Fine-grained quantum supremacy

Tomoyuki Morimae

(YITP, Kyoto University)

1 hour

Joint work with Suguru Tamaki (Kyoto University)

TM and Tamaki, arXiv:1901.01637, 1902.08382

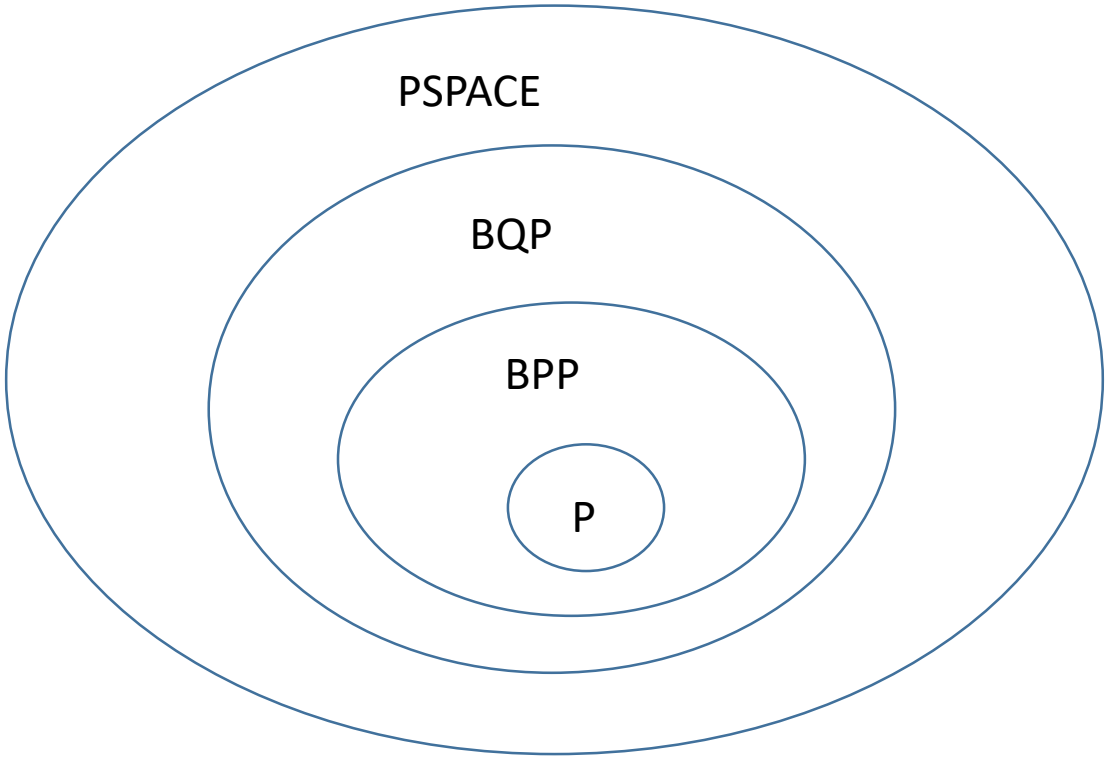
Quantum computing is really faster than classical computing?

Shor's factoring → not showing BQP≠BPP
Simon's algorithm → oracle separation of BQP and BPP

Unconditional BQP≠BPP is open

If BQP≠BPP is shown then P≠PSPACE is shown

→ showing BQP≠BPP is extremely hard!



What can we do next?

(1) Show ``If BQP=BPP then polynomial-time hierarchy collapses”

→ open
(There exists an oracle that separates BQP and P but PH is infinite [Fortnow-Rogers])

(2) Consider other problems than decision problems

→ sampling problem

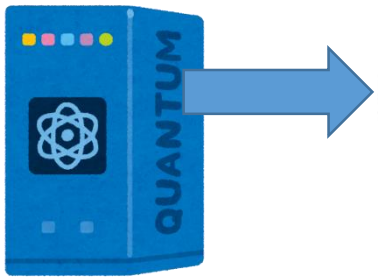
We can show

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

→ This is quantum supremacy, and the main subject of the present paper!

