Title: Fine-grained quantum supremacy and stabilizer rank

Speakers: Tomoyuki Morimae

Collection: Symmetry, Phases of Matter, and Resources in Quantum Computing

Date: November 27, 2019 - 10:15 AM

URL: http://pirsa.org/19110131

Abstract: It is known that several sub-universal quantum computing models cannot be classically simulated unless the polynomial-time hierarchy collapses. However, these results exclude only polynomial-time classical simulations. In this talk, based on fine-grained complexity conjectures, I show more ``fine-grained" quantum supremacy results that prohibit certain exponential-time classical simulations. I also show the stabilizer rank conjecture under fine-grained complexity conjectures.

Fine-grained quantum supremacy and stabilizer rank

Tomoyuki Morimae

Yukawa Institute for Theoretical Physics,

Kyoto University

40min

TM and Tamaki, arXiv:1901.01637
Hayakawa, TM, and Tamaki, arXiv:1902.08382

YUKAWA INSTITUTE FOR THEORETICAL PHYSICS

Outline

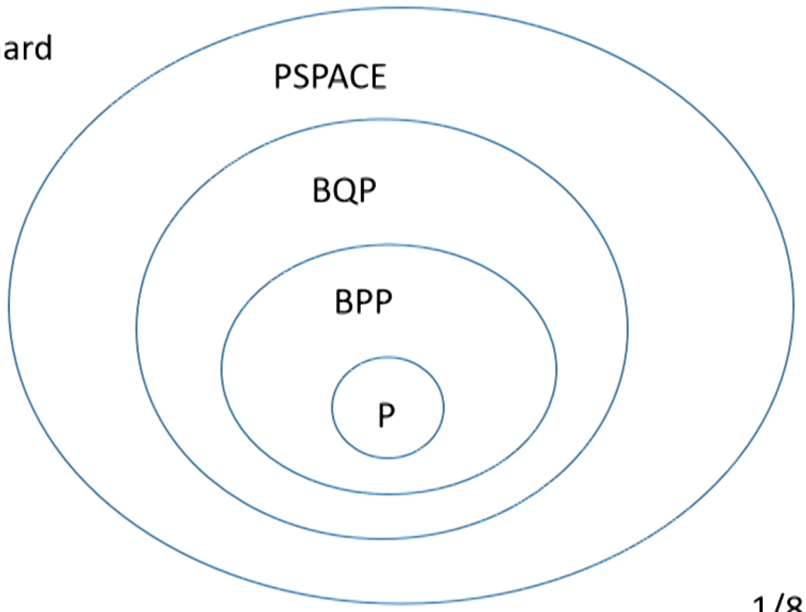
- Basic back ground of ``traditional” quantum supremacy theory (10min)
- Fine-grained quantum supremacy (15min)
- T-scaling and stabilizer rank (15min)

``Traditional" quantum supremacy theory

We want to (theoretically) show quantum computing is really faster than classical computing

In terms of complexity theory, it means BQP≠BPP.
it is still open!

Showing BQP≠BPP will be extremely hard
(BQP≠BPP → P≠PSPACE)



1/8

Four approaches to separate Q and C

That said, we have many evidences that Q is faster than C.

