discussed in greater detail in Section 2.6 of [13]). Furthermore, this implies that $\Psi_0(\Gamma) \leq \Psi(\Gamma)$ and the following graph-theoretic characterization is also provided:

Proposition 17 (Proposition 4.8 from [13]). *For any graph Γ, we have $\Psi(\Gamma) \leq \vartheta(\Gamma)$.*

With this we can show our generalized uncertainty relation.

Lemma 18 (Generalized uncertainty relation). *Let $\{A_i\}_{i=1}^M$ be a set of Weyl operators with an associated anti-commutation graph Γ_A. For any pure state $\psi = |\psi\rangle\langle\psi|$, we have that*

$$\sum_{i=1}^M \operatorname{Tr}(\psi A_i)^2 \leq \Psi_0(A) \leq \Psi(\Gamma_A) \leq \vartheta(\Gamma_A). \tag{17}$$

Proof. The first inequality is directly from Lemma 15. By definition, we have $\Psi_0(\Gamma_A) \leq \Psi(\Gamma_A)$, which is the second inequality. The last inequality follows from Proposition 17. □

4 A Tolerant Testing Algorithm

In this section we prove our main theorem. We start from the core fact derived in [3], namely that if Bell difference sampling succeeds with high probability, there exists a subspace $V \subset \mathbb{F}_2^{2n}$ of Weyl operators with high expected probability mass under the characteristic distribution p_ψ:

Theorem 19. *Let $|\psi\rangle$ be an n-qubit quantum state such that $\mathbb{E}_{x\sim q_\psi}\left[2^n p_\psi(x)\right] \geq \gamma$ for $\gamma \in [0,1]$ and $2^n \geq \frac{C'' \ln(C'''/\gamma)}{\gamma^3}$ with C'', C''' some constants. Then there exists a subspace V of $\mathbb{F}_2^{2n}$ such that:*

$$\sum_{x\in V} |\langle\psi| W_x |\psi\rangle|^2 \geq C_1 \gamma^{49} |V|, \tag{18}$$

and

$$\sum_{x\in V} |\langle\psi| W_x |\psi\rangle|^2 \geq C_2\gamma^{51}2^n, \tag{19}$$

with C_1 *and* C_2 *some constants.*

We prove this theorem in the appendix. A version of this theorem, that does not include the mild n dependence, can also be proven by following the logic of [3] through their Section 4 towards Corollary 4.11, and Claims 4.12 and 4.13 (together with Lemma 3.3), and taking care to tally up all powers of γ (which is not done explicitly in [3]). This yields a similar theorem but with powers of γ equal to 361 and 368 instead of 49 and 51.

Our goal will now be to find an isotropic subspace V_0 of the subspace V that also has a large probability mass. We will do this by providing an upper bound and a lower bound on the Lovász theta of the anti-commutation graph Γ_V of (Weyl operators associated to) the subspace V. To do this we note that for the Weyl operators associated to a subspace V there exist integers m, k (with $k+m \leq n$) and an n-qubit Clifford unitary U such that (abusing notation somewhat):

$$UVU^\dagger = \langle Z_1, X_1, \ldots, Z_k, X_k, Z_{k+1}, \ldots, Z_{k+m}\rangle \overset{\text{def}}{=} W. \tag{20}$$

where P_i is a Pauli operator on the i'th qubit. With this structure, and the uncertainty relation we derived above we can control $\vartheta(\Gamma_W) = \vartheta(\Gamma_V)$ from both above and below.

Lemma 20. *Let* W, k, m *be defined as above, with associated anti-commutation graph* Γ_W*. For any pure state* $\psi = |\psi\rangle\langle\psi|$*, we have that*

$$C_1\gamma^{49}|W| \leq \sum_{x\in W} \mathrm{Tr}(\psi W_x)^2 \leq \vartheta(\Gamma_W) \leq \frac{|W|}{2^k} = 2^{k+m}. \tag{21}$$

Proof. The lower bound is given by Lemma 18 and Theorem 19. It is thus sufficient to show $\vartheta(\Gamma_W) \leq \frac{|W|}{2^k}$. It is straightforward to see that

$$\Gamma_W \supseteq \Gamma_{\mathcal{P}_k} \boxtimes \overline{K_{2^m}}, \tag{22}$$

where $\Gamma_{\mathcal{P}_k}$ is the anti-commutation graph of the (Weyl operators in the) k-fold Pauli group, and $\overline{K_{2^m}}$ is the complement graph of the complete graph with 2^m vertices. According to properties of the Lovász theta (Fact 5, Fact 3), we have

$$\vartheta(\Gamma_W) \leq \vartheta\left(\Gamma_{\mathcal{P}_k} \boxtimes \overline{K_{2^m}}\right) = \vartheta(\Gamma_{\mathcal{P}_k}) \cdot \vartheta\left(\overline{K_{2^m}}\right). \tag{23}$$

Note that $\Gamma_{\mathcal{P}_k}$ is actually the complement graph of the *symplectic graph* $\mathrm{Sp}(2k, 2)$ defined in [20] with one extra isolated vertex (corresponding to the identity operator). According to Fact 4 we have $\vartheta(\Gamma_{\mathcal{P}_k}) = \vartheta\left(\overline{\mathrm{Sp}(2k,2)}\right) + 1$. With $\vartheta\left(\overline{\mathrm{Sp}(2k,2)}\right) = 2^k - 1$ (from Theorem 3.29 of [20]), $\vartheta\left(\overline{K_{2^m}}\right) = 2^m$ (directly from the definition of ϑ), and $|W| = 2^{2k+m}$, we conclude that

$$\vartheta(\Gamma_W) \leq 2^{k+m} = \frac{|W|}{2^k}. \tag{24}$$

□

As a conclusion of this section, We have the following corollary, which will be used to prove a polynomial gap tolerant testing theorem for stabilizer states.