Sampling

We say that a quantum computing is classically sampled within a multiplicative error ε in time T if there exists a T-time classical probabilistic algorithm such that



$z \in \{0,1\}^n$

Quantum computer

Classical probabilistic T-time algorithm

$z \in \{0,1\}^n$

Multiplicative error sampling: $|p_z - q_z| \leq \epsilon p_z$

Probability that quantum computer outputs z

Probability that classical computer outputs z

If quantum computing is classically sampled within a multiplicative error ε<1 in polynomial time, then PH collapses to the second level.

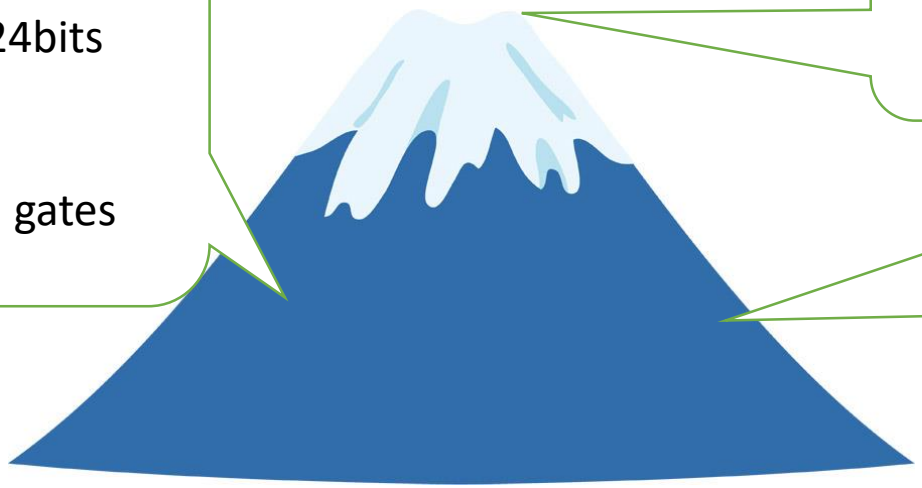
Advantage: Simpler machine is enough

If QC is classically sampled then PH collapses.

→ QC is not necessarily universal, but can be ``weak" machine

Factoring of 1024bits

2000 qubits
10^11 quantum gates



Ultimate goal:
Many qubits
universal
Fault-tolerant

Near-term goal

Demonstrate Q supremacy with weak machine

Weak machines that exhibit Q supremacy

Depth-4 circuit
Terhal and DiVincenzo, QIC 2004

Boson Sampling
Aaronson and Arkhipov, STOC 2011

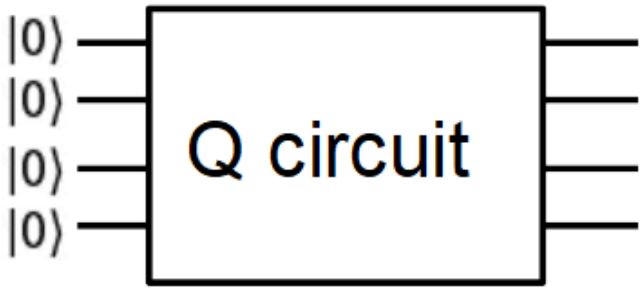
Commuting gates(IQP)
Bremner, Jozsa, and Shepherd, Proc. Roy. Soc. A 2010
（Related to classical Ising model [Fujii and TM, NJP 2015]）

One-clean qubit model
TM, Fujii, and Fitzsimons, PRL 2014

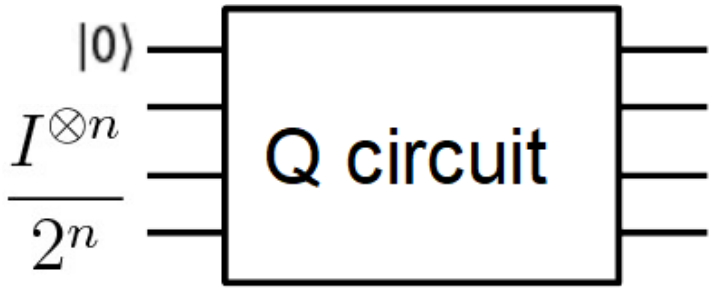
HC1Q model
TM, Nishimura, and Takeuchi, Quantum 2018

Random gates
Fefferman et al. Nature Phys. 2018

One-clean qubit model



通常の量子計算



One clean qubit model

[Knill and Laflamme, PRL 1998]