1. Query complexity (Grover, Simon, etc.)

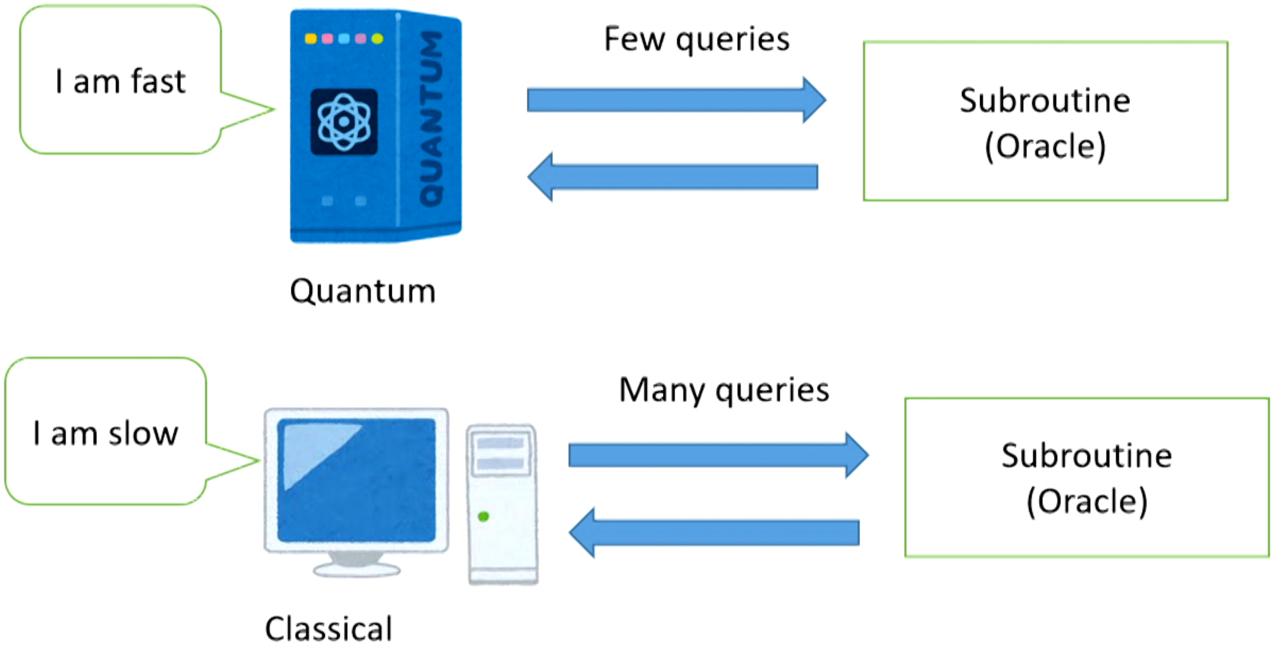
2. Faster than classical best algorithms (Shor, Q simulation, etc.)

3. Quantum supremacy (Sampling)

4. Shallow circuit

2/8

Query complexity



→Grover, Simon, etc.
→ Standard approach in complexity theory
→Q-C separation is possible unconditionally
→Query complexity ≠ real time complexity

3/8

Faster than classical best

Evaluate real time complexity

Show faster than classical best algorithms

Factoring: classical is slow, quantum is fast

→no known mathematical proof that classical is slow

Classical fast algorithm for factoring could be found！

Classical best algorithm could be updated!

Ex: recommendation system

→Ewin Tang...

4/8

Sampling

Let U be an n-qubit quantum circuit

$$p_z \equiv |\langle z|U|0^n\rangle|^2 \qquad z \in \{0,1\}^n$$

p_z is classically sampled within a multiplicative error ε in time T iff there exists a classical T time probabilistic algorithm that outputs z with probability q_z such that

$$|p_z - q_z| \leq \epsilon p_z$$

for all z

p_z is classically sampled within an additive error ε in time T iff there exists a classical T time probabilistic algorithm that outputs z with probability q_z such that

$$\sum_z |p_z - q_z| \leq \epsilon$$

If quantum computing is classically sampled in polynomial time, then PH collapses

5/8

Multiplicative error sampling

If a sub-universal model is classically sampled within a multiplicative error ε<1, then the polynomial-hierarchy collapses to the 3rd level

$$|p_z - q_z| \leq \epsilon p_z$$

Depth-4 circuit: Terhal-DiVincenzo (BQP is in AM)
IQP: Bremner-Jozsa-Shepherd
Boson sampling: Aaronson-Arkhipov
DQC1 (one-clean qubit model): Knill-Laflamme; Morimae-Fujii-Fitzsimons

postBQP=postBPP

3rd level collapses can be improved to the 2nd level collapse [Fujii-Kobayashi-Morimae-Nishimura-Tani-Tamate (abc)]