Corollary 21. *Let* $|\psi\rangle$ *be a pure state, and let* V *be the subspace given in Theorem 19, with associated anti-commutation graph* Γ_V*. There exists an isotropic subspace* $V_0 \subseteq V$*, such that*

$$\sum_{x\in V_0} \mathrm{Tr}(\psi W_x)^2 \geq \frac{C_1\gamma^{49}}{1+C_1\gamma^{49}} \sum_{x\in V} \mathrm{Tr}(\psi W_x)^2. \tag{25}$$

Proof. By Lemma 20 and Equation (18), we have that

$$C_1\gamma^{49} \cdot |V| \leq \sum_{x\in V} \mathrm{Tr}(\psi W_x)^2 \leq \vartheta(\Gamma_V) \leq \frac{|V|}{2^k}, \tag{26}$$

which implies $2^k \leq \frac{1}{C_1}\gamma^{-49}$. As a direct consequence of Lemma 12 from [16], we can thus cover V with 2^k+1 isotropic subspaces of V. Therefore there must exist a specific isotropic $V_0 \subseteq V$, such that

$$\sum_{P\in V_0} \mathrm{Tr}(\psi P)^2 \geq \frac{1}{2^k+1} \sum_{P\in V} \mathrm{Tr}(\psi P)^2 \geq \frac{C_1\gamma^{49}}{1+C_1\gamma^{49}} \sum_{P\in V} \mathrm{Tr}(\psi P)^2. \tag{27}$$

□

Note that the existence of V_0 lower bounds the stabilizer fidelity of $|\psi\rangle$, since we can always extend this isotropic subspace to a Lagrangian subspace, which gives rise to a stabilizer state. This leads to the main theorem.

Theorem 22. *Let* $|\psi\rangle$ *be a state and let* $\gamma = \mathbb{E}_{x\sim q_\psi}\left[2^n p_\psi(x)\right]$*. Then there exists some constant* C*, such that*

$$C\gamma^{100} \leq \mathcal{F}_S(|\psi\rangle) \leq \gamma^{\frac{1}{6}}. \tag{28}$$

Proof. The second inequality is exactly Fact 13. We will prove the first inequality. We begin by padding $|\psi\rangle$ with $|0\rangle$ states such that $2^n \geq \frac{C'' \ln(C'''/\gamma)}{\gamma^3}$. Note that this leaves the stabilizer fidelity unchanged (this follows from the contraction identity in App. G of [14]). Also note that $\gamma \geq \mathcal{F}_S(|\psi\rangle)^6 \geq 2^{-6n}$, so this never requires more that cn qubits to do[2]. From Theorem 19 and Corollary 21, there exists a subspace V, an isotropic subspace V_0 and constants C_1, C_2, such that:

$$\sum_{x\in V_0} \mathrm{Tr}(\psi W_x)^2 \geq \frac{C_1\gamma^{49}}{1+C_1\gamma^{49}} \sum_{x\in V} \mathrm{Tr}(\psi W_x)^2 \tag{29}$$

$$\geq \frac{C_1\gamma^{49}}{1+C_1\gamma^{49}} C_2\gamma^{51}2^n \tag{30}$$

$$= \frac{C_1C_2\gamma^{100}}{1+C_1\gamma^{49}} 2^n \tag{31}$$

We can extend V_0 to a Lagrangian subspace V_0^* such that

$$\sum_{x\in V_0^*} p_\psi(x) = \sum_{x\in V_0^*} \frac{\mathrm{Tr}(\psi W_x)^2}{2^n} \geq \frac{C_1C_2\gamma^{100}}{1+C_1\gamma^{49}} \tag{32}$$

Following Proposition 10, we conclude that

$$\mathcal{F}_S(|\psi\rangle) \geq \frac{C_1C_2\gamma^{100}}{1+C_1\gamma^{49}} \geq \frac{C_1C_2\gamma^{100}}{1+C_1} = C\gamma^{100}, \tag{33}$$

where $C = \frac{C_1C_2}{1+C_1}$. □

[2] This padding procedure is a technical trick to overcome the large-n requirement in the proof of Theorem 19. We believe this is a proof artifact. In fact it can be removed by using the version of Theorem 19 from [3], at the cost of a substantially higher power of γ.

From this we can obtain a tolerant testing algorithm. The argument is standard, but we include it for completeness, and to get an explicit value for the polynomial degree in the gap. For the proof of Theorem 1 we need a standard Chernoff bound:

Lemma 23 (Chernoff-Hoeffding)**.** *Let $X_1, \dots, X_m$ be independent random variables such that $a \leq X_i \leq b$ almost surely for all i. Then,*

$$\mathbb{P}\left(\left|\frac{1}{m}\sum_{i=1}^{m} X_i - \mathbb{E}\left[\frac{1}{m}\sum_{i=1}^{m} X_i\right]\right| \geq \delta\right) \leq 2e^{-\frac{2\delta^2 m}{(b-a)^2}} \tag{34}$$

Theorem 1. *Let $\epsilon_1, \epsilon_2 \in [0,1]$ and let $|\psi\rangle$ be a state with stabilizer fidelity*

$$\mathcal{F}_S(|\psi\rangle) := \max_{|S\rangle \in \mathrm{STAB_n}} |\langle\psi|S\rangle|^2, \tag{1}$$

either (1) larger than ϵ_1 or (2) smaller than ϵ_2. If $\epsilon_2 \leq C'\epsilon_1^{600}$ for some constant C', then $O\big(\epsilon_1^{-12}\big)$ rounds of Bell difference sampling can distinguish between case (1) and case (2) with probability greater than $2/3$.

