# Fine-grained quantum supremacy

Tomoyuki Morimae

(YITP, Kyoto University)

45min

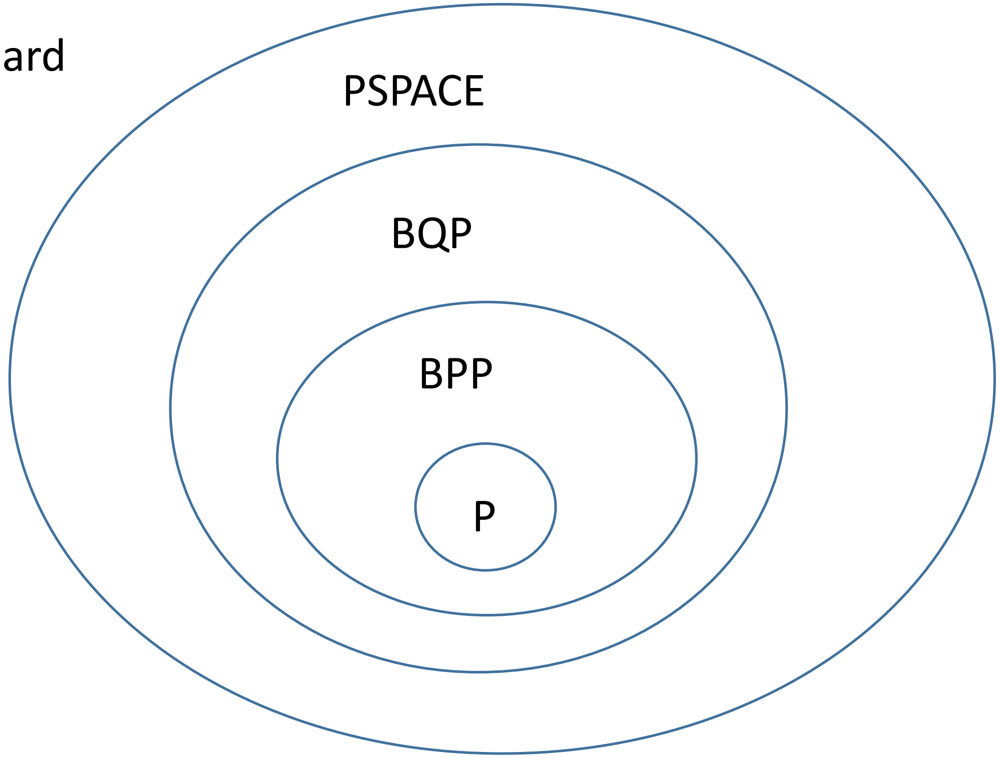
Joint work with Suguru Tamaki (Hyogo University)

TM and Tamaki, arXiv:1901.01637, 1902.08382

# People believe quantum computing is faster than classical computing, but…

In terms of complexity theory, it is still open:
BQP≠BPP is not yet shown

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



# Three approaches

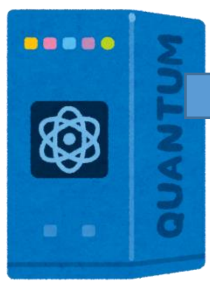
That said,…there have been many results that suggest quantum speedups

| | Advantage | Disadvantage |
|---|---|---|
| Concrete quantum algorithms:<br><br>Factoring, quantum simulation, machine learning(?), etc. | Useful | Not sure really classically hard (Ewin Tang…) |
| Query complexity:<br><br>Simon, Grover, etc. | Useful<br><br>Classical-quantum separation is rigorously shown | The quantum-classical separation is not a real time complexity: assuming oracles |
| (Sampling) Quantum supremacy:<br><br>Boson sampling, IQP, DQC1, random circuit, etc. | Reliable complexity conjecture<br><br>Weak machines are enough | No useful application is known |

# Sampling

We say that a quantum computer is classically sampled (simulated) in time T if…

Quantum computer




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

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 simulated in polynomial time, then PH collapses to the second level.