NQP=NP

L is in NP iff there exists a PPT machine such that
If x in L then p_{acc}>0
If x is not in L then p_{acc}=0

$$\mathrm{PH} \subseteq \hat{\mathrm{BP}} \cdot \mathrm{coC_{=}P} = \hat{\mathrm{BP}} \cdot \mathrm{NQP} \subseteq \hat{\mathrm{BP}} \cdot \mathrm{NP} \subseteq \mathrm{AM}$$

6/8

Additive error sampling

If a sub-universal model is classically sampled within an additive error, then the polynomial-hierarchy collapses to the 3rd level

$$\sum_z |p_z - q_z| \le \epsilon$$

IQP: Bremner-Montanaro-Shepherd
Boson sampling: Aaronson-Arkhipov
DQC1: Morimae
Random circuit: Bouland-Fefferman-Vazirani

Computing f(z) within a multiplicative error 1/100 for at least 1/10 fraction of z is #P-hard

f(z): Ising partition function, permanent, etc.

Following versions are proven:

Computing f(z) ~~within a multiplicative error 1/100~~ exactly for at least 1/10 fraction of z is #P-hard
Computing f(z) within a multiplicative error 1/100 for at least ~~1/10 fraction of~~ a single z is #P-hard

Only for Boson sampling, an additional conjecture, anti-concentration, is necessary.

Shallow quantum circuit

Bravyi-Gosset-Koenig 2018

Universal quantum (BQP)

``weak" quantum

Sampling (under complexity conjectures)

Universal classical (P)

``very weak" quantum (constant depth)

Shallow circuit （unconditional）

``very weak" classical (constant depth)

8/8

Fine-grained quantum supremacy

Fine-grained quantum supremacy

Traditional quantum supremacy:

Sub-universal quantum models cannot be classically simulated in polynomial time (unless PH collapses)

These results do not exclude super-polynomial time classical simulations
→They could be simulated in classical $2^{0.5N}$ time…

Exponential-time classical simulation is infeasible, and hence useless →wrong!

(1) Near-term medium-size quantum machine could be classically simulated.
(2) Non-trivial exponential-time classical simulation algorithm.
[e.g., Bravyi-Smith-Smolin-Gosset: $2^{0.48t}$-time algorithm]

→Can we also exclude exponential-time classical simulation?

1/11

``Standard” complexity theory will not be useful for this purpose.

→ It is not ``fine-grained”: only polynomial vs exponential.

fine-grained complexity theory! (SETH, OV, 3SUM, APSP…)

Main result (Informal):

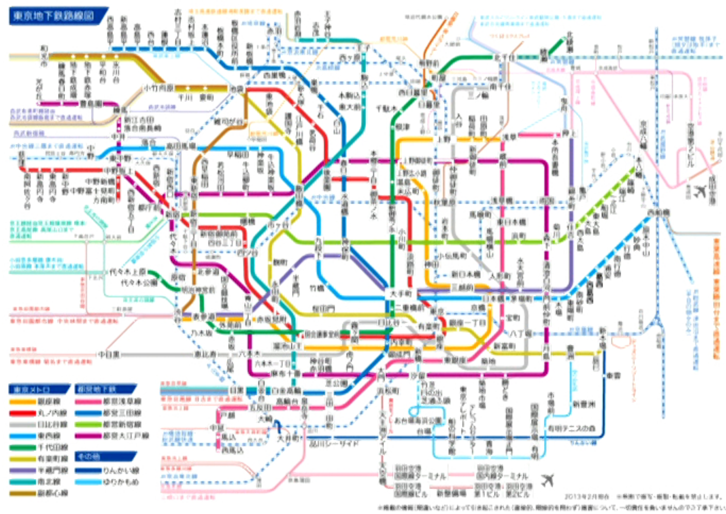
Sub-universal quantum computing models cannot be classically sampled even in some exponential-time under certain fine-grained complexity conjectures.

