Quadratic Lower Bounds on the Approximate Stabilizer Rank

(a Probabilistic Approach)

56th Annual ACM Symposium
on Theory of Computing (STOC 2024)
June 24-28, 2024, Vancouver, Canada

SAEED MEHRABAN
TUFTS CS

MEHRDAD TAHMASBI
UIUC CS

arXiv: 2305.10277

Main question:

How hard is it to simulate quantum computations on classical computers?

Can we rigorously separate P and BQP? → Would imply $P \neq PSPACE$

Can we rigorously show specific simulation techniques will take exponential time?

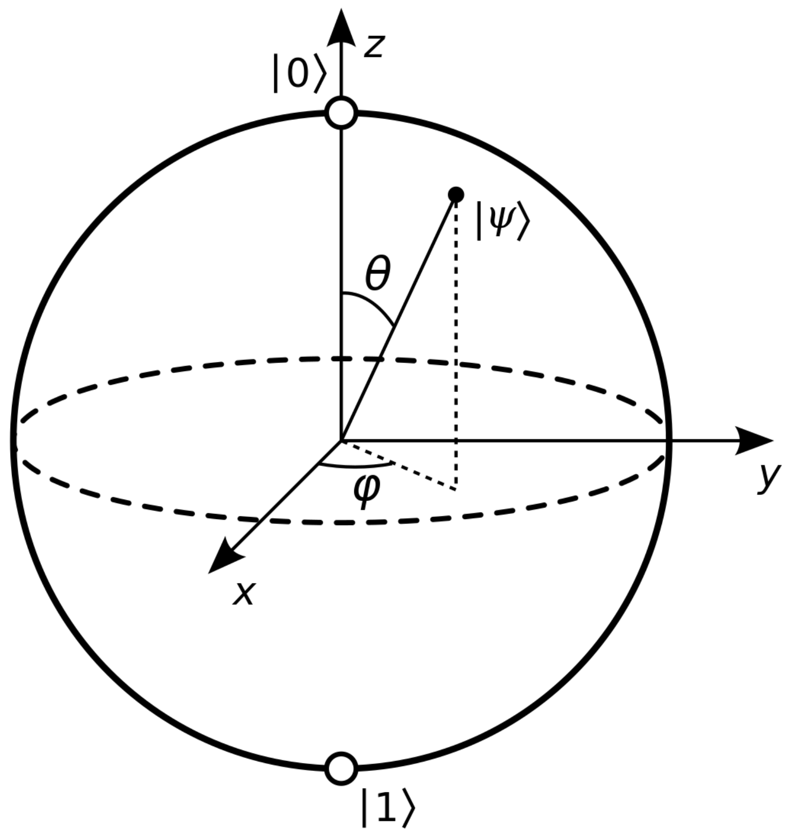
This talk

What is a quantum bit?