Proof. Let $\gamma = \mathbb{E}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right]$. We choose D_1, D_2 such that

$$\begin{aligned} D_1 &:= \epsilon_1^6, \\ D_2 &:= \left(\frac{\epsilon_2}{C}\right)^{1/100}, \end{aligned} \tag{35}$$

where C is the constant from Theorem 22. We define $D := \frac{D_1+D_2}{2}$. The algorithm now does the following: We perform Bell sampling m times, obtaining samples $x_1, \dots, x_m$ to compute an estimate $\overline{\gamma}$ of the expectation value. The $x_1, \dots, x_m$ are Bernoulli distributed with mean $p_{\text{accept}} = \frac{1}{2} + \frac{1}{2}\gamma$ (see Equation (9)). We will set our estimate $\overline{\gamma}$ to be

$$\overline{\gamma} = \frac{1}{m}\sum_{i=1}^{m}(2x_i - 1). \tag{36}$$

Note that $\mathbb{E}[\overline{\gamma}] = \gamma$. We make the following decisions based on this data:

- If $\overline{\gamma} \geq D$, we output $\mathcal{F}_S(|\psi\rangle) \geq \epsilon_1$,
- If $\overline{\gamma} < D$, we output $\mathcal{F}_S(|\psi\rangle) \leq \epsilon_2$.

From the promise we know that either $\mathcal{F}_S(|\psi\rangle) \geq \epsilon_1$, or that $\mathcal{F}_S(|\psi\rangle) \leq \epsilon_2$. Suppose that (1) $\mathcal{F}_S(|\psi\rangle) \geq \epsilon_1$, then by Theorem 22:

$$\gamma^{1/6} \geq \mathcal{F}_S(|\psi\rangle) \geq \epsilon_1. \tag{37}$$

Thus $\gamma \geq D_1$. On the other hand, if (2) $\mathcal{F}_S(|\psi\rangle) \leq \epsilon_2$, then, again by Theorem 22,

$$C\gamma^{100} \leq \mathcal{F}_S(|\psi\rangle) \leq \epsilon_2. \tag{38}$$

Thus $\gamma \leq D_2$. This tells us that

$$\gamma \leq D_2 \text{ or } D_1 \leq \gamma. \tag{39}$$

Now suppose that $\mathcal{F}_S(|\psi\rangle) \geq \epsilon_1$, but $\overline{\gamma} < D$. Then the true value of γ is greater than or equal to D_1. Therefore, the difference $|\overline{\gamma}-\gamma| \geq \alpha$, where we define $\alpha = \frac{D_1-D_2}{3}$. We set $C' = \frac{C}{2^{100}}$. By assumption we have that $\epsilon_2 \leq \frac{C}{2^{100}}\epsilon_1^{600}$. Equivalently, $\left(\frac{\epsilon_2}{C}\right)^{1/100} \leq \frac{1}{2}\epsilon_1^6$, so $D_2 \leq \frac{1}{2}D_1$. Therefore, it holds that $D_1 - D_2 \geq \frac{1}{2}D_1$, so $\alpha \geq \frac{1}{6}D_1$. Similarly, suppose that $\mathcal{F}_S(|\psi\rangle) \leq \epsilon_2$, but $\overline{\gamma} \geq D$. Then the true value of γ is less than or equal to D_2. Therefore, the difference $|\overline{\gamma} - \gamma| \geq \alpha$. So using the a Chernoff-Hoeffding bound (Lemma 23) with $a = -1, b = 1$, we can upper bound the probability that the algorithm makes a mistake by

$$\mathbb{P}\left(|\overline{\gamma} - \gamma| \geq \alpha\right) \leq 2e^{-\frac{1}{2}\alpha^2 m} \leq 2e^{-\frac{1}{72}\epsilon_1^{12} m}. \tag{40}$$

Now assuming that $m \geq \frac{\log(3)72}{\epsilon_1^{12}}$, this probability is lower than $1/3$. □

Acknowledgements

We would like to thank the Qusoft testing & learning reading group: Jop Briët, Amira Abbas, Yanlin Chen, Niels Neumann, Davi Castro-Silva & Jeroen Zuiddam, without whom this paper would not have been written. We also thank Krystal Guo and Māris Ozols for teaching us about symplectic graphs. JH would like to thank Johannes Jakob Meyer for pointing out reference [1], and Carlos de Gois for alerting us to his work [6] after we put out a first version of this paper. JH acknowledges funding from the Dutch Research Council (NWO) through a Veni grant (grant No.VI.Veni.222.331) and the Quantum Software Consortium (NWO Zwaartekracht Grant No.024.003.037). ZB is supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme (KAT2).

A An Improved Bound on the Polynomial Degree

In this section we present an improvement to the degree of the polynomial gap of the tester, beyond what can be achieved by directly relying on the work of [3] (summarized below Theorem 19). We will almost entirely retrace their argument but obtain various parametric improvements and simplifications. The main bottleneck in obtaining a lower degree polynomial relationship is the black box use of theorems from additive combinatorics. It is unclear how this can be fully avoided.

