

Testing & learning stabilizer-like states

Srinivasan Arunachalam (IBM Research)

Based on joint works with Arkopal Dutt (IBM Research)



Quantum computing

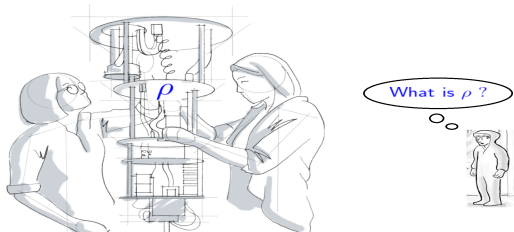
A computer that harnesses the power of quantum physics

What can a quantum computer do?

Factoring, Searching, Simulation and several other algorithms

BUT... building a **fault-tolerant** quantum computer is a hard **engineering** problem

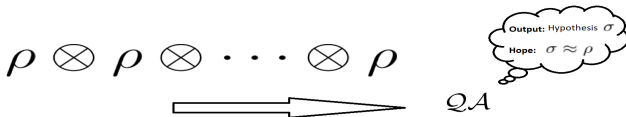
More recently, **small-scale low-error** quantum devices



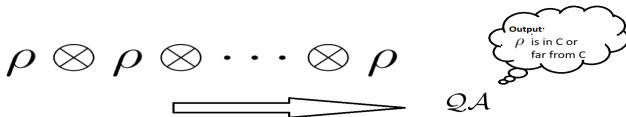
Can we **certify and calibrate the output** of quantum devices?

Learning and testing a state

Learning. How many **copies** of an n -qubit state ρ are necessary and sufficient to **produce classical description** of a state σ that **approximates** ρ well enough?



Testing. Let C be a **fixed known class** of states. How many **copies of** ρ are necessary and sufficient to test **if** $\rho \in C$ or is promised to be far.



Motivation. Fundamental question, experimental verification, understanding noise.

Without prior information. **Provably hard**, require $\text{poly}(D)$ copies.

What if unknown ρ belonged to a **structured class** of states?

Can testing/learning be done efficiently for structured states?

Motivation for the talk

When is quantum computing simulable?

*Gottesman-Knill theorem: a circuit with Clifford gates is **simulable efficiently** on a classical device. For the full power of quantum, need **T** gates.*

Is everything known about testing/learning the outputs of these circuits?



Overview of talk

When is quantum computing simulable?

*Gottesman-Knill theorem: a circuit with Clifford gates is **simulable efficiently** on a classical device. For the full power of quantum, need **T gates**.*

Is everything known about testing/learning the outputs of these circuits?

- 1 **Learn** output of Clifford circuits (i.e., **stabilizer states**)? **Yes** [AG'03, Mon'17]
- 2 What about Clifford+ **few T gates**, still learnable? **Yes** [GIKL, LOH, HG'24]
- 3 Are “**sum of stabilizers**” learnable? **Kind of** [AD'26]
- 4 Given an arbitrary $|\psi\rangle$, is it **close to** a stabilizer state? **Kind of** [AD'24]
- 5 If close, can we **find a nearby** stabilizer? **Kind of** [AD'25, CGYZ'24]
- 6 Can we test and learn **real** stabilizer states? **YES** [ABDY'23, AAGW'26]

Cliffords and stabilizers

We will be considering **very** simple classes of quantum states (yet not well understood):

Cliffords. A Clifford unitary is generated by Paulis $\{\mathbb{I}, X, Y, Z\}$ and

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

Stabilizer states. Consider a **Clifford unitary** C then output of

$$|\psi\rangle = C|0^n\rangle$$

is a **stabilizer state**!

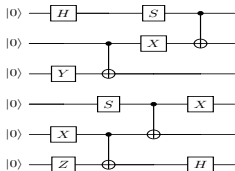
Why care? Known to be classical simulable and easily implementable. Have found **applications** in error correcting codes, complexity theory, cryptography, etc.

For quantum computation. If we allow Cliffords + **T gates** get universality

[Bravyi et al.'19] If a unitary U consists of Cliffords + $O(\log n)$ T gates, then U is **simulable efficiently**. Is $U|0^n\rangle$ also **learnable**?

Given copies of $|\psi\rangle = U|0^n\rangle$, what is the complexity of testing/learning ?

