

# Stabilizer complexity of quantum states and connections with frame theory

Saeed Mehraban  
Tufts University

Based on joint work with Mehrdad Tahmasbi

AMS meeting 2026

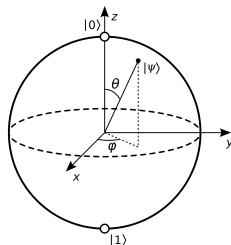
# Motivation

- Stabilizer states are central in quantum information science (error correction, simulation, etc).
- **This talk:** “View stabilizer states as **mathematical frames** and study the **sparsest decomposition** of quantum states into these frames.”
- We mainly focus on three measures:  
**stabilizer rank**, the **Gowers norm** and **stabilizer fidelity**.

# Quantum states

- **Qubit:** The state of a two level-system quantum is specified by  $|\psi\rangle \in \mathbb{C}^2$
- $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ ,  $\alpha, \beta \in \mathbb{C}$  are called amplitudes  $|\alpha|^2 + |\beta|^2 = 1$ . Upon measurement

$$Pr(0) = |\alpha|^2, \quad Pr(1) = |\beta|^2.$$



- **General quantum states:**  $|\psi\rangle \in \mathbb{C}^d$  for  $1 \leq d \leq \infty$ ,  $|\psi\rangle = \sum_j \alpha_j |j\rangle$  with  $\sum_j |\alpha_j|^2 = 1$ . Upon measurement, we obtain

$$Pr(j) = |\alpha_j|^2.$$

# Quantum operations

- $U \in \mathbb{C}^{d \times d}$  is a **unitary matrix** if  $U^\dagger = U^{-1}$  where  $U_{jk}^\dagger = U_{kj}^*$ . It is a **generalization of orthogonal matrices** to the complex number field.
- The evolution of a closed system is according to a **unitary matrix** (which preserves the law of probability).

$$U : |\psi\rangle \in \mathbb{C}^d \mapsto U|\psi\rangle$$

- Basic unitary gates:

$$\text{Pauli: } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\text{Clifford: } H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{Non-Clifford: } T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

# Pauli Matrices, Pauli Group, and Clifford Group

**Pauli matrices:**

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

Together with the identity  $I$ , they form the single-qubit Pauli operators.

**$n$ -qubit Pauli group  $\mathcal{P}_n$ :**

$$\mathcal{P}_n = \left\{ i^k P_1 \otimes \cdots \otimes P_n \mid k \in \{0, 1, 2, 3\}, P_j \in \{I, X, Y, Z\} \right\}$$

- Closed under multiplication (up to phases  $\{\pm 1, \pm i\}$ )
- Elements either commute or anticommute

**Clifford group  $\text{Cliff}_n$ :**

$$\text{Cliff}_n = \left\{ U \in U(2^n) \mid U P U^\dagger \in \mathcal{P}_n \quad \forall P \in \mathcal{P}_n \right\}$$

- Normalizer of the Pauli group
- Generated by  $\{H, S, \text{CNOT}\}$
- Maps Pauli operators to Pauli operators under conjugation

# Background: Three definitions for stabilizer states

- 1 **Definition via abelian subgroup of Pauli group:**  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  is a stabilizer state iff there exists an abelian subgroup of  $\mathcal{P}$  with  $2^n$  elements such that for any  $P \in \mathcal{P}_n$ ,  $P|\phi\rangle = |\phi\rangle$ .
- 2 **Definition via quadratic phases:**  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  is a stabilizer state iff there exists an affine subspace  $A \subseteq \mathbb{F}_2^n$ , and quadratic  $Q$  and linear  $\ell$  functions :  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$  such that:

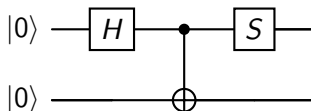
$$|\phi\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} (-1)^{Q(x) + \ell(x)} |x\rangle$$

- 3 **Definition via invariant under Clifford operations:** The set of stabilizer states is the orbit of  $|0^n\rangle$  under  $\text{Cliff} = \langle H, S, CNOT \rangle$ .  
That means each stabilizer state can be produced by a Clifford circuit starting with  $|0^n\rangle$ .