Calculating Jones polynomial faster than classical
[Shor and Jordan 2007]

Not here
[Ambainis et al. 2000]

classical

Universal quantum

Fast classical algorithm for Jones polynomial could be found…

Q supremacy of one-clean qubit model

If one-clean qubit model is classically sampled in polynomial time within a multiplicative error <1, then PH collapses to the 2^{nd} level

TM, Fujii, and Fitzsimons, PRL 2014
Fujii, Kobayashi, TM, Nishimura, Tamate, and Tani, ICALP 2018; PRL 2018

Fine-grained quantum supremacy

All previous quantum supremacy results

→ QC cannot be classically simulated in polynomial time (unless PH collapses)

→It could be classically simulated in super-polynomial time…

→Can we also exclude exponential-time classical simulation?

→YES! We can show these models cannot be classically sampled in exponential time (under some conjectures).

``Standard" complexity theory consider only polynomial or not, so it is not enough.

→ fine-grained complexity theory!

Conjectures

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

Our conjecture 1:

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 $2^{(1-a)n}$

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

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

Result 1

Our conjecture 1:

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 $2^{(1-a)n}$

Result 1:

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

If $N = n^{10}$, $2^{(1-a)N^{\frac{1}{10}}}$ -time simulation is prohibited.
Only superpolynomial result.

Result 2

Our conjecture 2:

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 2:

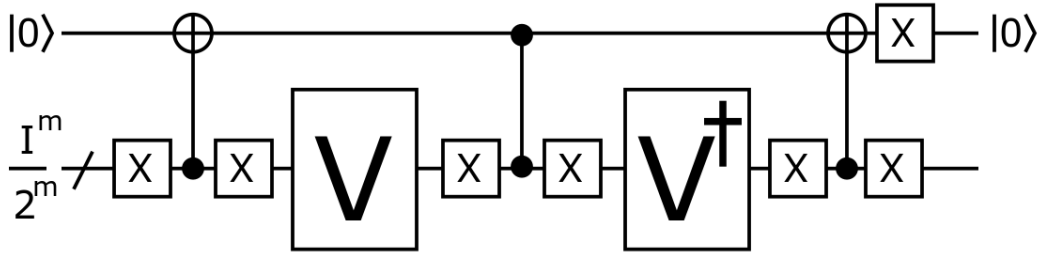
Assume that Conjecture 2 is true. Then, for any a>0, there exists an N-qubit one-clean qubit model that cannot be classically sampled within a multiplicative error <1 in time $2^{(1-a)(N-3)}$

Exponential-time result!!

Proof idea:

Given Boolean circuit f, construct a one-clean-qubit circuit such that

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



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} within a multiplicative error ε<1. 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 $q_{acc} \geq (1-\epsilon)p_{acc} > 0$

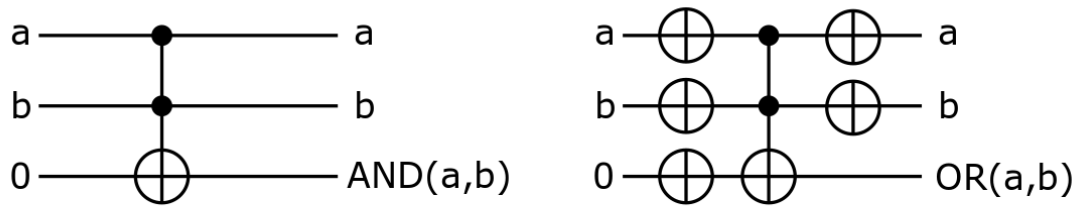
If gap(f)=0 then $q_{acc} \leq (1+\epsilon)p_{acc} = 0$

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

→ contradicts to the conjecture!

Given Boolean circuit f:{0,1}^n → {0,1}

AND and OR can be replaced with Toffoli using ancilla bit



$$U(|x\rangle \otimes |0^{\xi}\rangle) = |junk(x)\rangle \otimes |f(x)\rangle$$

$$V = H^{\otimes x+\xi}(I^{\otimes x+\xi-1} \otimes Z)U(H^{\otimes n} \otimes I^{\otimes \xi})$$

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

For log-depth circuit on n variables, we can construct an N=n+3 qubit one-clean-qubit quantum circuit V such that

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

Hence, $2^{(1-a)n} = 2^{(1-a)(N-3)}$ time classical sampling is prohibited

$$VX^aH^bX^aH^bV = X^{a\wedge b}$$

[Cosentino, Kothari, Paetznick, TQC 2013]

Q supremacy based on OV

Conjecture 3:

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 − δ}.