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$$

$$= \alpha|0\rangle + \beta|1\rangle$$

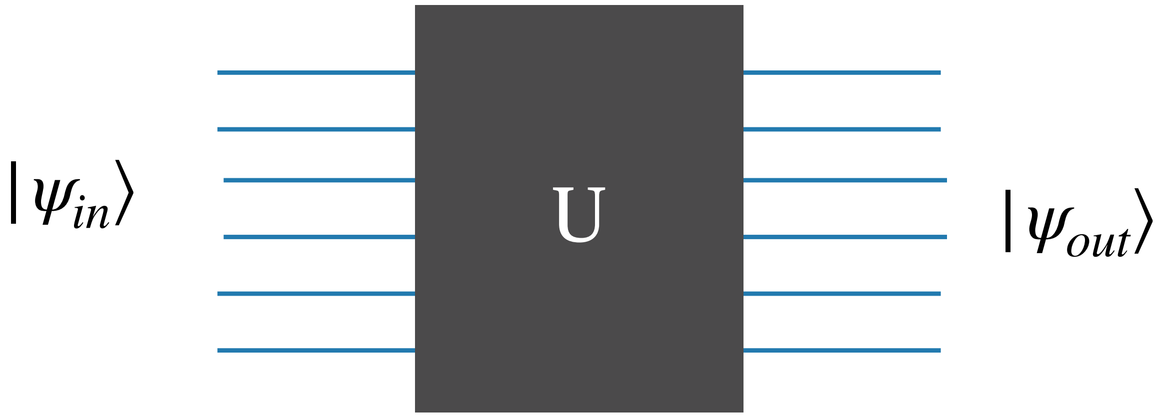
$$|\alpha|^2 + |\beta|^2 = 1$$



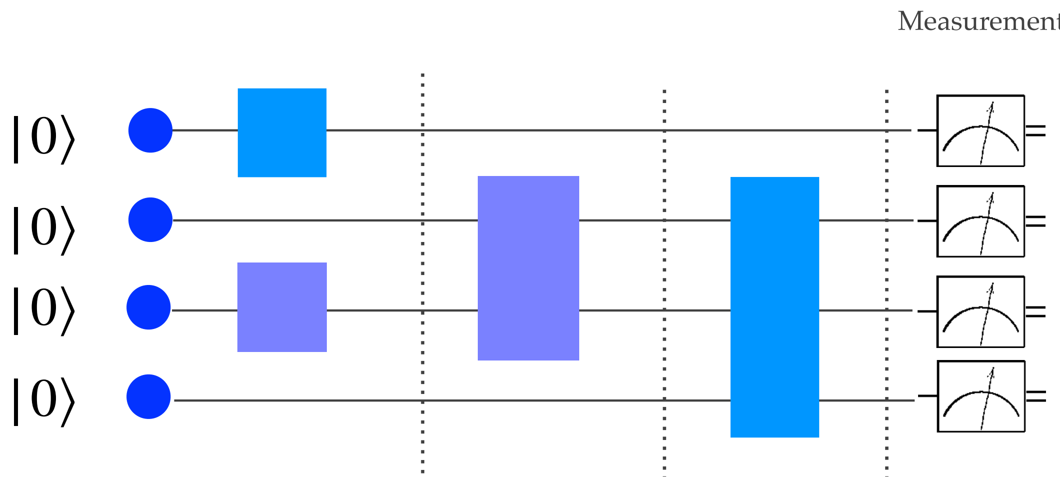
Quantum operations are given by unitary matrices

$$|\psi_{out}\rangle = U|\psi_{in}\rangle$$

$$U^\dagger = U^{-1}$$



$$Pr(x) = |\alpha_x|^2$$



$$|\psi_{out}\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Quantum circuits

Special quantum operations

Pauli

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

Clifford

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

Clifford + T gates are universal for quantum computing

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Gottesman-Knill Theorem:

Starting with Stabilizer states,

Clifford gates can be simulated efficiently

What is a stabilizer state?

We say A stabilizes $|\psi\rangle$, if $A|\psi\rangle = |\psi\rangle$

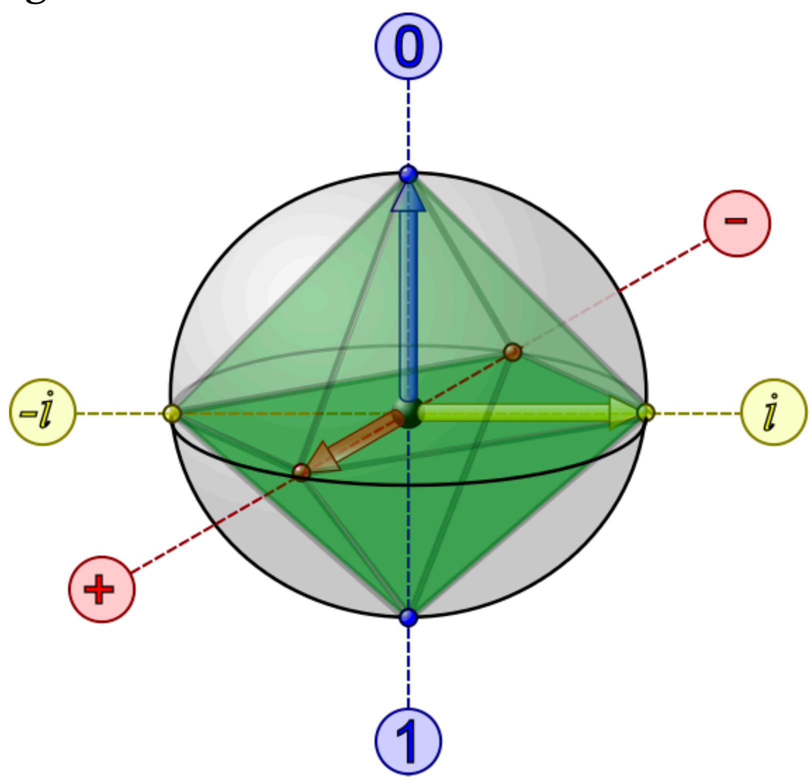
Pauli group $\mathscr{P} = \{e^{im\pi/2}A_1 \otimes \ldots \otimes A_n : A_i \in \{I, X, Y, Z\}, m \in \{0,1,2,3\}\}$