# Example of stabilizer states

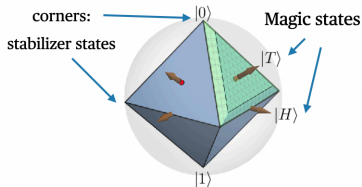
For instance consider the quantum state  $\frac{|00\rangle + i|11\rangle}{\sqrt{2}}$

- 1 It is stabilized by  $Z_1 Z_2$  and  $X_1 Y_2$ .
- 2  $A = \{00, 11\}$ ,  $Q(x) = 1$ ,  $\ell(x) = x_1$
- 3 Here is the Clifford circuit



### The T state

$$|T\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$$

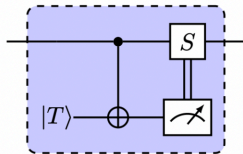


credit: Dawkins Howard, PRL

Example: 1 qubit

### Magic state teleportation:

Clifford circuits on specific “magic” states can simulate universal quantum computations.



=



# Measures of Stabilizer Complexity

- **Stabilizer fidelity**  $F(\psi)$  of a quantum state  $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$  is the maximum overlap between  $|\psi\rangle$  and any stabilizer state.

$$F(\psi) = \max_{|s\rangle \in \text{Stab}_n} |\langle \psi | s \rangle|$$

- **Approximate stabilizer rank**  $\chi_\delta(\phi)$  of a quantum state  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  is the smallest number  $r$  such that there exists  $c_1, \dots, c_r \in \mathbb{C}$  and  $|s_1\rangle, \dots, |s_r\rangle \in \text{Stab}_n$  such that

$$\| |\phi\rangle - (c_1 |s_1\rangle + \dots + c_r |s_r\rangle) \| \leq \delta.$$

- Measure **based on the Gowers norm** which we will define shortly

# Why Stabilizer Rank Matters

## Stabilizer rank:

- Stabilizer rank measures how “far” a state is from the efficiently simulable stabilizer world

## Why is it important?

### ● Classical simulation:

- Stabilizer states  $\Rightarrow$  efficient simulation (Gottesman–Knill)
- If  $|\psi\rangle$  has stabilizer rank  $r$ , then many quantities can be simulated in time  $\text{poly}(n) \cdot r$

### ● Resource theory of magic:

- Stabilizer rank quantifies non-Clifford resources (“magic”)
- Low rank  $\Rightarrow$  weak quantum advantage

### ● Bridging classical and quantum complexity:

- Small stabilizer rank  $\Rightarrow$  efficient classical approximation algorithms
- Large stabilizer rank believed necessary for quantum speedups

## Takeaway:

Stabilizer rank is a **complexity measure** controlling the hardness of simulating quantum systems.

## Main result 1

## Previous bounds on stabilizer rank

	Exact	Approximate	Technique
Bravyi Smith Smolin 2016	$\Omega(\sqrt{n})$	--	
Peleg, Shpilka, Volk, 2022	$\Omega(n)$	$\tilde{\Omega}(\sqrt{n})$	Linear algebra techniques, complexity reductions
Labib, 2022	$\Omega(n)$	--	Higher order Fourier analysis
Lovitz, Steffan 2022	$\tilde{\Omega}(n)$	$\tilde{\Omega}(\sqrt{n})$	Number theory
M, Tahmasbi 2023	$\tilde{\Omega}(n^2)$	$\tilde{\Omega}(n^2)$	Probabilistic method + quantum state synthesis

Major open question  
 $P \neq NP?$



Can we show that NP-complete problems do not have short representation within a specific model? (e.g. circuits with specific structure, ...)



**Specific model:** linear combination of an overcomplete functional basis.  
In particular quadratic phases

**Williams CCC 2018:** For any  $k$  there is a function  $f: \{0,1\}^n \rightarrow \{0,1\}$  in  $NP$  such that that in any decomposition  $f(x) = \sum_{i=1}^r c_i(-1)^{Q_i(x)}$  into quadratic phases  $r \geq n^k$ .