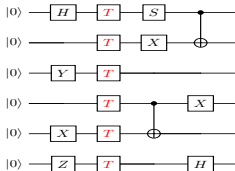
A short history on learning Clifford+T circuits



Learning output of Clifford circuits:

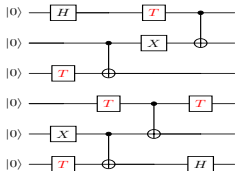
Aaronson, Gottesmann'03: $O(n)$ copies
(entangled measurement on all copies)

Montanaro'17: $O(n)$ copies
(Bell sampling on just 2 copies)



Clifford + **single-layer** of t many T gates:

Lai, Cheng'20: a $\text{poly}(n, 2^t)$ copy algorithm
decomposed T gate as **sum of 2 stabilizers**



Clifford + t many T gates

Grewal, Iyer, Liang, Kretschmer'23 '24 '24
Leone, Oliviero, Hama'24
Hangleiter, Gullans'24:

a $\text{poly}(n, 2^t)$ copy algorithm
these states have “**low stabilizer dimension**”

What's next?

So far. If the circuit C is Clifford + T gates, then C is **simulable in time $\text{poly}(n, 2^t)$** and $|\psi\rangle = C|0^n\rangle$ is **learnable in time $\text{poly}(n, 2^t)$**

Is everything that is simulable also learnable?

Crucial in these algorithms, if U is **Clifford + t many T gates**, then $|\psi\rangle = U|0^n\rangle$ is

$$|\psi\rangle = \sum_{i=1}^{2^t} c_i |\phi_i\rangle \text{ where } |\phi_i\rangle \text{ is stabilizers, } \{c_i\}_i \text{ is } \underline{\text{"low dimensional"}}$$

which motivates their learners. **But not all** stabilizer rank- k states

$$V|0^n\rangle = \sum_{i=1}^k c_i |\phi_i\rangle \text{ for stabilizers } |\phi_i\rangle$$

produced by Clifford + $\log k$ many T gates. Many circuits V s are **simulable** in $\text{poly}(n, k)$

Are stabilizer-rank k states learnable in time $\text{poly}(n, k)$?

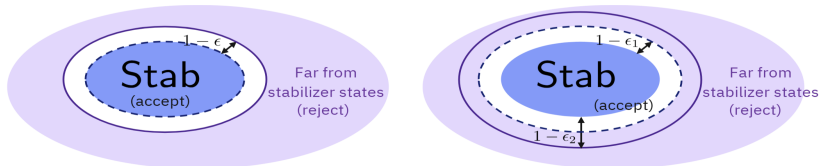
Even **rank-2** states not known to be learnable. In [AD'25], give an **unconditional $\text{poly}(n, 2^{k^2})$** algorithm, **conditional $\text{poly}(n, 2^k)$** algorithm.

Open question: Getting a $\text{poly}(n, k)$ is still open.

Even if resolved, can we **test** stabilizer structure with **far fewer** samples than learning?

A short history on testing stabilizers

Recall. Given copies of $|\psi\rangle$ decide if $|\psi\rangle$ is close or far from class of stabilizer states.



Formally Let Stab be the class of stabilizer states. Given copies of $|\psi\rangle$, decide if:

- 1 $|\langle\psi|\phi\rangle|^2 \geq \epsilon_1$ for **some** $|\phi\rangle \in \text{Stab}$
- 2 $|\langle\psi|\phi\rangle|^2 \leq \epsilon_2$ for **all** $|\phi\rangle \in \text{Stab}$

for $\epsilon_2 \leq \epsilon_1$, promised one of them is the case

How many copies suffices to test this?

- 1 $\epsilon_1 = 1, \epsilon_2 \leq 0.9$: Gross, Nezami, Walter'17 gave a 6-copy tester
- 2 $\epsilon_1 \geq 0.8, \epsilon_2 \leq 0.6$: Grewal, Iyer, Liang, Kretschmer'24 gave a 6-copy tester
- 3 $\epsilon_1 \geq 0, \epsilon_2 \leq \epsilon_1 - \delta$: Chen, Gong, Ye, Zhang'24 uses $\text{poly}(1/\delta, (1/\epsilon_1)^{\log 1/\epsilon_1})$ copies
- 4 $\epsilon_1 \geq 0, \epsilon_2 \leq \epsilon_1^C$: [AD'24] uses $\text{poly}(1/\epsilon_1)$ copies

Stabilizer states are testable robustly using constant many copies

Bell sampling, viewed as taking derivatives

What is really in the heart of these testing/learning algorithms?