A quantum state is called a stabilizer state if there is a (Abelian) subgroup of $\mathscr{P}$ that stabilizes it.

Fact: Stabilizer states are exactly states that can be generated by Clifford operations, starting from $|0\ldots 0\rangle$

Single qubit stabilizer states:

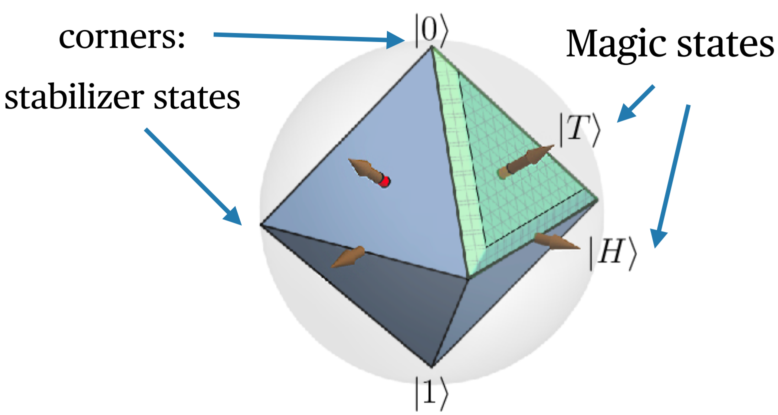
“Special discrete subset of quantum states that are stabilized by Pauli strings.”