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

Result 3:

Assume that Conjecture 3 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 $2^{\frac{(2-\delta)(N-4)}{3c}}$

Proof idea:

We can construct an N=3d+4 qubit quantum circuit V such that

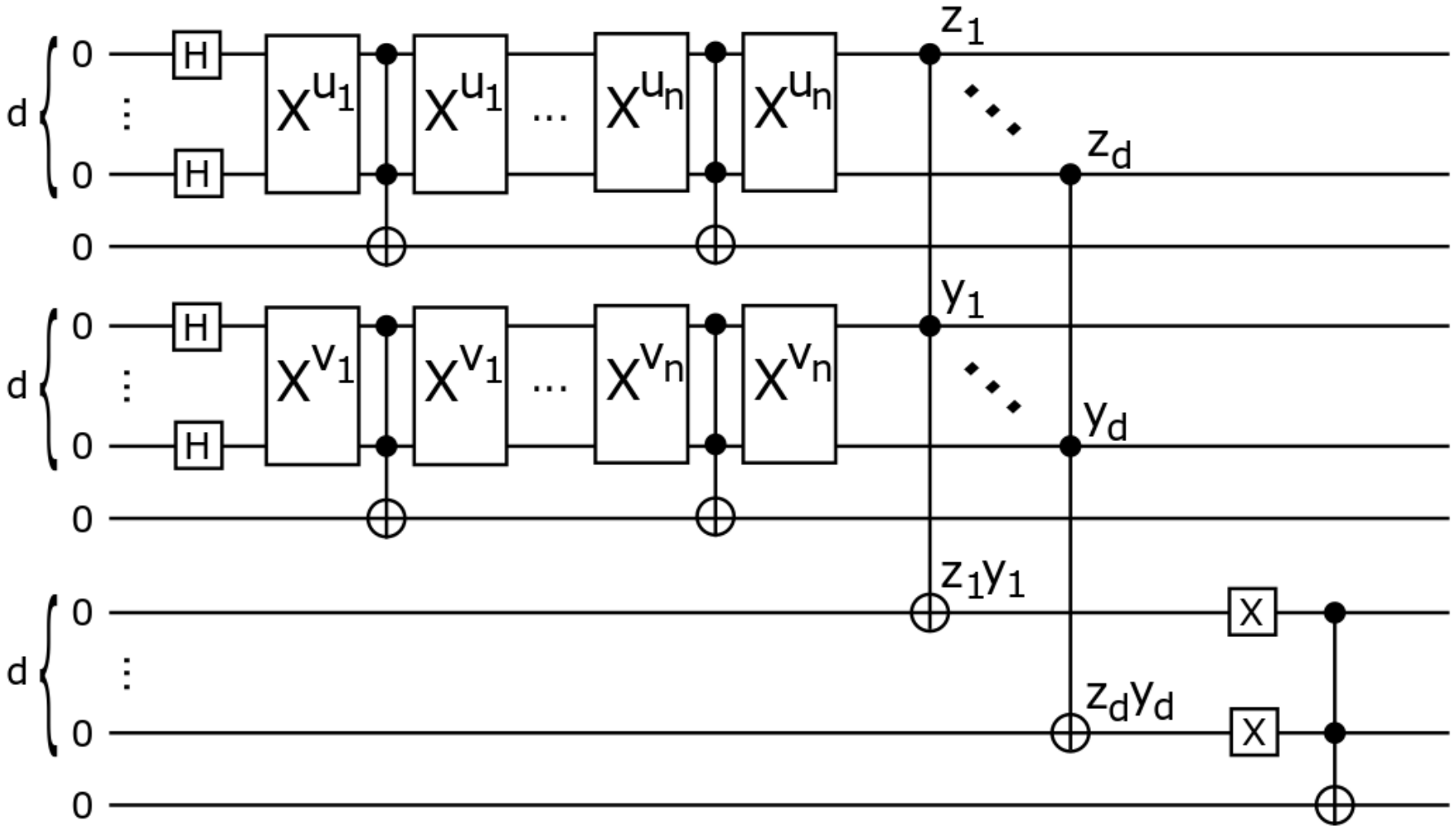
$$p_{acc} = \frac{gap^2}{2^{poly}}$$

If p_acc is classically sampled within a multiplicative error <1 in time

$$n^{2-\delta} = 2^{\frac{(2-\delta)(N-4)}{3c}}$$

then conjecture is violated.