**Open question:**

Can we prove the same thing for functions in  $P$ ?

Can give an example of a function in  $P$  which requires  $r = \omega(n)$  representation?

**M, Tahmasbi 2023:** an example of a function that requires  $\tilde{\Omega}(n^2)$  terms

**Open question:**

Quadratic uncertainty principle

Show that the AND i.e.  $(-1)^{x_1 \cdots x_n}$  function requires exponential representation into quadratic phases

## Second application: Quantum Property Testing

Let  $\rho \in \mathbb{C}^{d \times d}$ .

- **Full-state tomography:** Given  $\rho^{\otimes n}$  output an approximation to  $\rho$ .
- **Sample complexity:** We need  $n = \Omega(d^2/\epsilon^2)$  samples to estimate  $\rho$  within  $\epsilon$  trace distance [Haa+16].
- If  $\rho \in (\mathbb{C}^{2 \times 2})^{\otimes m}$ ,  $d = 2^m$ ; we need exponentially many samples in  $m$ .
- **Quantum property testing:** Testing specific properties of a quantum state using much fewer samples
- E.g., testing if the rank of a density matrix is a given constant requires only a constant number of copies [OW15]
- **Main application 2:** Property testing for stabilizerness

# Tolerant Testing of Stabilizer States

## Problem Statement

Given a quantum state  $|\psi\rangle$  with the promise that its stabilizer fidelity  $F(\psi)$  satisfies:

$$F(\psi) \geq \epsilon_1 \quad \text{or} \quad F(\psi) \leq \epsilon_2,$$

decide which case holds.

- This generalizes exact testing by allowing a **gap** between acceptance and rejection thresholds.
- Known as *tolerant property testing* in theoretical computer science.

# Existing Results for Testing Stabilizer States

## Exact Testing ( $\epsilon_1 = 1$ )

[Mon17]  $\mathcal{O}(n)$  copies suffice to *identify* an  $n$ -qubit stabilizer via **Bell sampling**.

[GNW21] Only **6 copies** needed to test exact stabilizer states (vs. far in fidelity) using **Bell difference sampling** (via a variant of Schur–Weyl duality for Cliff gp).

## Tolerant Testing ( $\epsilon_1 < 1$ )

[Gre+22]  $\mathcal{O}(k^{12})$  copies sufficient to distinguishing between  $\epsilon_1 \geq 1/k$  vs.  $\leq 2^{-\mathcal{O}(n)}$  (e.g. Haar-random ensemble).

[Gre+24b] showed that finding a stabilizer state with good overlap with a given state using polynomial samples and exponential post-proc. (improved to poly-time in [Che+24])

[Gre+24a] For  $\epsilon_2 \leq \frac{4\epsilon_1^6 - 1}{3}$  and  $\mathcal{O}(\text{poly}(1/\epsilon_1))$  samples (limits  $\epsilon_1 \geq \sqrt[3]{1/2}$ ).

[AD24] Improved to work with  $\epsilon_2 \leq 2^{-\text{poly}(1/\epsilon_1)}$ , for phase states assuming  $\epsilon_2 = \epsilon^{\mathcal{O}(1)}$  (Complexity:  $\text{poly}(n/\epsilon_1)$ )

## Main result 2: Tolerant Testing

### Theorem (Improved bounds on tolerant testing)

Let  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  with the promise that either  $F(\phi) \geq \epsilon_1$  or  $\leq \epsilon_2$ . Using  $\text{poly}(1/\epsilon_1)$  copies of a quantum state  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  and a circuit of size  $n \cdot \text{poly}(1/\epsilon_1)$  we can distinguish between the two cases with probability of error  $\leq 1/3$  provided that  $\epsilon_2 \leq \epsilon_1^C$  for a sufficiently large absolute constant  $C > 0$ .