Credit: Jonas Anderson et. al. UNM

The T state

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

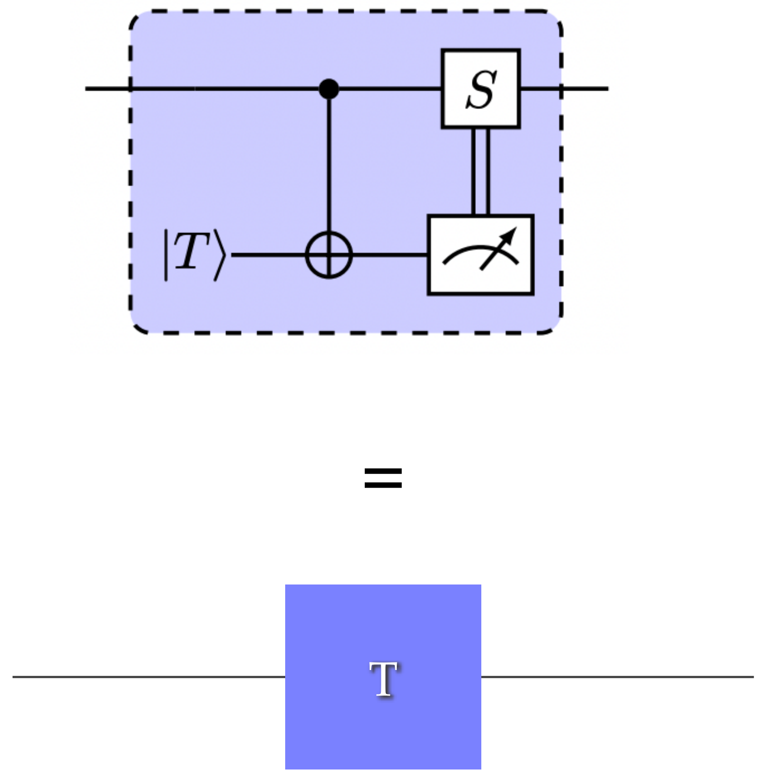


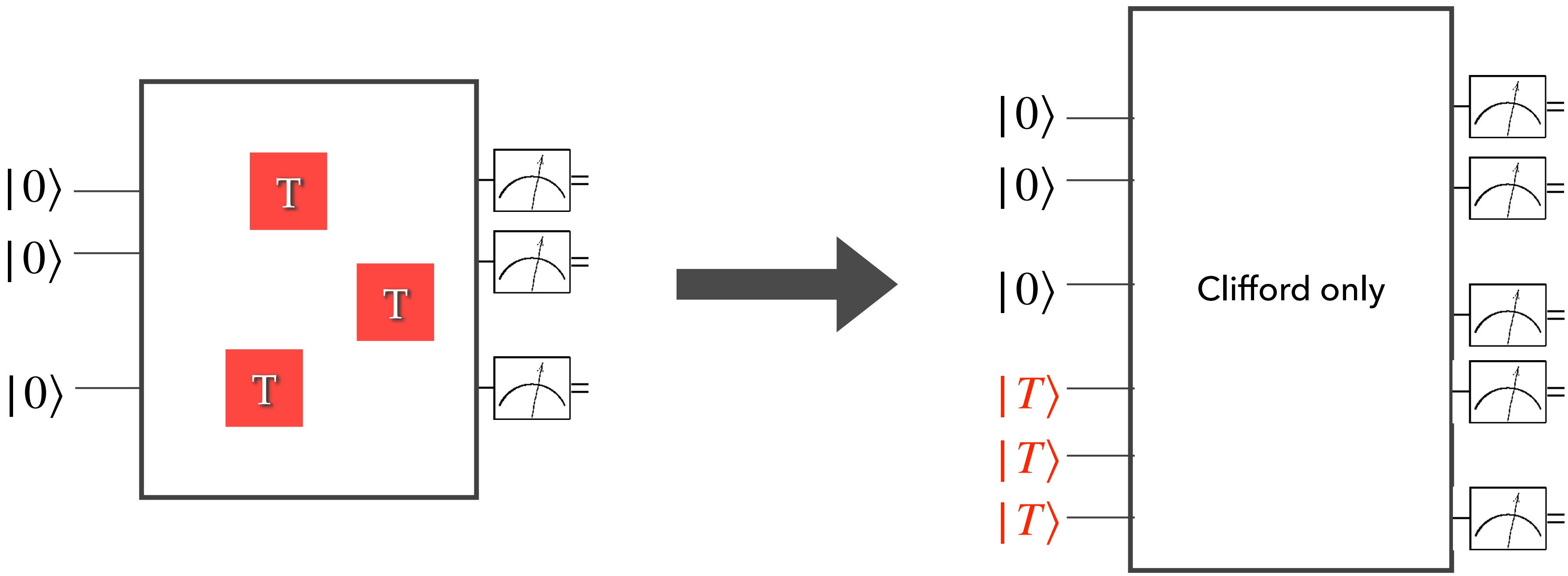
credit: Dawkins Howard, PRL

Example: 1 qubit

Magic state teleportation:

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





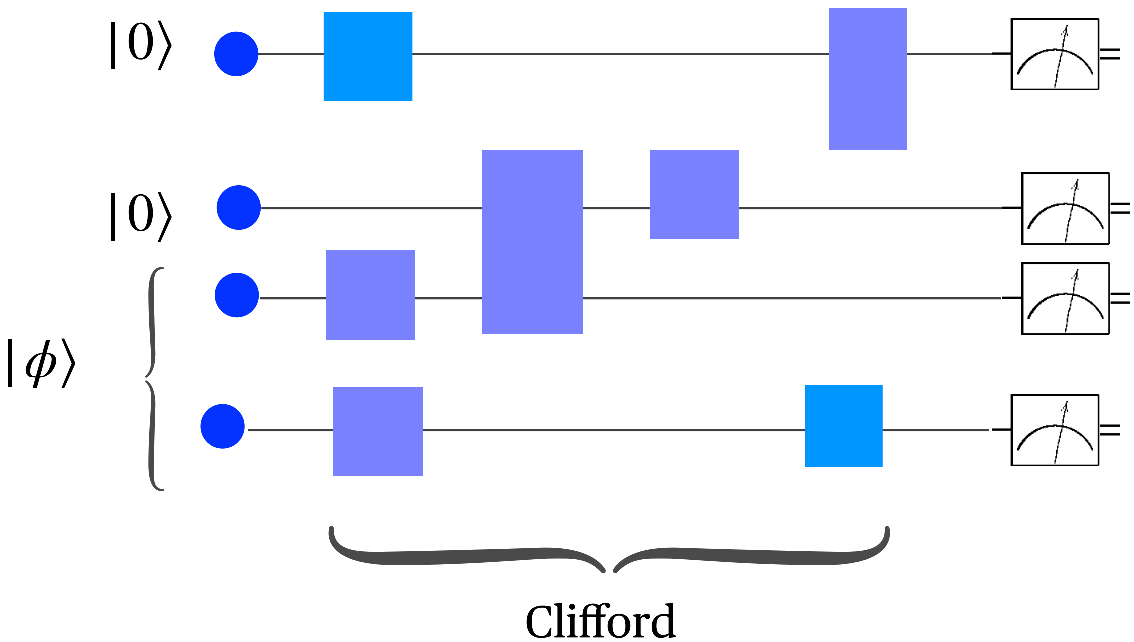
|0⟩
|0⟩
|0⟩
T
T
T
|0⟩
|0⟩
|0⟩
|T⟩
|T⟩
|T⟩
Clifford only