$$N = 3d + 4 = 3(c \log n) + 4 \rightarrow n = 2^{\frac{N-4}{3c}}$$


d
0
H
X^{u_1}
X^{u_1}
...
X^{u_n}
X^{u_n}
z_1
z_d
0
d
0
H
X^{v_1}
X^{v_1}
...
X^{v_n}
X^{v_n}
y_1
y_d
0
d
0
z_1y_1
X
z_dy_d
X
0

Q supremacy based on 3-SUM

Conjecture 4:

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-δ} 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 4:

Assume the conjecture 4 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 $2^{\frac{(2-\delta)(N-15)}{3(3+\eta)}}$

Proof idea:

We can construct an N=3r+9 qubit quantum circuit V such that

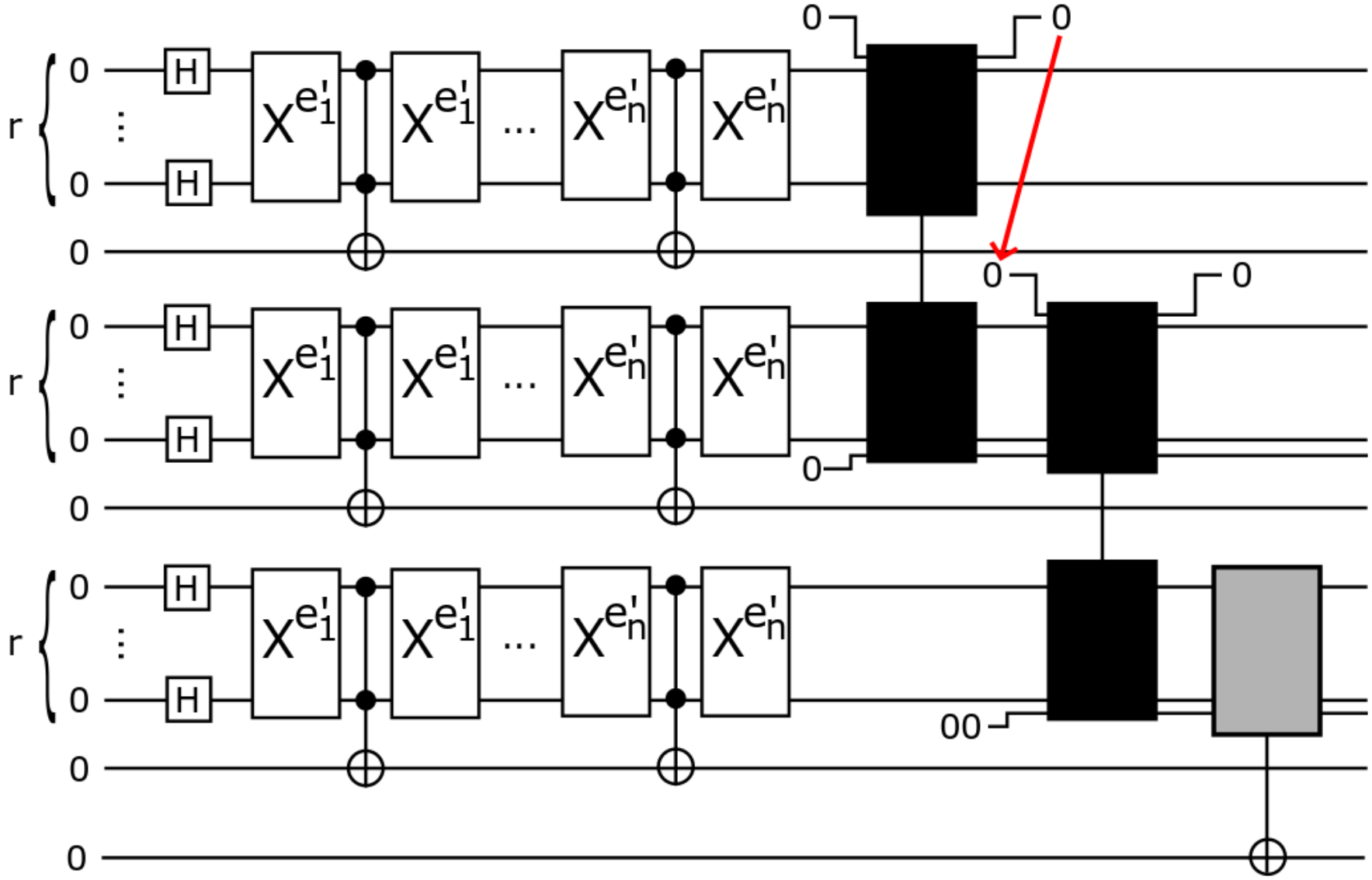
$$p_{acc} = \frac{gap^2}{2^{poly}}$$