## Tool: Gowers-3 norm

- For a function  $f : \mathbb{F}_2^n \rightarrow \mathbb{C}$  define Gowers 3-norm:

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

Theorem (see [HHL19])

- If  $P$  is a polynomial of degree 2 then  $\|(-1)^P\|_{U^3} = 1$ .
- For any polynomial  $P : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  of degree 2 it holds that  $\|f\|_{U^3} \leq |\langle (-1)^P, f \rangle|$ .
- For any polynomial  $P : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  of degree 2, if  $\|f\|_{U^3} \geq \epsilon$ , then  $|\langle (-1)^P, f \rangle| \geq \delta(\epsilon, P)$ .

For  $f, g : \mathbb{F}_2^n \rightarrow \mathbb{C}$ ,  $\langle f, g \rangle := \mathbb{E}(f(x)\overline{g(x)})$ .

# Main Theorem: Gowers Norm & Fidelity

## Definition (quantum Gowers norm)

For a quantum state  $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x g(x) |x\rangle$ , let  $\|\phi\|_{U^3} := \|g\|_{U^3}$ .

## Theorem

If  $\|\phi\|_{U^3}^8 \geq \gamma$ , then  $\exists$  stabilizer  $|s\rangle$  such that  $|\langle\phi|s\rangle| \geq \gamma^{C_2}/C_1$  for some absolute constants  $C_1, C_2$ .

## Theorem

[AD '24] There is a quantum algorithm that uses  $O(1/\delta)$  copies of a quantum state  $|\psi\rangle$  and outputs a  $\delta$  additive estimation to a number  $R$  such that

$$\|\psi\rangle\|_{U^3}^{16} \leq R \leq \|\psi\rangle\|_{U^3}^8.$$

# Zauner's Conjecture and Stabilizer Complexity

**SIC-POVMs and fiducial states.** A set of unit vectors  $\{|\psi_i\rangle\}_{i=1}^{d^2} \subset \mathbb{C}^d$  forms a *symmetric informationally complete POVM* (SIC-POVM) if

$$|\langle \psi_i, \psi_j \rangle|^2 = \frac{1}{d+1} \quad \text{for all } i \neq j.$$

A *fiducial state* is a single state  $|\phi\rangle$  whose orbit under the Weyl–Heisenberg group generates such a SIC.

**Zauner's conjecture.** For every dimension  $d$ , there exists a Weyl–Heisenberg SIC-POVM, equivalently a fiducial state whose orbit gives a SIC.

**Why are fiducial states interesting here?**

- They are in a sense maximally spread out under the Pauli/Weyl action.
- Their overlaps with the Weyl orbit are extremely uniform.
- Overlap between stabilizer states, on the other hand, are far from uniform
- This suggests they may be very far from the highly algebraic stabilizer world.

**Question.**

What is the stabilizer complexity of SIC fiducial states?

**Speculation.**

Fiducial states are likely *extremally far* from the stabilizer set, perhaps having very small stabilizer fidelity and very large stabilizer rank.

# Open questions

We end with some open questions

- Tolerant testing of stabilizer rank?
- Tight bounds relating Gowers norms and stabilizer fidelity?
- Extremal examples (e.g., SIC fiducial states)?

**Thank you for your attention!**

# Generalized Pauli operators

- Generalized Pauli operators:

$$X^a = X^{a_1} \otimes \dots \otimes X^{a_n}, Z^b = Z^{b_1} \otimes \dots \otimes Z^{b_n}$$

with  $a, b \in \mathbb{F}_2^n$ . They satisfy

$$X^a |x\rangle = |x + a\rangle, \quad Z^b |x\rangle = (-1)^{\langle x, b \rangle} |x\rangle,$$

where  $\langle x, b \rangle = \sum_i x_i b_i$  (additions mod 2).

- Weyl operator:**  $W(z) := i^{\langle y, \alpha \rangle} X^y Z^\alpha$ ,  $z = (y, \alpha) \in \mathbb{F}_2^{2n}$ .
- Symplectic inner product:** Let  $z_1 = (y_1, \alpha_1), z_2 = (y_2, \alpha_2) \in \mathbb{F}_2^{2n}$ ,

$$[z_1, z_2] := \langle y_1, \alpha_2 \rangle + \langle y_2, \alpha_1 \rangle.$$

- Commutation relationships:**

$$W(z_1)W(z_2) = (-1)^{[z_1, z_2]} W(z_2)W(z_1)$$

- $T \subset \mathbb{F}_2^{2n}$  **Lagrangian subspace** if  $|T| = 2^n$  and for any  $z_1, z_2 \in T$ ,  $[z_1, z_2] = 0$  (they commute).  $T$  corresponds to a stabilizer group.