How hard is it to simulate the following circuit?

If $|\phi\rangle$ is a stabilizer state then we can do it in polynomial time.

What if $|\phi\rangle$ is not a stabilizer state?

It depends on the **stabilizer rank** of $|\phi\rangle$!



Approximate Stabilizer rank:

$\chi_\delta(|\phi\rangle)$ minimum number r s.t.

$|\phi\rangle \approx_\delta c_1|s_1\rangle + \ldots + c_r|s_r\rangle$ s_i stabilizer states.

Exact rank: $\delta = 0$

Bravyi Gosset 2016:

Universal quantum circuits using mT gates can be approximately simulated within error $O(\delta)$ in time $poly(n) \times \chi_\delta(|T\rangle^{\otimes m})$.

Proof idea: Teleport T gates to simulate the computation using Clifford gates on $|T\rangle^{\otimes m}$ states. Decompose the computation into χ_n Gottesman-Knill algorithms (each taking $poly(n)$ time).

Upperbound:

$\chi(|T\rangle^{\otimes n}) = O(2^{0.3963n})$

(Qassim-Pashayan-Gosset 2018)

Question:

Can we show that $\chi(|T\rangle^{\otimes n}) = 2^{\Omega(n)}$?

We better do, otherwise BQP has a fast classical simulation :-)

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 $f: \{0,1\}^n \to \{0,1\}$ 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

Proof of our result:

Step 1:
Approx Stabilizer rank of a random state is $\approx 2^n$

→

Step 2:
We can prepare arbitrary state using $\approx 2^{n/2}$ number of T gates
(and many ancilla qubits)

→

Step 3:
We can teleport T gates into T states

Step 2 is based on a non-trivial result of Low, Kliuchnikov and Schaeffer from 2018 (LKS 18) that we can synthesize arbitrary quantum states using $2^{n/2}$ T gates and many ancilla qubits

Theorem 1: If $|\phi\rangle$ is sampled from the Haar measure over n qubits, then

$$Pr\left(\chi_\delta(|\phi\rangle) \geq (1-\delta^2)^2 \frac{2^n}{\text{poly}(n)}\right) \geq 1 - o(1)$$

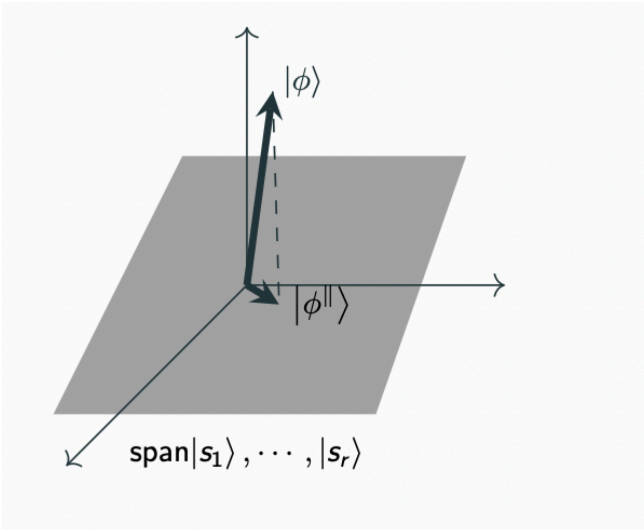
Proof idea:

Let $|s_1\rangle, \ldots, |s_r\rangle$ be a collection of r stabilizer states and

$|\phi^{\parallel}\rangle$ be the projection of $|\phi\rangle$ onto $\text{span}\{|s_1\rangle, \ldots, |s_r\rangle\}$.