If p_acc is classically sampled within a multiplicative error <1 in time

$$2^{\frac{(2-\delta)(N-15)}{3(3+\eta)}}$$

then conjecture is violated.

$$n^{2-\delta} \geq 2^{\frac{(2-\delta)(N-15)}{3(3+\eta)}}$$


r
0
H
$X^{e'_1}$
$X^{e'_n}$
...
00

Clifford+T quantum computing

Clifford gates: H, S=diag(1,i), and CNOT
→Classically simulatable (Gottesman-Knill theorem)

Clifford+T=universal

$$T = diag(1, e^{i\pi/4})$$

Intuitively, Q circuit with more T is more quantum….

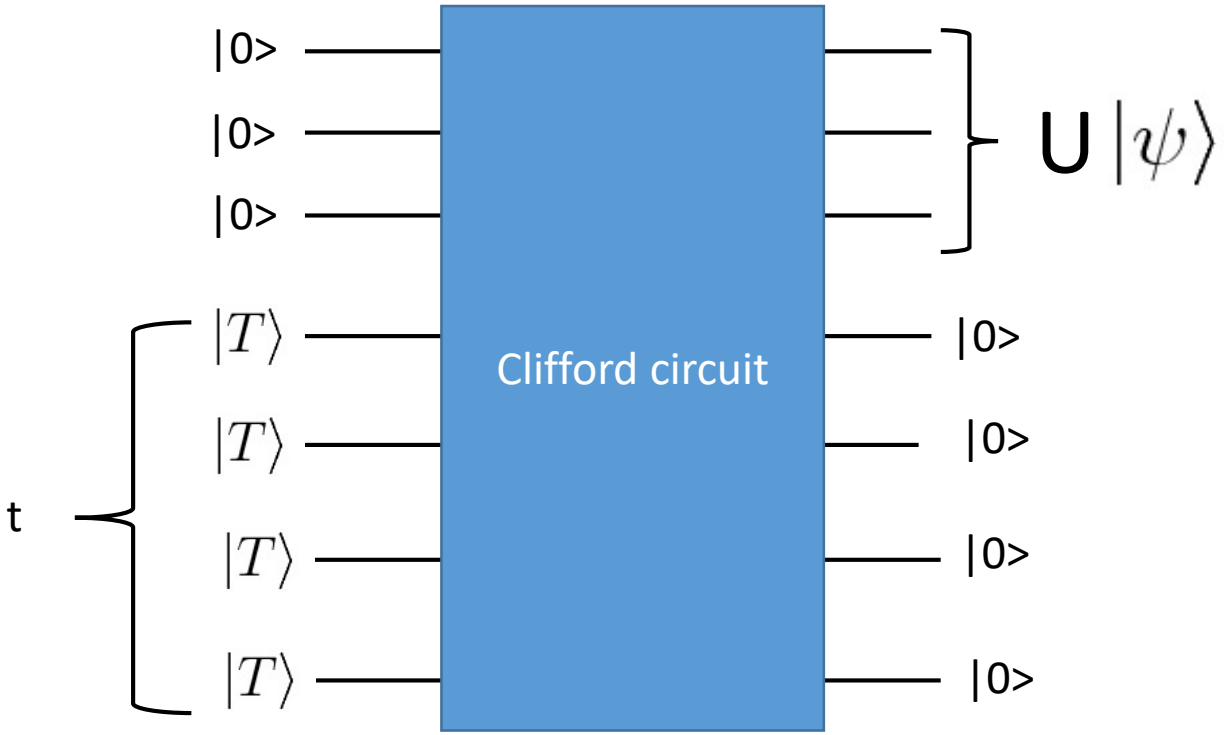
Classical calculation of the acceptance probability of quantum circuit over Clifford and t T gates:

Trivial upperbound: 2^t time (brute force)

Trivial lowerbound: poly(t) (assuming BQP≠BPP)

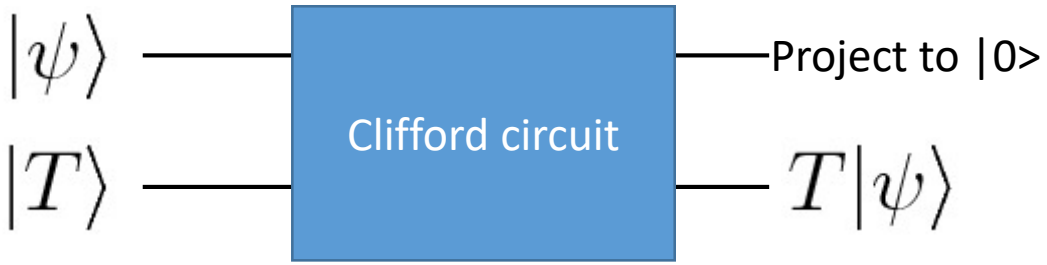
2^{0.468t} time [Bravyi-Gosset].

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



Bravyi-Gosset simulation algorithm

Stabilizer rank $\chi(|\psi\rangle)$: smallest k such that

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

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

$$\begin{aligned}\langle 0^n|U|0^n\rangle &= \langle 0^n|V(|0^m\rangle \otimes |T\rangle^{\otimes t}) \\ &= \sum_{j=1}^{\chi} c_j \langle 0^n|V(|0^m\rangle \otimes |\phi_j\rangle^{\otimes t})\end{aligned}$$

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

Therefore, Clifford+T QC can be classically simulated in 2^{0.468t} time.

Classical calculation of the acceptance probability of quantum circuit over Clifford and t T gates:

Trivial upperbound: 2^t time (brute force)

Trivial lowerbound: poly(t) (assuming BQP≠BPP)

2^{0.468t} time [Bravyi-Gosset].

Can we improve Bravyi-Gosset algorithm to 2^{o(t)} time?

→No (under ETH)
(Huang-Newman-Szegedy also showed independently)

ETH

Let f be a 3-CNF with m clause. Solving SAT for f needs time $2^{\Omega(m)}$

Proof: on the white board

Result for sampling

ETH

Let f be a 3-CNF with m clause. Solving SAT for f needs time $2^{\Omega(m)}$

Conjecture 5:

Let f be a 3-CNF with m clauses. Deciding gap(f)≠0 or =0 needs non-deterministic time $2^{\Omega(m)}$

1. #f>0 or =0 → gap(f)≠0 or =0
2. Deterministic time → non-deterministic time

Result

Conjecture 5:

Let f be a 3-CNF with m clauses. Deciding gap(f)≠0 or =0 needs non-deterministic time $2^{\Omega(m)}$

Result 5:

Assume that Conjecture 3 is true. Then, there exists Clifford+T quantum circuit with t T gates that cannot be classically sampled within a multiplicative error <1 in time $2^{o(t)}$

Stabilizer rank conjecture

Stabilizer rank: smallest k such that

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

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

Bravyi and Gosset

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

Stabilizer-rank conjecture: $\chi(|T\rangle^{\otimes t}) \geq 2^{\Omega(t)}$

Assuming ETH, we can show the stabilizer conjecture
→ unconditional proof is open!