Bell sampling. Here, view it as a way of taking “derivatives”

Every stabilizer state written as $|\psi\rangle = \sum_{x \in A} (-1)^{x^t B x} \cdot i^{S \cdot x} |x\rangle$ for a subspace $A \subseteq \mathbb{F}_2^n$

For simplicity let $A = \{0, 1\}^n$, $S = 0^n$. **Goal is to learn** $B \in \mathbb{F}_2^{n \times n}$.

A learning algorithm take **two copies** of $|\psi\rangle$

$$\begin{aligned}
|\psi\rangle \otimes |\psi\rangle &= \sum_{x,y} (-1)^{x^t B x + y^t B y} |x, y\rangle \\
&\xrightarrow{\text{CNOT}} \sum_{x,y} (-1)^{x^t B x + y^t B y} |x, x + y\rangle \\
&\stackrel{\text{rewrite}}{=} \sum_{x,z} (-1)^{x^t B x + (x+z)^t B (x+z)} |x, z\rangle \stackrel{\text{simplify}}{=} \sum_{x,z} (-1)^{x^t (B+B^t)z + z^t B z} |x, z\rangle
\end{aligned}$$

Measure the second register and suppose we **obtain** $\tilde{z}$, resulting state is

$$(-1)^{\tilde{z}^t B \tilde{z}} \left(\sum_x (-1)^{x^t (B+B^t) \tilde{z}} |x\rangle \right) |\tilde{z}\rangle \xrightarrow{\text{Had}} |(B+B^t) \cdot \tilde{z}\rangle |\tilde{z}\rangle$$

2 copies of $|\psi\rangle$ allow to take **one derivative** of $x^t B x$ (in the **direction of** $\tilde{z}$).

2n copies to take **n derivatives** and **learn** B , hence $|\psi\rangle$ completely

Almost all learners/testers use Bell sampling before a structural analysis.

New conceptual contribution for *tolerant testing*

Gowers norm: A way to obtain generalized derivatives

- 1 Well-known in the classical functional analysis community:

For a **Boolean function** $f : \{0, 1\}^n \rightarrow \{-1, 1\}$, define the k -th Gowers norm as

$$\|f\|_{U^{k+1}}^{2^{k+1}} = \mathbb{E}_{x, h_1, \dots, h_k \in \{0, 1\}^n} \left[\prod_{S \subseteq [k]} f\left(x + \sum_{i \in S} h_i\right) \right].$$

- 2 Essentially **average derivatives**: let $k = 1$, then

$$\|f\|_{U^2}^4 = \mathbb{E}_{x, h} [f(x) f(x + h)]$$

and for $k = 2$, we have

$$\|f\|_{U^3}^8 = \mathbb{E}_{x, h_1, h_2} [f(x) \cdot f(x + h_1) \cdot f(x + h_2) \cdot f(x + h_1 + h_2)]$$

- 3 Define Gowers norm for **quantum states**: If $|\psi\rangle = \sum_x f(x) |x\rangle$ where $f = (f(x))_x \in \mathbb{C}^d$ is an ℓ_2 -normed vector, define its Gowers norm similarly
- 4 Fairly new to the quantum community; **hinted** by a work of Tao, Eisner'07
- 5 **Straightforward generalization**. What's the use?

Tolerant testing stabilizer states

- 1 Given copies of n -qubit $|\psi\rangle$, s.t. $|\psi\rangle$ is ε_1 -close to stabilizer or ε_2 -far from all

$$\text{Decide if : } \max_{|\phi\rangle \in \text{Stab}} |\langle\psi|\phi\rangle|^2 \geq \varepsilon_1 \text{ versus } \max_{|\phi\rangle \in \text{Stab}} |\langle\psi|\phi\rangle|^2 \leq \varepsilon_2$$

- 2 Previously [GNW'21, GIKL'24] considered $\varepsilon_1 \geq 0.8$. What about arbitrary $\varepsilon_1, \varepsilon_2$?

Why care? A natural question, “real-world” scenario, quantifying magic in states

[AD'24] there is a $\text{poly}(1/\varepsilon_1)$ sample and $O(n \cdot \text{poly}(1/\varepsilon_1))$ -time tester

- 1 Classically, seminal result: $\text{GOWERS}(f, 3) \geq \varepsilon$, then f is close to degree-2.