Related works:

Dalzell-Harrow-Koh-La Placa: Multiplicative error sampling of IQP, QAOA, Boson sampling

Huang-Newman-Szegedy: Strong simulation based on ETH

Exponential time hypothesis



Find a solution among 2^n possibilities

Impossible in *poly(n)* time → P≠NP hypothesis

Impossible in $2^{o(n)}$ time → Exponential time hypothesis (ETH)

Almost 2^n time is necessary → Strong exponential time hypothesis (SETH)

3/11

SETH-like conjecture

SETH:

For any a>0, there exists k such that k-CNF-SAT over n variables cannot be solved in time $2^{(1-a)n}$

Modified SETH:

Let f be a log-depth Boolean circuit over n variables. Then for any a>0, deciding gap(f)≠0 or =0 cannot be done in non-deterministic time $2^{(1-a)n}$

$$gap(f) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$$

1: k-CNF → log-depth Boolean circuit
2: #f>0 or =0 → gap(f)≠0 or =0
3: deterministic time → non-deterministic time

4/11

Result

Modified SETH:

Let f be a log-depth Boolean circuit over n variables. Then for any a>0, deciding gap(f)≠0 or =0 cannot be done in non-deterministic time $2^{(1-a)n}$

Result:

Assume that Conjecture is true. Then, for any a>0, there exists an N-qubit one-clean qubit model that cannot be classically sampled within a multiplicative error <1 in time $2^{(1-a)(N-3)}$

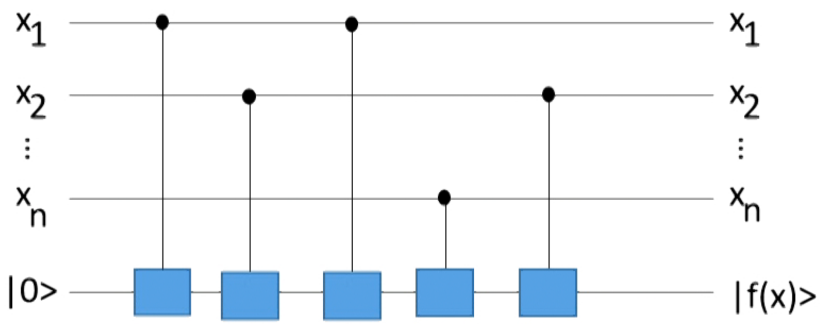
One-clean qubit model cannot be classically simulated in exponential time!

2^N -time simulation is possible: our result is optimal!

Similar results hold for many other sub-universal models (such as HC1Q)

Proof idea:

Any log-depth Boolean circuit f can be computed with single work qubit and n input qubits [Cosentino, Kothari, Paetznick, TQC 2013]

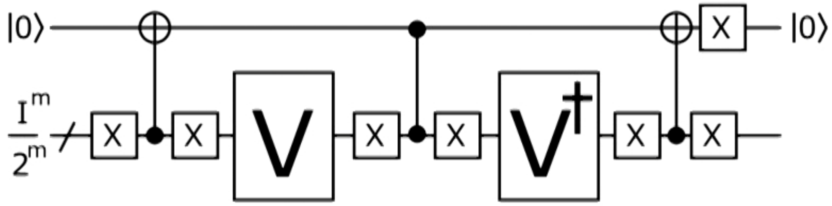


Hence we can construct an N=n+1 qubit quantum circuit V such that

$$|\langle 0^N | V | 0^N \rangle|^2 = \frac{gap(f)^2}{2^n}$$

6/11

With V, construct the one-clean-qubit circuit



If gap(f)≠0 then p_{acc}>0

If gap(f)=0 then p_{acc} =0

Assume that p_{acc} is classically sampled in time $2^{(1-a)N}$. Then, there exists a classical $2^{(1-a)N}$ -time algorithm that accepts with probability q_{acc} such that

$$|p_{acc} - q_{acc}| \leq \epsilon p_{acc}$$

If gap(f)≠0 then $q_{acc} \geq (1-\epsilon)p_{acc} > 0$

If gap(f)=0 then $q_{acc} \leq (1+\epsilon)p_{acc} = 0$

Hence, gap(f)≠0 or =0 can be decided in non-deterministic $2^{(1-a)n}$ time

→ contradicts to the conjecture!