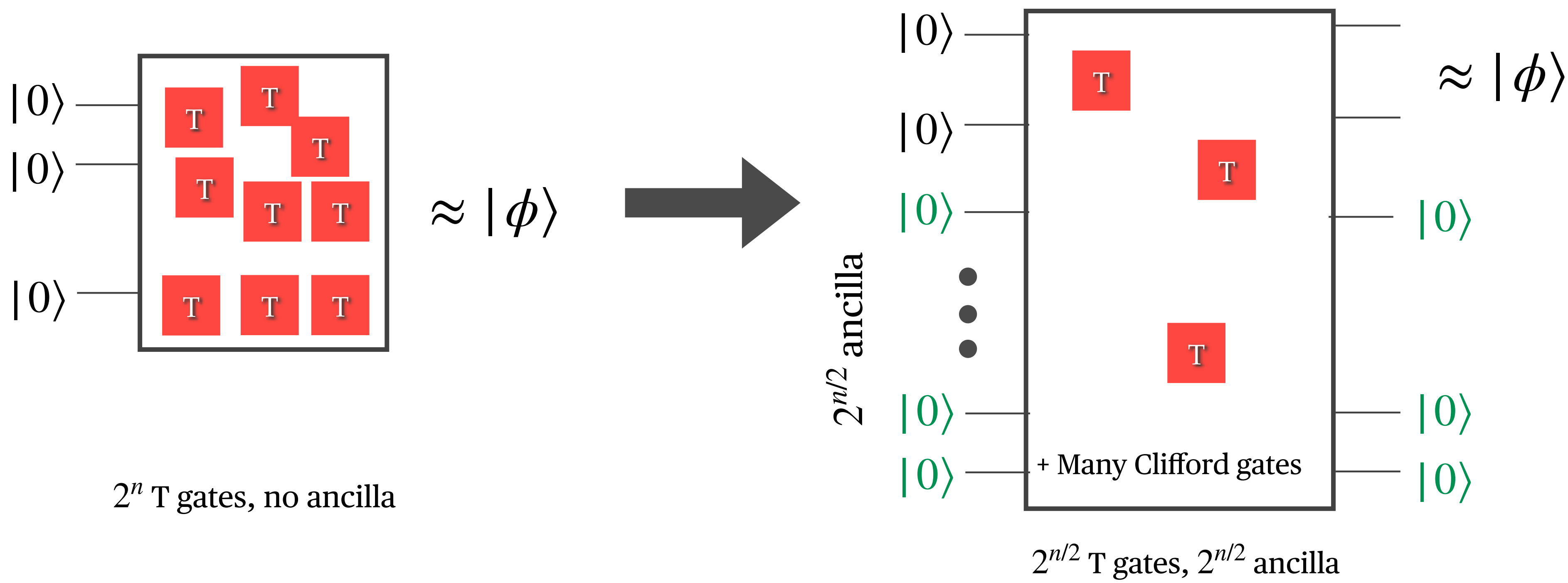
$\||\phi^{\parallel}\rangle\|$ strongly concentrates a small value when $r < \dfrac{2^n}{poly(n)}$