# Characteristic function

## Definition (Characteristic function)

For  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  define the characteristic function  $f_\phi : \mathbb{F}_2^{2n} \rightarrow \mathbb{R}$  with  $f_\phi(z) = |\langle \phi | W(z) | \phi \rangle|^2$ .

### Properties:

- **Normalization:**

$$\frac{1}{N} \sum_{z \in \mathbb{F}_2^{2n}} f(z) = 1$$

furthermore  $f(0) = 1$ .

## Lemma (Fidelity and characteristic function; [GNW21]; [Gre+24b])

Let  $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$  and a Lagrangian subspace  $T \subset \mathbb{F}_2^{2n}$  then  $F(\phi) \geq \sum_{z \in T} f_\phi(z)$ .

## Lemma

If  $V \subseteq \mathbb{F}_2^{2n}$  is a subspace, then for any  $z_0 \in \mathbb{F}_2^{2n}$ ,  $\sum_{z \in V} f(z) \geq \sum_{z \in V} f(z + z_0)$ .

A corollary of these lemmas is that if we can find  $V \subset \mathbb{F}_2^{2n}$  such that  $\sum_{z \in V} f(z) \geq \epsilon$ , and furthermore  $V$  can be covered by  $K$  affine subspaces then  $F(\phi) \geq \epsilon/K$ .


# Proof outline for phase states

We first outline how [AD24] achieve this bound for [phase states](#)<sup>1</sup>. Proof follows closely that of the classical inverse Gowers theorem<sup>2</sup>. It consists of two major steps.

- 1 Probabilistic construction of an almost linear function,
- 2 Use this map to find an almost linear subspace with high weight
- 3 Use additive combinatorics to cover this subspace with a few affine subspaces
- 4 Find a Lagrangian subspace with high weight  $\implies$  lower bound on fidelity

---

<sup>1</sup>Taking the form  $|\phi\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle$

<sup>2</sup>Weaker quasipolynomial bound were mentioned in [MT24]. 

# Probabilistic Construction of an almost linear function

**Construction:** Probabilistically construct  $\zeta : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  via:

- Choose  $\zeta(y) = \alpha$  with probability  $f(y, \alpha)$ .

**Properties:**

Assuming  $\|\phi\|_{U^3} \geq \gamma$ , this function has the following properties:

- $f(y, \zeta(y)) = \text{poly}(\gamma)$  for poly( $\gamma$ ) fraction of  $y$ .
- $\zeta(x + y) = \zeta(x) + \zeta(y)$  for poly( $\gamma$ ) fraction of  $x, y$ .

**Limitation:**  $\zeta$  is a valid probability distribution only for phase states. For instance if  $|\phi\rangle = |0\rangle$ , then  $f_\phi(y, \alpha) = 0$  for all  $y \neq 0$ .

# Tools from additive combinatorics (overview)

- Using the almost-linear  $\zeta$  we find an almost linear subspace with high weight.
- Using Balog-Szemerédi-Gowers [BS94] we find a subset  $S$  with small doubling:  $|S + S| \leq K|S|$ .
- Apply resolution to Marton's conjecture ([Gow+23]) to cover  $S$  using a few translates of a linear subspace.
- Cover this subspace with a few Lagrangians.

## Conclusion:

- Find linear map  $\ell$  such that  $\mathbb{E}_y |\langle \phi | X^y Z^{\ell(y)} | \phi \rangle|^2 = \text{poly}(\gamma)$ .
- From this, recover a stabilizer “phase” state with overlap  $\text{poly}(\gamma)$ .

# Tools from additive combinatorics (details)

## Theorem (Balog and Szemerédi [BS94])

Let  $(G, +)$  be an Abelian group and  $S \subset G$  with  $\Pr_{z_1, z_2 \in S}[z_1 + z_2 \in S] \geq \epsilon$ . There exists,  $S' \subset S$  with  $|S'| \geq \frac{\epsilon|S|}{3}$  and  $|S' + S'| \leq (\frac{6}{\epsilon})^8 |S|$ .