7/11

SETH

OV

3SUM

APSP (=NWT)

Fine-grained quantum supremacy can be shown based on these conjectures.

FG Q supremacy based on OV

Conjecture:

Given d-dim vectors, $u_1, \ldots, u_n, v_1, \ldots, v_n \in \{0,1\}^d$
with d=clog(n).
For any δ>0 there is a c>0 such that deciding gap≠0 or gap=0 cannot be done in non-deterministic time $n^{2-\delta}$.

$$gap = |\{(i,j) \mid u_i \cdot v_j = 0\}| - |\{(i,j) \mid u_i \cdot v_j \neq 0\}|$$

Result:

Assume that Conjecture is true. Then, for any δ>0 there is a c>0 such that there exists an N-qubit quantum computing that cannot be classically sampled within multiplicative error ε<1 in time $2^{\frac{(2-\delta)(N-4)}{3c}}$

OV is derived from SETH: even if SETH fails, OV can still survive

9/11

FG Q supremacy based on 3-SUM

Conjecture:

Given the set $S \subset \{-n^{3+\eta}, \ldots, n^{3+\eta}\}$ of size n, deciding gap≠0 or =0 cannot be done in non-deterministic $n^{2-\delta}$ time for any η,δ>0.

$$gap = |\{(a,b,c) \mid a+b+c=0\}| - |\{(a,b,c) \mid a+b+c \neq 0\}|$$

Result:

Assume the conjecture is true. Then, for any η,δ>0, there exists an N-qubit quantum computing that cannot be classically sampled within a multiplicative error ε<1 in time $2^{\frac{(2-\delta)(N-15)}{3(3+\eta)}}$

No relation is known between SETH and 3SUM

A kind of risk hedge..

10/11

Additive-error FG supremacy

Let f be an n-variable degree-3 polynomial over F_2. It is impossible to compute gap(f) within a multiplicative error 1/100 in PTIME(2^{aN})^NTIME(m) for at least 1/10 fraction of z.

There exists a constant b and an N-qubit IQP model whose output probability distribution cannot be sampled within an additive error 1/100 in time 2^{bN}.

Proof idea

(1) Markov

(2) Stockmeyer → generalizing to exponential time classical algorithm

(3) Anti-concentration

11/11

T-scaling and stabilizer rank

T-scaling

So far, we have considered N-scaling (qubit scaling)

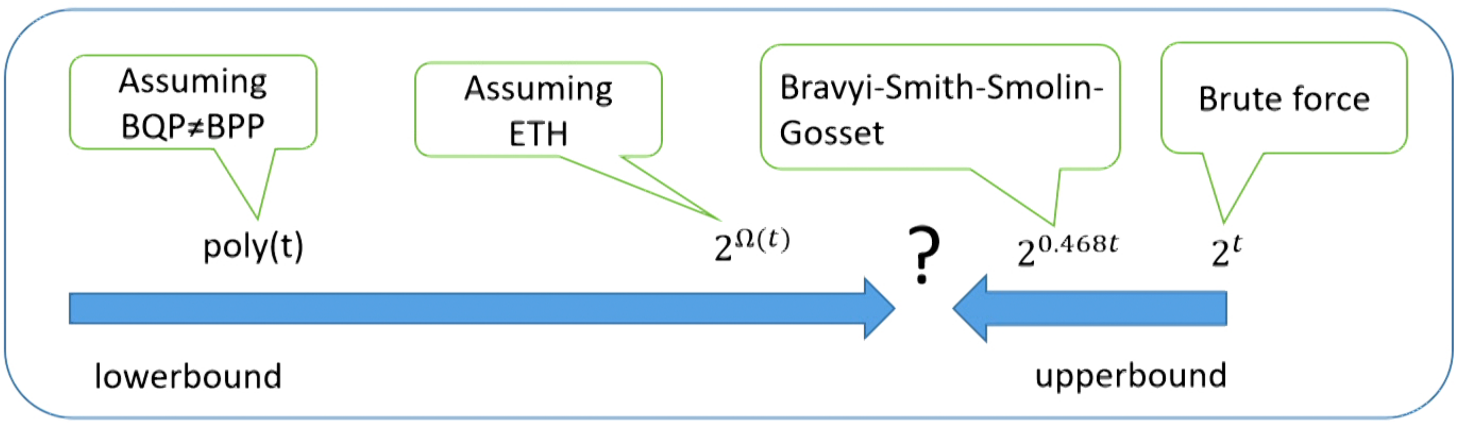
E.g., Sub-universal models cannot be classically simulated in classical 2^{aN} time