We use union bound over different collections of stabilizer states

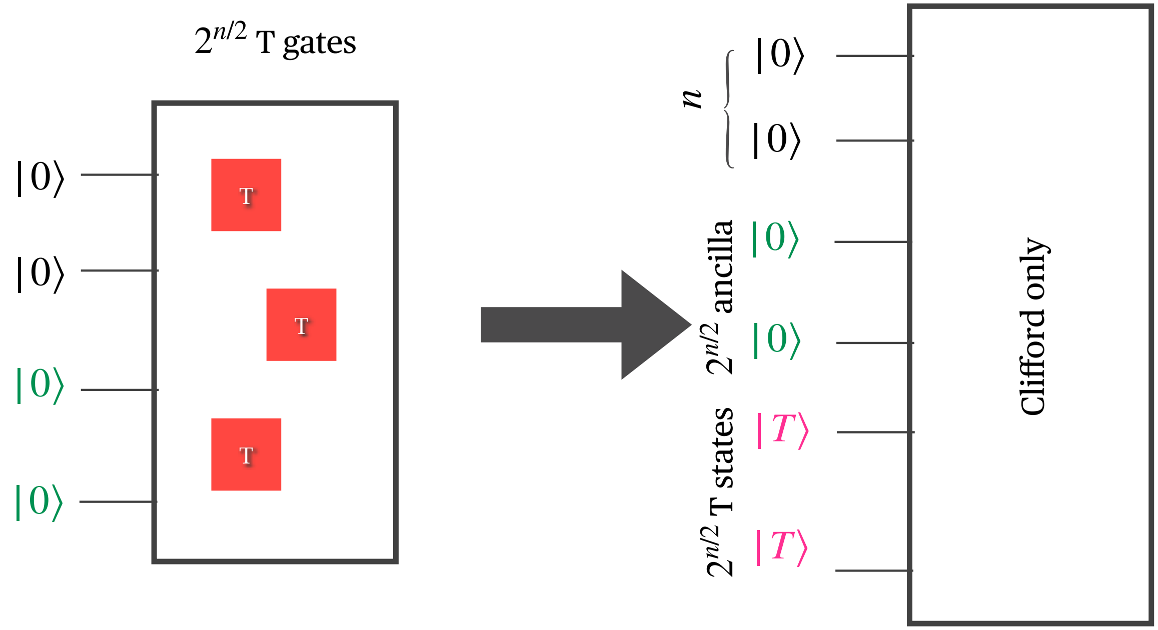


Theorem 2: (LKS 18)

Starting from $|0\dots0\rangle$ any quantum state over n qubits can be constructed using $2^{n/2}$ T gates, $2^{n/2}$ ancilla qubits and many Clifford gates



Step 3: Perform gate teleportation



Lemma 3: Stabilizer rank does not change under gate teleportation

Putting it all together:

$$\chi_\delta(|0^{n+\lambda}\rangle|T\rangle^{\otimes 2^{n/2}}) \geq \chi_\delta(|0^n\rangle|\phi\rangle) \geq 2^{n-o(1)}$$

Change of variables: $m = 2^n \implies \chi_\delta(|T\rangle^{\otimes m}) \geq \tilde{\Omega}(m^2)$

Discussion and open questions:

- **Going beyond quadratic bounds:**
  Idea 1: Other random ensembles? For Haar measure our bounds are almost tight
  Idea 2: If $\chi_\delta(|\psi\rangle \otimes |\phi\rangle) > 2^{(1+\epsilon)n}$ for random n qubit states may imply stronger lower bounds

- **Any deeper complexity theoretic insights?**
  Previous results used a "natural" property of low stabilizer rank states
  We prove lower bound from an upper bound (state synthesis) problem

- **Other physical particles (Bosons, Fermions, …)**

Thank You!

Discussion and open questions:

- **Going beyond quadratic bounds:**

Idea 1: We need a ``pseudo-random" state that has high stabilizer rank but requires few T gates to prepare.

Idea 2: Stabilizer rank is extensive for random states.
I.e. If $|\psi\rangle$ and $|\phi\rangle$ random states then $\chi_\delta(|\psi\rangle \otimes |\phi\rangle) > (\chi_\delta(|\psi\rangle)\chi_\delta(|\phi\rangle))^{1/2+\epsilon}$
It is enough to show this for $\epsilon \sim \dfrac{1}{\sqrt{n}}, \delta \sim \dfrac{1}{2^n}$. We can show this for $\epsilon = 1/2, \delta = \dfrac{1}{2^{2^n}}$.

- **Barrier to proving stronger bounds?**

All the previous techniques (Labib, Peleg, Shpilka, Volk, Lovitz, Steffan 2022) stopped at the linear lower bound. They had one thing in common they used **a property of low stabilizer ranks**. In a way **they gave a natural proof**!

Our work does not use a property. **We rather reduce the lower bound question to an upper bound on a state synthesis problem.**

Is there a deeper complexity theoretic insight involved?

- **Other directions**

Conditional lower bounds:

We can show that exact stabilizer rank is superpolynomial unless permanent has short circuits.

Can we say the same thing about approximate rank?

Bosonic Gaussian rank

Question: Decompose $z_1 \ldots z_n$ into sum of Gaussian Holomorphic functions