A.1 Obtaining a Large Nearly Linear Subset

The main contribution of this appendix is a sharply refined version of Theorem 4.5 of [3], which shows the existence of a large set $S \subseteq \mathbb{F}_2^{2n}$ that is nearly linear (in a precise probabilistic sense) and has large point-wise probability mass under the characteristic distribution p_ψ. We believe that our version of this result is optimal (at least with respect to its scaling with γ). We note that the techniques in this theorem could also be used to parametrically improve the landmark result on low degree testing from Samorodnitsky[19]. We have the following:

Theorem 24. *Let $|\psi\rangle$ be an n-qubit quantum state. Then if $\mathbb{E}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \geq \gamma$, and $2^n \geq \frac{C''\ln(C'''/\gamma)}{\gamma^3}$ with C'', C'' some constants, there exists a set $S \subseteq \mathbb{F}_2^{2n}$ such that*

(1) $|S| \geq \frac{\gamma}{2}2^n$,
(2) For all $x \in S$, $2^n p_\psi(x) \geq \frac{\gamma}{4}$,
(3) $\mathbb{P}_{s,s'\in S}[s + s' \in S] \geq \frac{\gamma}{6}$.

Proof. We begin by defining the set:

$$X = \left\{x \in \mathbb{F}_2^{2n} : 2^n p_\psi(x) \geq \frac{\gamma}{4}\right\}. \tag{41}$$

We prove that this set is large, and then construct S as a random subset of X. It is clear that $\frac{\gamma}{4}|X| \le \sum_{x\in X} 2^n p_\psi(x) \le \sum_{x\in\mathbb{F}_2^{2n}} 2^n p_\psi(x) = 2^n$. This implies that $|X| \le \frac{4}{\gamma}2^n$. Furthermore, we can lower bound $|X|$ using Markov's inequality:

$$\gamma \le \mathop{\mathbb{E}}_{x\sim q_\psi}\left[2^n p_\psi(x)\right] \le \mathop{\mathbb{P}}_{x\sim q_\psi}\left[2^n p_\psi(x) \ge \frac{\gamma}{4}\right] + \frac{\gamma}{4}. \tag{42}$$

Since $q_\psi(x) \le 2^{-n}$ for all x, we have

$$\mathop{\mathbb{P}}_{x\sim q_\psi}\left[2^n p_\psi(x) \ge \frac{\gamma}{4}\right] = \sum_{x\in X} q_\psi(x) \le |X|2^{-n}. \tag{43}$$

Combining the above we obtain a lower bound:

$$|X| \ge \frac{3}{4}\gamma \cdot 2^n. \tag{44}$$

Next we construct the set S. This is done through a sampling process on X. We take every $x \in X$, and independently randomly decide to include $x \in S$ with probability $2^n p_\psi(x)$. We will now prove that S satisfies the three properties of the theorem statement with non-zero probability. Note that the second property is automatically satisfied, since $S \subseteq X$.

The rest of the argument is probabilistic (over the random choice of S). We begin by calculating the expected size of S. It's easy to see that

$$\begin{aligned}\mathop{\mathbb{E}}_{S}[|S|] = \sum_{x\in X} 2^n p_\psi(x) &= 2^n \mathop{\mathbb{P}}_{x\sim p_\psi}[x\in X] &(45)\\ &= 2^n \mathop{\mathbb{P}}_{x\sim p_\psi}\left[2^n p_\psi(x) \ge \frac{\gamma}{4}\right]. &(46)\end{aligned}$$

Furthermore, from Proposition 12 we know that $\mathbb{E}_{x\sim q_\psi}\left[2^n p_\psi(x)\right] \le \mathbb{E}_{x\sim p_\psi}\left[2^n p_\psi(x)\right]$. According to Markov's inequality, we have

$$\begin{aligned}\gamma \le \mathop{\mathbb{E}}_{x\sim q_\psi}\left[2^n p_\psi(x)\right] &\le \mathop{\mathbb{E}}_{x\sim p_\psi}\left[2^n p_\psi(x)\right] &(47)\\ &\le \mathop{\mathbb{P}}_{x\sim p_\psi}\left[2^n p_\psi(x) \ge \frac{\gamma}{4}\right] + \frac{\gamma}{4}. &(48)\end{aligned}$$

Therefore $\mathbb{E}_S[|S|] \ge \frac{3}{4}\gamma \cdot 2^n$. Next we compute the expected "linearity" of S. In this argument we will need an upper bound on the size of S, which we will indirectly obtain from its expected size. Let λ be a constant, which we will choose later, and define A to be the event $\{|S| < (1+\lambda)\,\mathbb{E}_S[|S|]\}$.

Now we can compute the linearity. Define

$$L(S) = \mathop{\mathbb{P}}_{s,s'\in S}\left[s + s' \in S\right]. \tag{49}$$

We calculate the expected linearity $\mathbb{E}_S[L(S)]$ as follows:

$$\begin{aligned}&\mathop{\mathbb{E}}_{S}[L(S)] &(50)\\ &= \mathop{\mathbb{E}}_{S}\left[|S|^{-2}\sum_{x,y\in S}\mathbb{1}[x+y\in S]\right] &(51)\\ &= \mathop{\mathbb{E}}_{S}\left[|S|^{-2}\sum_{x,y\in X}\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\right] &(52)\\ &\ge \mathop{\mathbb{E}}_{S}\left[|S|^{-2}\sum_{x,y\in X}\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\mathbb{1}[A]\right] &(53)\\ &\ge \frac{2^{-2n}}{(1+\lambda)^2}\mathop{\mathbb{E}}_{S}\left[\sum_{x,y\in X}\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\mathbb{1}[A]\right] &(54)\end{aligned}$$

where the last inequality follows from $|S| \le (1+\lambda)\,\mathbb{E}_S[|S|]$ and $\mathbb{E}_S[|S|] = 2^n\,\mathbb{P}_{x\sim p_\psi}[x\in X] \le 2^n$. We can continue this calculation:

$$\begin{aligned}&\mathop{\mathbb{E}}_{S}\left[\sum_{x,y\in X}\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\mathbb{1}[A]\right] &(55)\\ &= \sum_{x,y\in X}\mathop{\mathbb{E}}_{S}[\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\mathbb{1}[A]] &(56)\\ &\ge \sum_{x,y\in X}\left(\mathop{\mathbb{E}}_{S}[\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]] - \mathop{\mathbb{P}}_{S}\left[\bar{A}\right]\right) &(57)\\ &= \sum_{x,y\in X}\mathop{\mathbb{E}}_{S}[\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]] - |X|^2\mathop{\mathbb{P}}_{S}\left[\bar{A}\right]. &(58)\end{aligned}$$