## Theorem ([Gow+23])

Let  $S \subset \mathbb{F}_2^n$  be a subset with  $|S + S| \leq K|S|$ . Then,  $S$  can be covered with  $(2K)^8$  translations of a subspace  $V \subset \mathbb{F}_2^n$  with  $|V| \leq |S|$

Combining the above theorems yields the following corollary, which is the main tool we need from additive combinatorics.

## Corollary

Let  $S \subset \mathbb{F}_2^n$  with  $\Pr_{z_1, z_2 \in S}[z_1 + z_2 \in S] \geq \epsilon$ . There exists an affine subspace  $V \subset \mathbb{F}_2^n$  with  $|S \cap V| \geq \frac{\epsilon^{K_2}}{K_1} |S|$  and  $|V| \leq |S|$  where  $K_1, K_2 \geq 0$  are absolute constants. One can choose  $K_2 = 73$  and  $K_1 = 3 \times 6^{72}$ .

# Non-Phase States: Limitations of Phase-State Proof

## Limitations of the previous approach for non-phase states:

- The stabilizer state produced from the previous approach is a phase state. However if we consider a non-phase state such as the computational basis, overlap with any phase state can be as small as  $1/\sqrt{N}$ .
- For phase states, for any  $y$ ,  $f(y, \alpha)$  is a probability distribution:  $\sum_{\alpha} f(y, \alpha) = 1$ .
- For general states  $\sum_{\alpha} f(y, \alpha)$  can be concentrated on few  $y$ .

## Ideas used by [AD24]:

- Sample  $(y, \alpha)$  using  $f(y, \alpha)$ , then linearize using additive combinatorics.
- Leads to non-commuting elements: need  $\exp(\text{poly}(\gamma^{-1}))$  many stabilizer subspaces.
- Implies a stabilizer state with weak overlap  $\geq \exp(-\text{poly}(\gamma^{-1}))$ .
- Relied on a conjecture

# Our Approach: Random Clifford Trick

**Idea:** Apply random Clifford  $C$  to  $|\phi\rangle$ .

- We use two properties of random Clifford:
  - 1 Stabilizer measures invariant under Clifford operations.
  - 2 Clifford group is a 3-design.
- This balances the quantum state: We show that for any quantum state  $|\phi\rangle$  there exist some Clifford  $C$  such that  $f_{C|\phi}(y, \alpha): \sum_{\alpha} f_{C|\phi}(y, \alpha) = O(1)$  for all  $y$ .
- We modify the phase-state proof to work in this case.

**Impact:**

- Better bounds, no conjectures.

**Remark:** Around the same time we put our work online (literally the day before), two groups [ABD24; BDH24] achieved similar exponential to polynomial bound. They use original techniques plus graph/algebraic tools to handle non-commuting elements.

# Bell Sampling and Gowers Norm Estimation

Given two copies of a state  $|\phi\rangle$ , *Bell sampling* is the process of measuring in the Bell basis:

$$\{|W_z\rangle := (W_z \otimes \mathbb{I})|\Phi^+\rangle : z \in \mathbb{F}^{2n}\}$$

where  $|\Phi^+\rangle := \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{F}^n} |x\rangle |x\rangle$  is the maximally entangled state.

Given four copies  $|\phi\rangle^{\otimes 4}$ , *Bell difference sampling* performs Bell sampling on the first two and last two copies to obtain  $z_1, z_2 \in \mathbb{F}^{2n}$ , then outputs  $z = z_1 + z_2$ .

From [GNW21, Eq (3.1)], the probability that Bell measurements on two copies give the same output is:

$$\frac{1}{2}(1 + \lambda), \quad \text{where } \lambda := \sum_{z \in \mathbb{F}^{2n}} q(z)f(z)$$

where  $f$  is the characteristic function of  $|\phi\rangle$ ,  $q = f * f$ , where  $(f * g)(x) = \mathbb{E}_{y \in \mathbb{F}_2^n} [f(y)g(x + y)]$ .