Samorodnitsky'07+GGMT'24 : $\|f\|_{U^3} \geq \varepsilon \implies \Pr_x[f(x) = (-1)^{g(x)}] \geq \text{poly}(\varepsilon)$,

where $g : \{0, 1\}^n \rightarrow \{0, 1\}$ is a quadratic function.

- 2 *Inverse Gowers theorem*: Gowers norm is related to stabilizer fidelity

If $\text{GOWERS}(|\psi\rangle, 3) \geq \varepsilon$, then there is a stabilizer $|\phi\rangle$ such that $|\langle\psi|\phi\rangle|^2 \geq \varepsilon^C$.

- 3 Furthermore $\text{GOWERS}(|\psi\rangle, 3)$ can be estimated with copies of $|\psi\rangle$
- 4 Proof of this is a non-trivial extension of the classical proof using techniques of additive combinatorics and stabilizer coverings (see also [BDH'24, MT'24]).

Learning the closest stabilizer state

So far. If $\text{GOWERS}(|\psi\rangle, 3) \geq \epsilon$, then there is a stabilizer $|\phi\rangle$ such that $|\langle\psi|\phi\rangle|^2 \geq \epsilon^C$.

Open question in [AD'24]: Can we find a close-enough stabilizer?

Agnostic learning. In [CGYZ'24], if $|\psi\rangle$ is τ -close to some stabilizer, one can find a stabilizer $|s'\rangle$ s.t.

$$|\langle\psi|s'\rangle|^2 \geq \tau - \epsilon,$$

in time $\text{poly}(n, 1/\epsilon, (1/\tau)^{\log 1/\tau})$.

Self-correction. In [AD'25] we initiate the task of self-correction: if $|\psi\rangle$ is τ -close to some stabilizer, one can find a stabilizer $|s'\rangle$ s.t.

$$|\langle\psi|s'\rangle|^2 \geq \tau^C.$$

Simpler than agnostic learning.

We algorithmize every step in [AD'24] and give a $\text{poly}(n, 1/\tau)$ algorithm for this task (assuming an algorithmic conjecture in mathematics).

What classes of states are efficiently self-correctable?

As a classical bonus. In [BDAGS'25] we **dequantize** the learning algorithms above and obtain **classical algorithms** for the polynomial Freiman-Ruzsa theorem (whose combinatorial version was a recent breakthrough by GMT'23)

Iterate to find more structure

So far. Let $|\psi\rangle$ be an arbitrary state.

- (1). If $\text{GOWERS}(|\psi\rangle, 3) \geq \varepsilon$, then there **exists a stabilizer** $|\phi\rangle$ such that $|\langle\psi|\phi\rangle|^2 \geq \varepsilon^C$.
- (2). Using [CGYZ'24, AD'25] to find “some structure”, i.e., stabilizer satisfying above.

For arbitrary $|\psi\rangle$, can we boost further to find more structure?

YES: Inspired by classical **boosting**, consider the following

- ➊ Check if $\text{GOWERS}(|\psi\rangle, 3) \geq \gamma$. If so, **find a stabilizer** $|\phi_1\rangle$ using (2).
- ➋ Given access to U_ψ , use **LCU to prepare** $|\psi_1\rangle = |\psi\rangle - |\phi_1\rangle$.
- ➌ Check if $\text{GOWERS}(|\psi_1\rangle, 3) \geq \gamma$. If so, **find a stabilizer** $|\phi_2\rangle$.
- ➍ **Boost further** to find stabilizers $|\phi_1\rangle, \dots, |\phi_t\rangle$ such that

$$|\psi\rangle \propto \underbrace{\sum_i c_i |\phi_i\rangle}_{:=\text{structured}} + \underbrace{|\phi^\perp\rangle}_{:=\text{unstructured}}$$

- ➎ In particular, unstructured $|\phi^\perp\rangle$ has **small stabilizer fidelity**.
- ➏ **Non-trivial aspects:** (i) no. of iterations, (ii) errors in subroutines, (iii) removing access to U_ψ . Made rigorous in [AD'26]
- ➐ **Why care?** Learning states with **low stabilizer extent**:
(unconditional) **quasipolynomial** time & (conditional) **polynomial** time.