Let us now compute $\mathbb{P}_S\left[\bar{A}\right]$. From Hoeffding's inequality, and the bounds $\mathbb{E}_S[|S|] \ge \frac{3}{4}\gamma\cdot 2^n$ and $|X| \le \frac{4}{\gamma}2^n$, we have that

$$\begin{aligned}\mathop{\mathbb{P}}_{S}\left[\bar{A}\right] = \mathop{\mathbb{P}}_{S}\left[|S| \ge \mathop{\mathbb{E}}_{S}[|S|] + \lambda\mathop{\mathbb{E}}_{S}[|S|]\right] &\le \exp\left\{-\frac{2\lambda^2(\mathbb{E}_S[|S|])^2}{|X|}\right\} &(59)\\ &\le \exp\left\{-\frac{2\lambda^2\frac{9}{16}\gamma^2\cdot 2^{2n}}{\frac{4}{\gamma}2^n}\right\} &(60)\\ &= \exp\left\{-9\lambda^2\gamma^3 2^{n-5}\right\}. &(61)\end{aligned}$$

Next we address the other term in Equation (58):

$$\begin{aligned}&\sum_{x,y\in X}\mathop{\mathbb{E}}_{S}\left[\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\right] &(62)\\ &= \sum_{\substack{x,y\in X;\\ x+y\in X}}\mathop{\mathbb{E}}_{S}\left[\mathbb{1}[x\in S]\mathbb{1}[y\in S]\mathbb{1}[x+y\in S]\right] &(63)\\ &\ge \sum_{\substack{x,y\in X;\\ x+y\in X}} 2^{3n}p_\psi(x)p_\psi(y)p_\psi(x+y) &(64)\\ &= 2^{2n}\sum_{\substack{x,y\in X;\\ x+y\in X}} 2^n p_\psi(x)p_\psi(y)p_\psi(x+y). &(65)\end{aligned}$$

To evaluate this last sum, we relate it to the related sum over $\mathbb{F}_2^{2n}$ (as opposed to X). Note that we have

$$\sum_{x,y\in\mathbb{F}_2^{2n}} 2^n p_\psi(x)p_\psi(y)p_\psi(x+y) = \mathop{\mathbb{E}}_{x\sim q_\psi}\left[|\langle\psi|W_x|\psi\rangle|^2\right] \ge \gamma. \tag{66}$$

Relating this sum to the summation in Equation (65) requires bounding three residual sums:

$$\sum_{x,y\in\mathbb{F}_2^{2n};x\notin X} 2^n p_\psi(x)p_\psi(y)p_\psi(x+y) \leq \frac{\gamma}{4}\sum_{x,y\in\mathbb{F}_2^{2n}} p_\psi(y)p_\psi(x+y) = \frac{\gamma}{4}, \tag{67}$$

$$\sum_{x,y\in\mathbb{F}_2^{2n};y\notin X} 2^n p_\psi(x)p_\psi(y)p_\psi(x+y) \leq \frac{\gamma}{4}\sum_{x,y\in\mathbb{F}_2^{2n}} p_\psi(x)p_\psi(x+y) = \frac{\gamma}{4}, \tag{68}$$

$$\sum_{x,y\in\mathbb{F}_2^{2n};x\notin X} 2^n p_\psi(x)p_\psi(y)p_\psi(x+y) \leq \frac{\gamma}{4}\sum_{x,y\in\mathbb{F}_2^{2n}} p_\psi(y)p_\psi(x+y) = \frac{\gamma}{4}. \tag{69}$$

Combining these and working out we obtain the lower bound:

$$\mathop{\mathbb{E}}_S[L(S)] \geq \frac{1}{(1+\lambda)^2}\left(\gamma - \frac{3}{4}\gamma - 2^{-2n}|X|^2 e^{-9\lambda^2\gamma^3 2^{n-5}}\right) \tag{70}$$

$$\geq \frac{1}{(1+\lambda)^2}\left(\frac{1}{4}\gamma - \frac{16}{\gamma^2}e^{-9\lambda^2\gamma^3 2^{n-5}}\right). \tag{71}$$

Fix $\lambda = 0.01$, for n such that $2^n \geq \frac{320000}{9}\cdot\frac{3\ln(1/\gamma)+\ln 1600}{\gamma^3} = \frac{C''\ln(C'''/\gamma)}{\gamma^3}$ with C' and C'' some constants, we have $\mathbb{E}_S[L(S)] \geq \frac{\gamma}{5}$. Using the Chernoff bound, Markov's inequality, and the union bound, we conclude that there exists S, such that $|S| \geq \frac{\gamma}{2}\cdot 2^n$ and $\mathbb{P}_{s,s'\in S}[s+s'\in S] \geq \frac{\gamma}{6}$. □

A.2 Proof of Theorem 19

Using Theorem 24 we can prove Theorem 19. This argument is exactly that of [3], chaining together the Balog-Szemeredi-Gowers and polynomial Freiman-Rusza theorems to obtain a subspace $V \subseteq \mathbb{F}_2^{2n}$ with appropriate parameters. We include it here in the interest of presenting a self-contained narrative.