END

Depth-scaling Q supremacy

Conjecture 3:

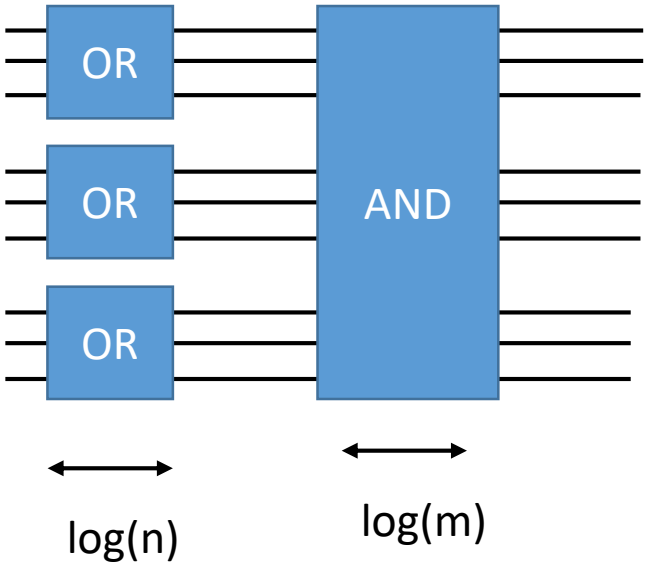
Let f be an n-variable CNF with at most cn clauses. For any a>0, there exists c>0 such that deciding gap(f)≠0 or gap(f)=0 needs non-deterministic time $2^{(1-a)n}$

Result 3:

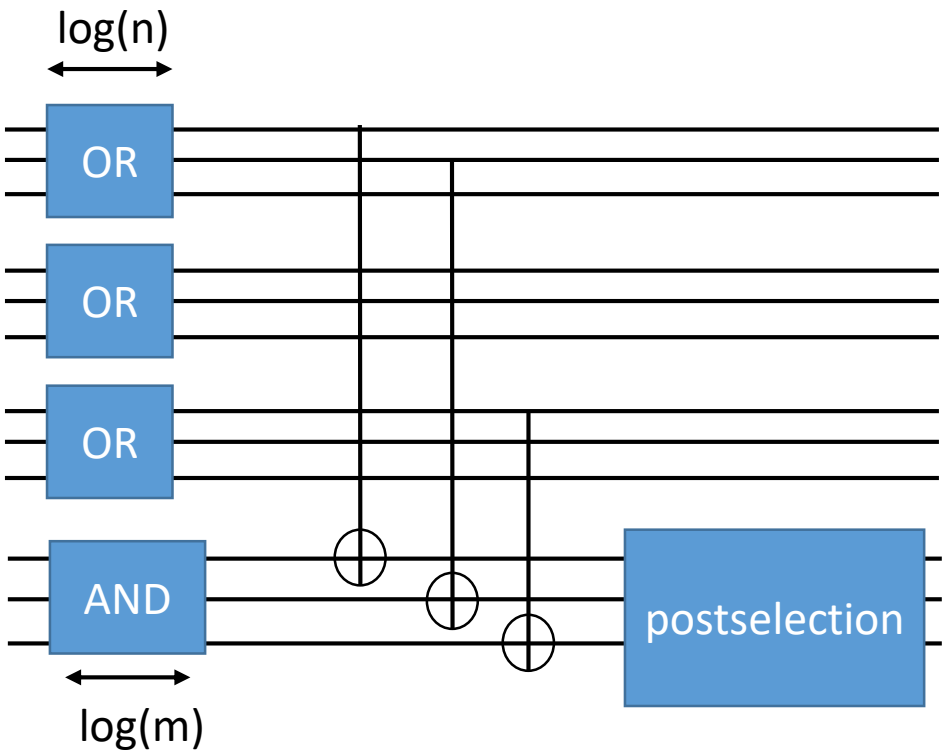
Assume that Conjecture 3 is true. Then, for any a>0 there exists c>0 and a d-depth quantum computing that cannot be classically sampled within a multiplicative error ε<1 in time $2^{(1-a)2^{d-\log_2 c-3}}$

Proof idea

Given n-variable m-clause CNF, naïve quantum circuit (depth log(n)+log(m))



Shallower quantum circuit (depth log(m))



$$|AND\rangle = \sum_{x \in \{0,1\}^m} |x\rangle \otimes |\prod_{j=1}^{m} x_j\rangle$$