# Advantage: weak machine is enough

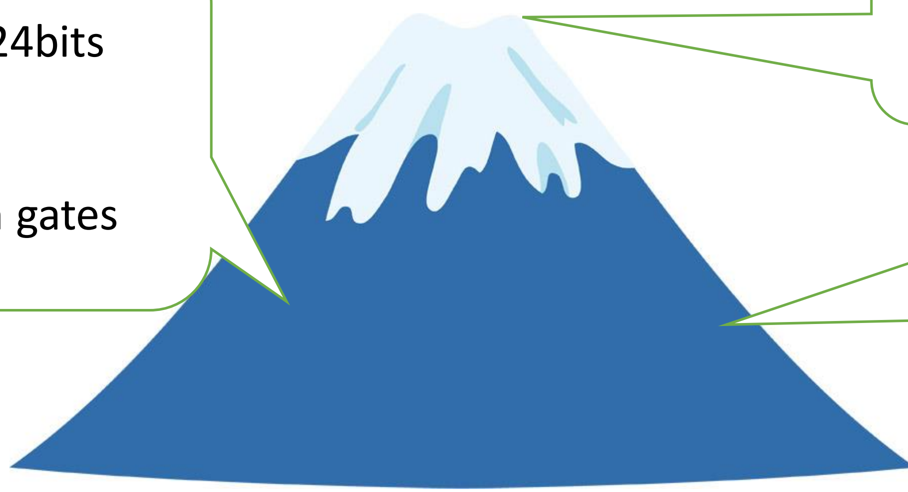
If QC is classically sampled then PH collapses.

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

Ultimate goal:
Many qubits
universal
Fault-tolerant

Factoring of 1024bits

2000 qubits
10^11 quantum gates

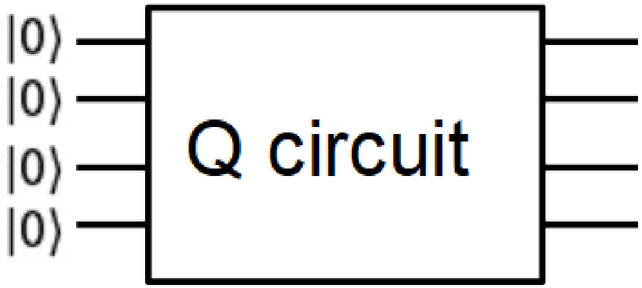


Near-term goal

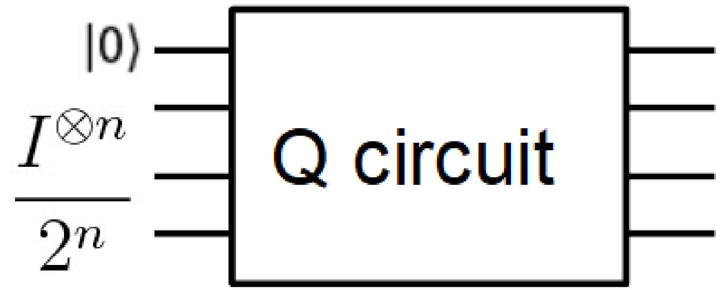
Demonstrate Q supremacy with weak machine

Q supremacy for sampling needs only weak machine
→useful for the near-term goal!

# One-clean qubit model




Standard QC




One clean qubit model

[Knill and Laflamme, PRL 1998]

Calculating Jones polynomial faster than classical

[Shor and Jordan 2007]

Not here

[Ambainis 2000]