Theorem 19. *Let $|\psi\rangle$ be an n-qubit quantum state such that $\mathbb{E}_{x\sim q_\psi}\left[2^n p_\psi(x)\right] \geq \gamma$ for $\gamma\in[0,1]$ and $2^n \geq \frac{C''\ln(C'''/\gamma)}{\gamma^3}$ with C'', C''' some constants. Then there exists a subspace V of $\mathbb{F}_2^{2n}$ such that:*

$$\sum_{x\in V}|\langle\psi|W_x|\psi\rangle|^2 \geq C_1\gamma^{49}|V|, \tag{18}$$

and

$$\sum_{x\in V}|\langle\psi|W_x|\psi\rangle|^2 \geq C_2\gamma^{51}2^n, \tag{19}$$

with C_1 and C_2 some constants.

Proof. We use Theorem 24 to guarantee the existence of a set S (with the properties given in Theorem 24. As we disussed there, this set is nearly linear. We can apply the Balog-Szemeredi-Gowers theorem to S, to give us another set S' which is of similar size and has *small doubling* (meaning the set $S'+S' := \{s+\hat{s} : s,\hat{s}\in S'\}$ is not much bigger than S'. Concretely the BSG theorem (adapted from [21]) is stated as follows:

Theorem 25 (Balog-Szemeredi-Gowers, modified form [4, 5, 7])**.** *Let $S \subseteq \mathbb{F}_2^{2n}$ such that $\mathbb{P}_{s,s'\in S}[s+s'\in S] \geq \epsilon$, then there exists a subset $S' \subseteq S$, such that*

(1) $|S'| \geq \frac{\epsilon}{2\sqrt{2}}|S|$,

(2) $\frac{|S'+S'|}{|S'|} \leq 8\left(\frac{1}{\varepsilon}\right)^6$.

The proof for this form of BSG theorem is based on [5], is postponed to Appendix C. We apply this theorem with $\epsilon = \frac{\gamma}{6}$ to obtain a set S' with $|S'| \geq \frac{\gamma}{18}|S|$ and $\frac{|S'+S'|}{|S'|} \leq \left(\frac{36}{\gamma}\right)^6$.

The next step is to argue that a set of small doubling can be covered by a few translates of a subspace V. This is the content of the polynomial Freiman-Ruzsa theorem.

Theorem 26 (Polynomial Freiman-Ruzsa [8, 9])**.** *If a set $S' \subseteq \mathbb{F}_2^{2n}$ has doubling constant at most K, then there exists a subspace V of $\mathbb{F}_2^{2n}$ with the follwing properties:*

(1) $|V| \leq |S'|$,

(2) S' is covered by at most $(2K)^8$ translates of V.

We apply the Polynomial Freiman-Ruzsa theorem to S', with $K = \left(\frac{36}{\gamma}\right)^9$, yielding a subspace $V \subseteq \mathbb{F}_2^{2n}$. Now by the pigeonhole principle, there must exist a translate of V, say $V+y$, that contains at least $\frac{1}{(2K)^8}|S'|$ members of S'. Each element $x\in S'$ has $p_\psi(x) \geq 2^{-n}\frac{\gamma}{4}$, so

$$\frac{1}{|V+y|}\sum_{x\in V+y}p_\psi(x) \geq \frac{1}{|V|}\sum_{x\in(V+y)\cap S'}2^{-n}\gamma/4 \tag{72}$$

$$\geq \frac{1}{|V|}(2K)^{-8}|S'|2^{-n}\frac{\gamma}{4} \tag{73}$$

$$\geq (2K)^{-8}2^{-n}\frac{\gamma}{4}. \tag{74}$$

So we have

$$\mathop{\mathbb{E}}_{x\in V+y}p_\psi(x) \geq (2K)^{-8}2^{-n}\frac{\gamma}{4} = C_1\gamma^{73}2^{-n}, \tag{75}$$

for some constant C_1. Through a clever little argument in [3] (Corollary 4.11), we have that this value is even larger on V:

$$\mathop{\mathbb{E}}_{x\in V}p_\psi(x) \geq \mathop{\mathbb{E}}_{x\in V+y}p_\psi(x) \geq C_1\gamma^{73}2^{-n}. \tag{76}$$

If we rewrite this equation we get

$$\sum_{x\in V}|\langle\psi|W_x|\psi\rangle|^2 \geq C_1\gamma^{73}|V|. \tag{77}$$

Besides,

$$\sum_{x\in V}|\langle\psi|W_x|\psi\rangle|^2 \geq (2K)^{-8}\sum_{x\in S'}|\langle\psi|W_x|\psi\rangle|^2 \tag{78}$$

$$\geq (2K)^{-8}\frac{\gamma}{4}|S'|. \tag{79}$$

Note that $|S'| \geq \frac{\varepsilon}{3}\cdot|S| \geq \frac{\varepsilon}{3}\cdot\frac{\gamma}{2}2^n$, we conclude that

$$\sum_{x\in V}|\langle\psi|W_x|\psi\rangle|^2 \geq (2K)^{-8}\frac{\gamma}{4}\cdot\frac{\varepsilon}{3}\cdot\frac{\gamma}{2}2^n = C_2\gamma^{75}2^n. \tag{80}$$

□

B Proof of Proposition 10

Proposition 10 (Proof of Theorem 3.3 of [12], Corollary 7.4 of [11])**.** *Let V be a Lagrangian subspace of $\mathbb{F}_2^{2n}$. Then,*

$$\mathcal{F}_S(|\psi\rangle) \ge \sum_{x\in V} p_\psi(x). \tag{6}$$

where $p_\psi(x) = 2^{-n}|\langle\psi|W_x|\psi\rangle|^2$ is the characteristic distribution of $|\psi\rangle$ (see below).