Learning phase states: a natural extension

$$\text{Let } |\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \underbrace{(-1)^{f(x)}}_{\text{binary}} |x\rangle, \quad |\phi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_q^n} \underbrace{\omega_q^{f(x)}}_{\text{generalized}} |x\rangle$$

where **degree of (unknown) f is d** . How many copies of $|\psi_f\rangle$ or $|\phi_f\rangle$ suffice to learn f ?

Why care? Stabilizer states, Pseudorandomness, IQP circuits, Quantum complexity

In [ABDY'22], we considered the learning question and showed **optimal bounds**.

	Separable	Entangled
degree- d Binary phase state	$\Theta(n^d)$	$\Theta(n^{d-1})$
degree- d Generalized phase states	$\Theta(n^d)$	$\Theta(n^{d-1})$

Natural approach. Taking **derivatives**? suppose f is degree-3

$$|\psi_f\rangle^{\otimes 2} \mapsto (s, \sum_x (-1)^{f(x)+f(x+s)} |x\rangle).$$

Recall that when f was degree-2, then $f(x) + f(x+s)$ was **degree-1**, so we can learn it by applying Hadamards, but now $f(x) + f(x+s)$ is **degree-2**, **unclear** how to learn!

Entangled protocol. Use the **Pretty good measurement**! Relate success probability to weight distribution of Reed-Muller codes and using known bounds, get n^{d-1} copies

Testing phase states

Is learning required? In complexity theory, suffices to **test low-degreesness**.

If we can test **generalized** phase states in time $\text{poly}(n, q, d)$, we'd get $\text{QMA}(2) = \text{NEXP}$.

But, in [AGW'26] we show that's not the case.

For $d = 2$, give an $\Omega(n)$ lower bound. For $d \geq 3$, give a $\Omega(n^{(d-1)/2})$ lower bound.

Proof sketch. Observe that degree- d polynomials are codewords of Reed-Muller codes

- 1 Consider a problem of **testing codeword states**: for a code $\mathcal{C} \subseteq \mathbb{F}_q^n$, given copies of $|\phi\rangle$, is it of the form $|\psi_c\rangle = \sum_{i \in [n]} \omega_q^{c_i} |i\rangle$ or 0.1-far from all such states.
- 2 To that end, for the code $\mathcal{C}$, we need to bound

$$\|\mathbb{E}_{c \in \mathcal{C}}[(|\psi_c\rangle\langle\psi_c|)^{\otimes t}] - \mathbb{E}_{c \in \mathbb{F}_q^n}[(|\psi_c\rangle\langle\psi_c|)^{\otimes t}]\|_{tr} \quad (\star)$$

- 3 Main idea: reduce $(\star)$ it to **average-case** noisy-codeword ($\text{ANC}(\mathcal{C})$) recovery:
Let e_t be a random string of weight t ,
Given He_t recover e_t (where H is the parity-check matrix of $\mathcal{C}$)
- 4 For every $\mathcal{C}$, we show $(\star) \leq 1 - \text{ANC}(\mathcal{C}^\perp)$, where $\mathcal{C}^\perp$ is the **dual** of the code $\mathcal{C}$.
- 5 Using (and generalizing) **weight-enumeration bounds** of Reed-Muller codes, we show that **if $t \ll n^{(d-1)/2}$** , then $\text{ANC}(\mathcal{C}^\perp) \geq 1 - o(1)$, **hence $(\star) \leq o(1)$** .
- 6 Assuming a **conjecture in information theory**, can be **improved to $\Omega(n^{d-1})$** , implying that testing and learning are **equally hard**.

Summary and Conclusion

Interplay between classical and quantum learning has yielded several fruitful results

Rich area with several open question even for simple classes of states

- 1 Test if $|\psi\rangle$ is $\geq \tau$ -close or $\leq \tau - \varepsilon$ far from stabilizer in $\text{poly}(n, 1/\tau, 1/\varepsilon)$?
- 2 Learning stabilizer rank k states in $\text{poly}(n, k)$?
- 3 Single copy lower bounds for testing stabilizer states?
- 4 Extending results to mixed states? See some progress by [IL'24]
- 5 Going beyond stabilizers: MPS, trivial states, higher levels of Clifford hierarchy
- 6 Testing Clifford circuits? See progress by [HBDEBH'25]. Sum of Cliffords?
- 7 Generalizing to the continuous variable setting?
- 8 Something more in between quantum learning and additive combinatorics?

THANK YOU