How about the T-scaling?

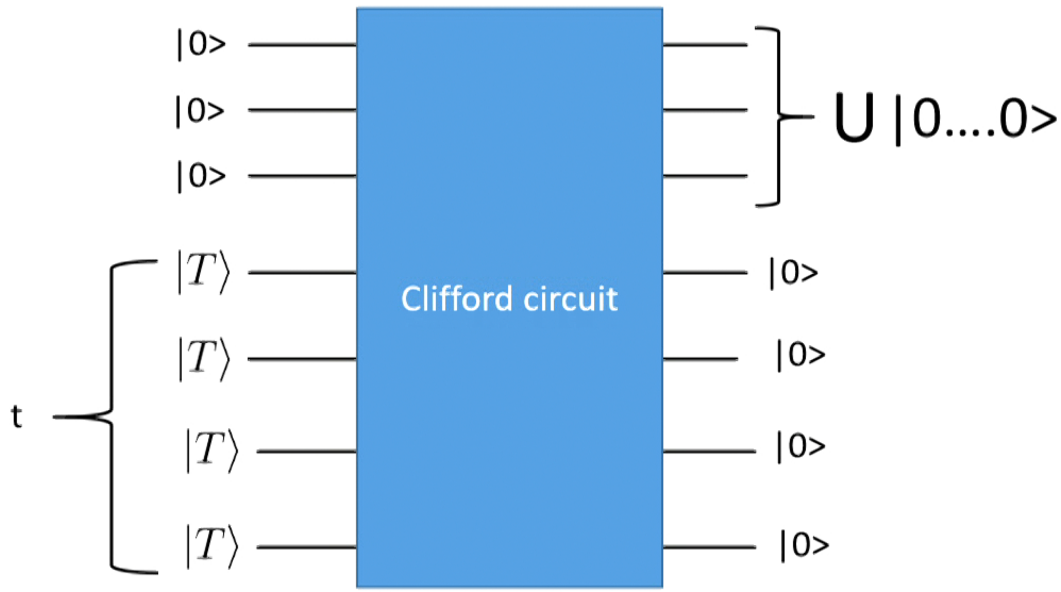
Clifford gates + T gate are universal. $$T = diag(1, e^{i\pi/4})$$

Clifford: easy
T: difficult

Near-term machines will have few T gates. → T-scaling is important!

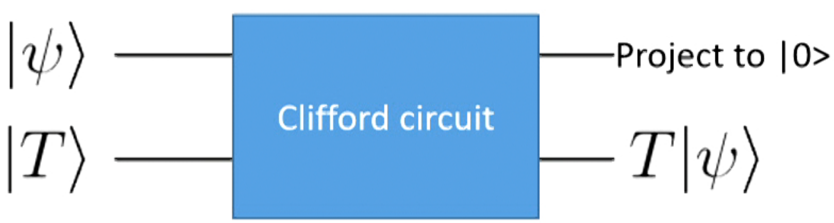


For any Q circuit U over Clifford and t T gates, there exists a Clifford circuit such that



$$|T\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$$

Magic state gadget



2/8

Classical simulation

Clifford circuit

$$\langle 0^n | U | 0^n \rangle = \sqrt{2^t} \langle 0^{n+t} | W (|0^n\rangle \otimes |T\rangle^{\otimes t})$$