Proof. Let V be Lagrangian subspace of $\mathbb{F}_2^n$. Then let $\{|\phi_\alpha\rangle\}_{\alpha\in\mathbb{F}_2^n}$ be the basis of eigenstates of the matrices $\{W_x : x\in V\}$. For each α, $|\phi_\alpha\rangle$ is a stabilizer state. Every $x\in V$ corresponds to a unique linear function $f_x : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$W_x = \sum_\alpha (-1)^{f_x(\alpha)}\,|\phi_\alpha\rangle\langle\phi_\alpha| \tag{81}$$

Now we have, setting $\psi = |\psi\rangle\langle\psi|$,

$$\begin{aligned}\mathcal{F}_S(|\psi\rangle) &\ge \max_\alpha \langle\phi_\alpha|\,\psi\,|\phi_\alpha\rangle &(82)\\ &= \max_\alpha \langle\phi_\alpha|\,\psi\,|\phi_\alpha\rangle \sum_\beta \left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle &(83)\\ &\ge \sum_\beta \left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle^2. &(84)\end{aligned}$$

We show that $2^n\sum_\beta \left|\phi_\beta\right\rangle\left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right| = \sum_{x\in V} W_x\psi W_x^\dagger$:

$$\begin{aligned}\sum_{x\in V} W_x\psi W_x^\dagger &= \sum_{x\in V}\sum_{\alpha,\beta\in\mathbb{F}_2^n} (-1)^{f_x(\alpha+\beta)}\,|\phi_\alpha\rangle\langle\phi_\alpha|\,\psi\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right| &(85)\\ &= \sum_{\alpha,\beta\in\mathbb{F}_2^n} 2^n\mathbb{1}[\alpha=\beta]\,|\phi_\alpha\rangle\langle\phi_\alpha|\,\psi\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right| &(86)\\ &= \sum_{\beta\in\mathbb{F}_2^n} 2^n\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right|. &(87)\end{aligned}$$

Now

$$\mathrm{Tr}\left[\left(\frac{1}{2^n}\sum_{x\in V} W_x\psi W_x^\dagger\right)^2\right] \tag{88}$$

$$= \mathrm{Tr}\left[\left(\sum_{\beta\in\mathbb{F}_2^n}\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle\left\langle\phi_\beta\right|\right)^2\right] \tag{89}$$

$$= \sum_\beta \left\langle\phi_\beta\right|\psi\left|\phi_\beta\right\rangle^2, \tag{90}$$

and

$$\mathrm{Tr}\left[\left(\frac{1}{2^n}\sum_{x\in V} W_x\psi W_x^\dagger\right)^2\right] \tag{91}$$

$$= \frac{1}{2^{2n}}\mathrm{Tr}\left[\sum_{x,y\in V}\psi W_x^\dagger W_y\psi(W_x^\dagger W_y)^\dagger\right] \tag{92}$$

$$= \frac{1}{2^n}\mathrm{Tr}\left[\sum_{y\in V}\psi W_y\psi W_y^\dagger\right] = \sum_{y\in V} p_\psi(x). \tag{93}$$

□

C Proof of Modified BSG Theorem

Theorem 25 (Balog-Szemeredi-Gowers, modified form [4, 5, 7])**.** *Let $S\subseteq\mathbb{F}_2^{2n}$ such that $\mathbb{P}_{s,s'\in S}[s+s'\in S]\ge\epsilon$, then there exists a subset $S'\subseteq S$, such that*

(1) $|S'| \ge \frac{\epsilon}{2\sqrt{2}}|S|$,

(2) $\frac{|S'+S'|}{|S'|} \le 8\left(\frac{1}{\varepsilon}\right)^6$.

Proof. The proof is based on [5]. For $x\in S+S$, let $r(x) = \left|\{(a,b)\in S^2 : a+b=x\}\right|$. Note that

$$\sum_{x\in S} r(x) = |S|^2 \mathop{\mathbb{P}}_{s,s'\in S}\left[s+s'\in S\right] \ge \varepsilon|S|^2. \tag{94}$$

We uniformly randomly choose Z from S. Let $B = S\cap(S+Z)$. Let $S = \left\{(a,b)\in S^2 : r(a+b)\le c\varepsilon^2|S|\right\}$. We have

$$\mathbb{E}[|B|] = \frac{1}{|S|}\sum_{z\in S}|S\cap(S+z)| = \frac{1}{|S|}\sum_{z\in S} r(z) \ge \varepsilon|S|, \tag{95}$$

and

$$\begin{aligned}\mathbb{E}\left[\left|B^2\cap S\right|\right] &= \sum_{(a,b)\in S}\Pr[a\in B\wedge b\in B] &(96)\\ &= \sum_{(a,b)\in S}\Pr[a\in S+Z\wedge b\in S+Z] &(97)\\ &\le \sum_{(a,b)\in S}\frac{r(a+b)}{|S|} &(98)\\ &\le \sum_{(a,b)\in S} c\varepsilon^2 &(99)\\ &\le c\varepsilon^2|S|^2. &(100)\end{aligned}$$

To conclude,

$$\mathbb{E}\left[2c|B|^2 - \left|B^2\cap S\right|\right] \ge c\varepsilon^2|S|^2. \tag{101}$$