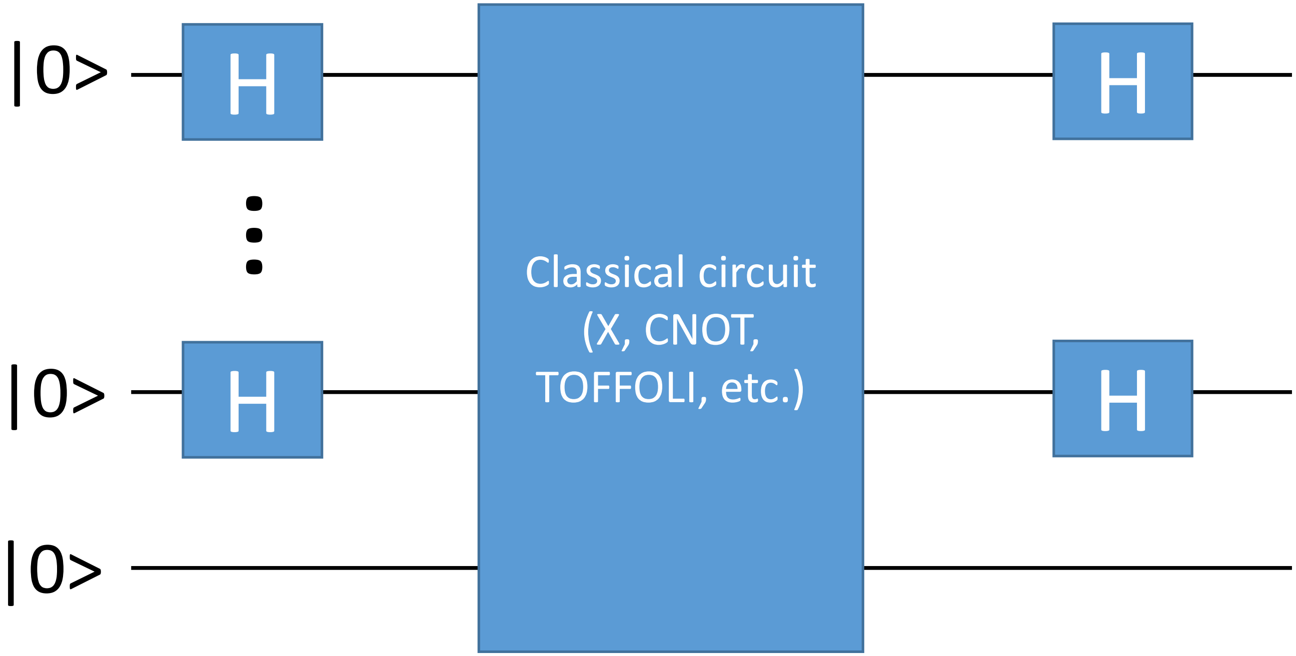
classical

Universal quantum

Fast classical algorithm for Jones polynomial could be found…

One-clean qubit model cannot be classically simulated unless PH collapses to the $2^{nd}$ level
[TM, Fujii, Fitzsimons, PRL 2012; Fujii, Kobayashi, TM, Nishimura, Tani, Tamate, PRL2018]

# HC1Q model




Second level of the Fourier hierarchy

Shor, Simon, etc..

HC1Q model cannot be classically simulated unless PH collapses to the 2nd level
[TM, Takeuchi, and Nishimura, Quantum2018]

# Weak machines exhibiting 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

Hamiltonian time-evolving system
Bermejo-Vega, Hangleiter, Schwarz, Raussendorf, Eisert, PRX 2018

Random circuits
Fefferman et al. Nature Phys. 2018

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

HC1Q model
TM, Nishimura, and Takeuchi, Quantum 2018

# Fine-grained quantum supremacy

Motivation:

All previous quantum supremacy results

Weak quantum machines cannot be classically simulated in polynomial time (unless PH collapses)

→They could be simulated in super-polynomial time…
These results do not exclude super-polynomial time classical simulations
[Remember Bravyi-Smith-Smolin-Gosset: 2^{0.48t}-time algorithm]

→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! (SETH, OV, 3SUM, APSP…)

# Exponential time hypothesis (ETH)

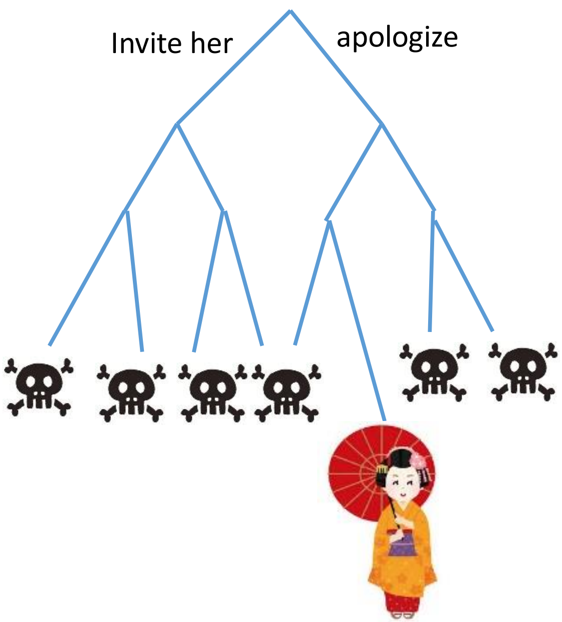
Kyoto is dangerous city…

The dean of a university in Kyoto

He held a home party every night

A neighbor said ``Nice! You look happy!”