**Lemma ([AD24], Lemma 3.8)**

*We can estimate  $\lambda$  up to error  $\pm\delta$  using  $O(1/\delta^2)$  copies and a circuit of size  $O(n/\delta^2)$ .*

This quantity is related to the Gowers 3-norm as [AD24, Eq. (4)]:

$$\| |\phi\rangle \|_{U^3}^{16} \leq \sum_{z \in \mathbb{F}^{2n}} q(z)f(z) \leq \| |\phi\rangle \|_{U^3}^8$$

## References I

- [ABD24] Srinivasan Arunachalam, Sergey Bravyi, and Arkopal Dutt. “A note on polynomial-time tolerant testing stabilizer states”. In: *arXiv preprint arXiv:2410.22220* (2024).
- [AD24] Srinivasan Arunachalam and Arkopal Dutt. “Tolerant testing stabilizer states”. In: *arXiv preprint arXiv:2408.06289* (2024).
- [BDH24] Zongbo Bao, Philippe van Dordrecht, and Jonas Helsen. “Tolerant testing of stabilizer states with a polynomial gap via a generalized uncertainty relation”. In: *arXiv preprint arXiv:2410.21811* (2024).
- [BS94] Antal Balog and Endre Szemerédi. “A statistical theorem of set addition”. In: *Combinatorica* 14 (1994), pp. 263–268. DOI: 10.1007/BF01212974. URL: <https://api.semanticscholar.org/CorpusID:30273837>.
- [Che+24] Sitan Chen, Weiyuan Gong, Qi Ye, and Zhihan Zhang. *Stabilizer bootstrapping: A recipe for efficient agnostic tomography and magic estimation*. 2024. arXiv: 2408.06967 [quant-ph]. URL: <https://arxiv.org/abs/2408.06967>.
- [GNW21] David Gross, Sepehr Nezami, and Michael Walter. “Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations”. In: *Communications in Mathematical Physics* 385.3 (2021), pp. 1325–1393. DOI: 10.1007/s00220-021-04118-7.
- [Gow+23] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. *On a conjecture of Marton*. 2023. arXiv: 2311.05762 [math.NT]. URL: <https://arxiv.org/abs/2311.05762>.
- [Gre+22] Sabeel Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. “Low-stabilizer-complexity quantum states are not pseudorandom”. In: *arXiv preprint arXiv:2209.14530* (2022).
- [Gre+24a] Sabeel Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. *Efficient Learning of Quantum States Prepared With Few Non-Clifford Gates*. 2024. arXiv: 2305.13409 [quant-ph]. URL: <https://arxiv.org/abs/2305.13409>.

## References II

- [Gre+24b] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Improved Stabilizer Estimation via Bell Difference Sampling". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. STOC 2024. Vancouver, BC, Canada: Association for Computing Machinery, 2024, pp. 1352–1363. ISBN: 9798400703836. DOI: 10.1145/3618260.3649738. URL: <https://doi.org/10.1145/3618260.3649738>.
- [Haa+16] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. "Sample-optimal tomography of quantum states". In: *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 2016, pp. 913–925. DOI: 10.1145/2897518.2897585.
- [HHL19] Hamed Hatami, Pooya Hatami, and Shachar Lovett. "Higher-order fourier analysis and applications". In: *Foundations and Trends in Theoretical Computer Science* 13.4 (2019), pp. 247–448. DOI: 10.1561/04000000064.
- [Mon17] Ashley Montanaro. "Learning stabilizer states by Bell sampling". In: *arXiv preprint arXiv:1707.04012* (2017).
- [MT24] Saeed Mehraban and Mehrdad Tahmasbi. "Quadratic Lower bounds on the Approximate Stabilizer Rank: A Probabilistic Approach". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. 2024, pp. 608–619. DOI: 10.1145/3618260.3649733.
- [OW15] Ryan O'Donnell and John Wright. "Quantum spectrum testing". In: *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*. 2015, pp. 529–538. DOI: 10.1145/2746539.2746582.