Therefore there exists z and B, such that $|B|\ge\frac{\varepsilon}{\sqrt{2}}|S|$ and $\left|B^2\cap S\right| \le 2c|B|^2$. Fix $c=\frac{1}{16}$, then we have B such that $|B|\ge\frac{\varepsilon}{\sqrt{2}}|S|$. Besides, let $\Gamma = (B\times B, E)$ be the bipartite graph with edge set

$$E = \left\{(a,b)\in B^2 : r(a+b)\ge\frac{\varepsilon^2}{16}|S|\right\}. \tag{102}$$

Then $|E| \ge \frac{7}{8}|B|^2$. Let $S'\subseteq B$ be the set of vertices with degree at least $\frac{3}{4}|B|$. Since $|E| = \sum_{x\in B}\deg(x)$, we have $|S'| \ge \frac{1}{2}|B| \ge \frac{\varepsilon}{2\sqrt{2}}|S|$. Furthermore, for every pair $a,b\in S'$, they share at least $\frac{1}{2}|B|$ common neighbors. We will show S' has small doubling number as follows. For each $u\in S'+S'$, let $(a_u,b_u)\in S'\times S'$ be a pair such that $a_u+b_u=u$. Then, the numbmer of quadruples $(a,b,c,d)\in S^4$ satisfying $(a+b)+(c+d)\in S'-S'$ is at least

$$\begin{aligned}\sum_{u\in S'+S'}\sum_{x\in B} r(a_u+x)r(b_u+x) &\ge \left|S'+S'\right|\left(\frac{1}{2}|B|\right)\left(\frac{\varepsilon^2}{16}|S|\right)^2 &(103)\\ &\ge \frac{1}{2\sqrt{2}}\varepsilon^5\left|S'+S'\right||S|^3. &(104)\end{aligned}$$

Since this number is at most $|S|^4$, we conclude that

$$\left|S'+S'\right| \le 2\sqrt{2}\varepsilon^{-5}|S| \le 8\varepsilon^{-6}\left|S'\right|. \tag{105}$$

□

References

[1] Eric R. Anschuetz, Chi-Fang Chen, Bobak T. Kiani, and Robbie King. 2024. Strongly interacting fermions are non-trivial yet non-glassy. arXiv:2408.15699

[2] Srinivasan Arunachalam, Sergey Bravyi, and Arkopal Dutt. 2024. A note on polynomial-time tolerant testing stabilizer states. arXiv:2410.22220

[3] Srinivasan Arunachalam and Arkopal Dutt. 2024. Towards tolerant testing stabilizer states. arXiv:2408.06289

[4] Antal Balog and Endre Szemerédi. 1994. A statistical theorem of set addition. *Combinatorica* 14, 3 (1994), 263–268. doi:10.1007/BF01212974

[5] Jop Briët. 2024. The Balog–Szemerédi–Gowers Lemma, Lecture notes in Additive Combinatorics. https://drive.google.com/file/d/1kX5wMe08OAJaXDu4dB9qXbJgXZhRA0f-/view

[6] Carlos de Gois, Kiara Hansenne, and Otfried Gühne. 2023. Uncertainty relations from graph theory. *Physical Review A* 107, 6 (2023), 062211. doi:10.1103/PhysRevA.107.062211

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

[8] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. 2023. On a conjecture of Marton. arXiv:2311.05762

[9] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. 2024. Marton's Conjecture in abelian groups with bounded torsion. arXiv:2404.02244

[10] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. 2023. Low-Stabilizer-Complexity Quantum States Are Not Pseudorandom. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPICS.ITCS.2023.64

[11] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. 2024. Improved stabilizer estimation via bell difference sampling. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. 1352–1363. doi:10.1145/3618260.3649738

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

[13] Matthew B Hastings and Ryan O'Donnell. 2022. Optimizing strongly interacting fermionic Hamiltonians. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 776–789. doi:10.1145/3519935.3519960

[14] Patrick Hayden, Sepehr Nezami, Xiao-Liang Qi, Nathaniel Thomas, Michael Walter, and Zhao Yang. 2016. Holographic duality from random tensor networks. *Journal of High Energy Physics* 2016, 11 (2016), 1–56. doi:doi.org/10.1007/JHEP11(2016)009

[15] Donald E. Knuth. 1993. The sandwich theorem. arXiv:math/9312214

[16] Debbie Leung, Laura Mancinska, William Matthews, Maris Ozols, and Aidan Roy. 2012. Entanglement can increase asymptotic rates of zero-error classical communication over classical channels. *Communications in Mathematical Physics* 311 (2012), 97–111. doi:10.1007/s00220-012-1451-x

[17] László Lovász. 1979. On the Shannon capacity of a graph. *IEEE Transactions on Information theory* 25, 1 (1979), 1–7. doi:10.1109/TIT.1979.1055985

[18] Saeed Mehraban and Mehrdad Tahmasbi. 2024. Improved bounds for testing low stabilizer complexity states. arXiv:2410.24202

[19] Alex Samorodnitsky. 2007. Low-degree tests at large distances. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*. 506–515. doi:10.1145/1250790.1250864

[20] Igal Sason. 2024. Observations on graph invariants with the Lovász ϑ-function. *AIMS Mathematics* 9, 6 (2024), 15385–15468. doi:10.3934/math.2024747

[21] Emanuele Viola. 2011. Selected results in additive combinatorics: An exposition. *Theory of Computing* (2011), 1–15. doi:10.4086/toc.gs.2011.003

Received 2024-11-04; accepted 2025-02-01