Clifford and t T-gates

$$= \sqrt{2^t} \sum_{i=1}^{\chi} c_i \langle 0^{n+t} | W (|0^n\rangle \otimes |\phi_i\rangle)$$

$$|T\rangle^{\otimes t} = \sum_{i=1}^{\chi} c_i |\phi_i\rangle$$

Stabilizer state
(Clifford gates on |0…0>)

Complex numbers

$$\chi \leq 2^{0.468t}$$

Therefore, U can be classically simulated in $2^{0.468t}$ time.
[Bravyi-Smith-Smolin-Gosset]

3/8

Can we improve $2^{0.468t}$ -time simulation? (Their result is not known to be optimal)

May be to $2^{0.001t}$-time...

But, not $2^{o(t)}$!

Result:

If ETH is true, then Clifford + t T gate quantum computing cannot be classically (strongly) simulated in $2^{o(t)}$ time.

ETH

3-CNF-SAT with *n* variables cannot be solved in time $2^{o(n)}$.

For simplicity, we consider strong simulation, but similar result is obtained for sampling

(Huang-Newman-Szegedy also showed the same result independently)

4/8

Sparcification lemma is important

ETH

3-CNF-SAT with n variables cannot be solved in time $2^{o(n)}$.

↓ Sparcification lemma [Impagliazzo, Paturi, Zane]

ETH

3-CNF-SAT with m clauses cannot be solved in time $2^{o(m)}$.

f: 3-CNF over n variables. Number m of clauses is n^3

$n^3 = t$

2m AND and m-1 OR → 3m-1 Toffoli → 7(3m-1) T gates

$$\langle 0^N | U | 0^N \rangle = \frac{\# f}{2^{poly(n)}}$$

t=7(3m-1) T gates and Clifford gates

$< 0^N | U | 0^N >$ cannot be computable in $2^{o(n)} = 2^{o(t^\wedge\{\frac{1}{3}\})}$time

6/8

Corollary: stabilizer rank conjecture is true (under ETH)

Stabilizer rank χ : smallest k such that

$$|\psi\rangle = \sum_{j=1}^{k} c_j |\phi_j\rangle$$

Complex numbers

Stabilizer state
(Clifford gates on |0…0>)

Bravyi-Smith-Smolin

$$\chi(|T\rangle^{\otimes t}) \leq 2^{0.468t}$$

Stabilizer-rank conjecture:

$$\chi(|T\rangle^{\otimes t}) \geq 2^{\Omega(t)}$$

Known best (unconditional) lowerbound

$$\chi(|T\rangle^{\otimes t}) \geq \Omega(\sqrt{t})$$

The stabilizer rank conjecture is true if ETH is true.

$$\langle 0^N | U | 0^N \rangle = \frac{\# f}{2^{poly(n)}}$$

7/8

H-scaling

H + diagonal gates are universal (e.g., Toffoli) [Aharonov, Shi]

Diagonal gates are ``classical" and H is the ``resource" for quantum speedups

It is interesting to consider complexity of classical simulation in H-counting

Upperbound:

There exists $2^{0.984965h}$-time classical algorithm to (strongly) simulate H+T+CZ circuit

Lowerbound:

Assume that Conjecture is true. Then for any constant a > 0 and for infinitely many h, there exists a quantum circuit with classical gates and h H gates whose output probability distributions cannot be classically sampled in time $2^{(1-a)h/2}$ within a multiplicative error ε < 1

Conjecture:

Let f be a poly-size Boolean circuit over n variables. Then for any a>0, deciding gap(f)≠0 or =0 cannot be done in non-deterministic time $2^{(1-a)n}$

8/8

Summary

- ``Traditional" quantum supremacy prohibit only polynomial-time classical simulations.
- Fine-grained quantum supremacy: based on classical fine-grained complexity conjectures, almost 2^N-time classical simulations are excluded.
- $2^{o(t)}$ -time classical simulation of Clifford+T circuits is impossible under ETH. (Stabilizer-rank conjecture is true under ETH.)