He invited the neighbor next time. Then…




It is often said that what Kyoto people say are different from what they think…

Everytime, you have to chose your choice very carefully…

If you take a wrong path, you will die…

Find a surviving path among 2^n possibilities

P≠NP conjecture:
Cannot solve in poly(n) time

Exponential time hypothesis (ETH):
2^Ω(n)-time is necessary

Strong ETH (SETH):
Almost 2^n-time is necessary

# SETH-like conjecture

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

Our conjecture:

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

# Result

Our conjecture:

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:

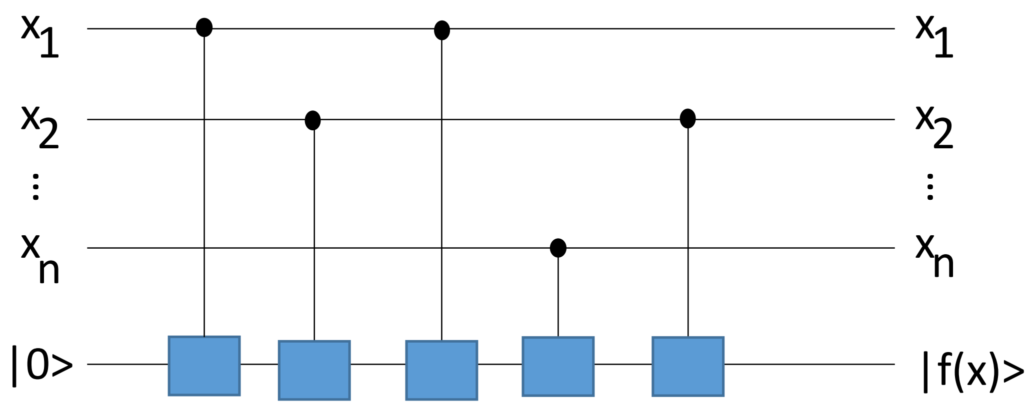
Assume that Conjecture is true. Then, for any a>0, there exists an N-qubit one-clean qubit model that cannot be classically sampled within a multiplicative error <1 in time $2^{(1-a)(N-3)}$

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

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

Proof idea:

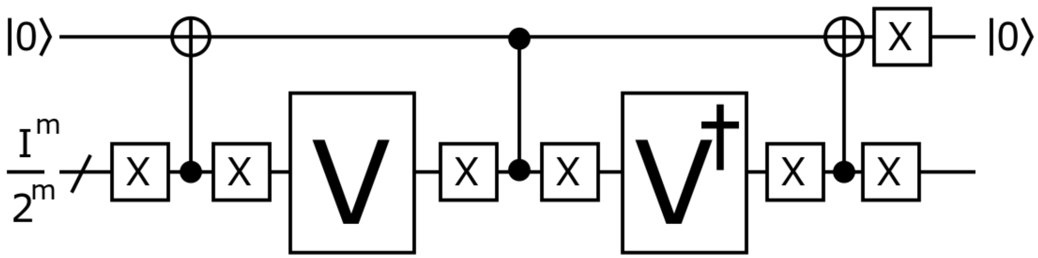
Any log-depth Boolean circuit f can be computed with single work qubit and n input qubits [Cosentino, Kothari, Paetznick, TQC 2013]




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

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

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!

# Q supremacy based on OV

Conjecture:

Given d-dim vectors, $u_1, ..., u_n, v_1, ..., v_n \in \{0,1\}^d$
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:

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

Proof idea:

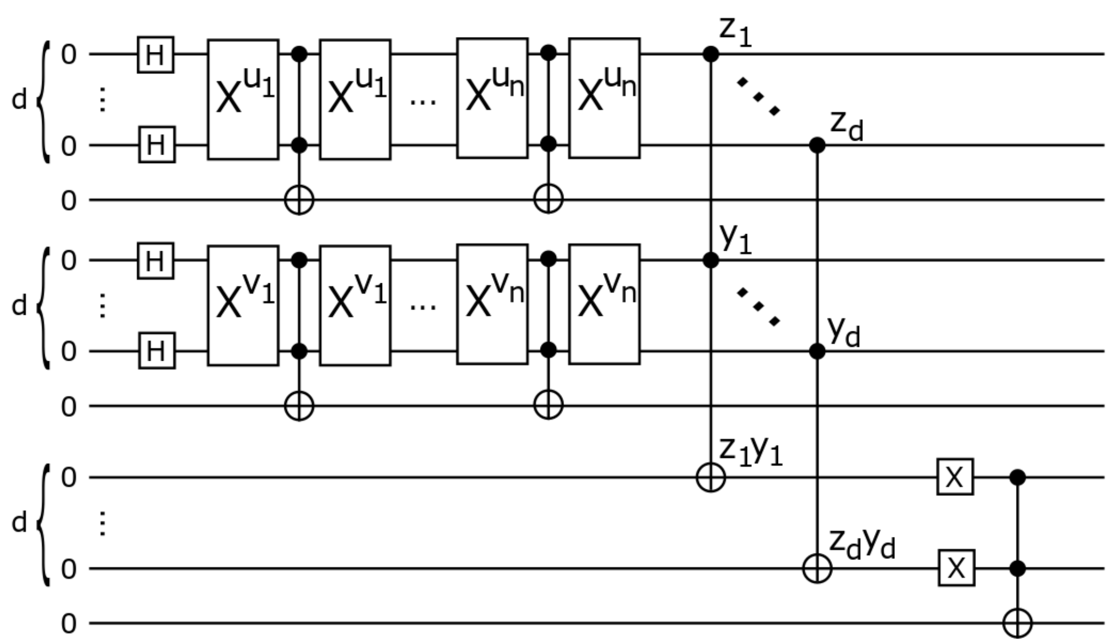
We can construct an N=3d+4 qubit quantum circuit V such that $$p_{acc} = \frac{gap^2}{2^{poly}}$$

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.

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



# 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-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:

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

Proof idea:

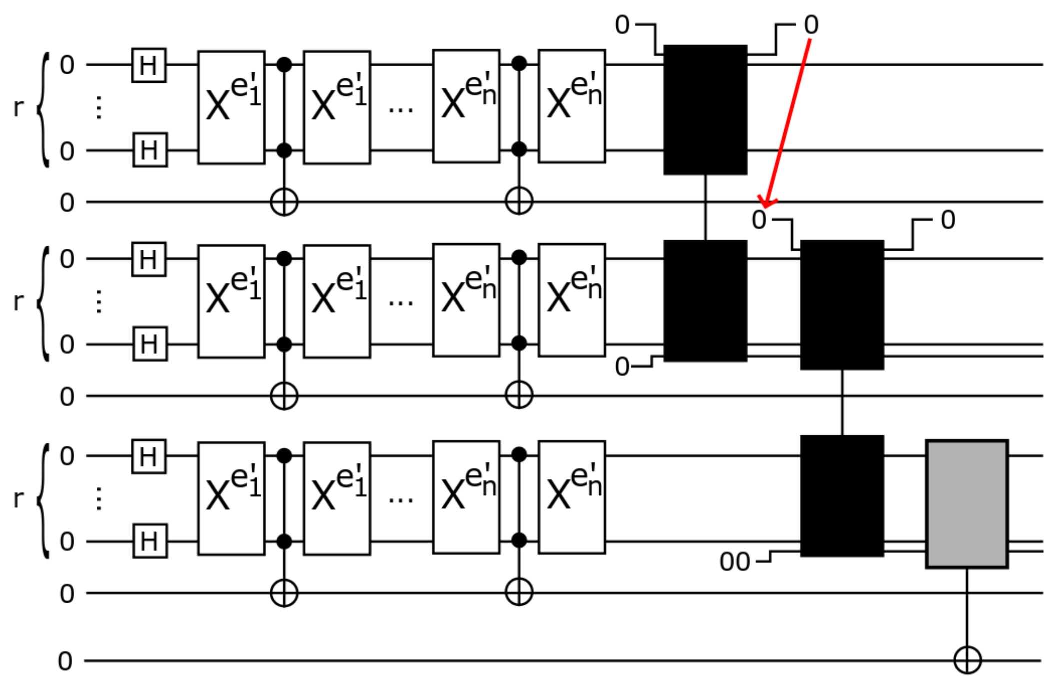
We can construct an N=3r+9 qubit quantum circuit V such that $$p_{acc} = \frac{gap^2}{2^{poly}}$$

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.

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



# T-scaling

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

My quantum machine cannot be classically simulated in 2^{an} time

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!

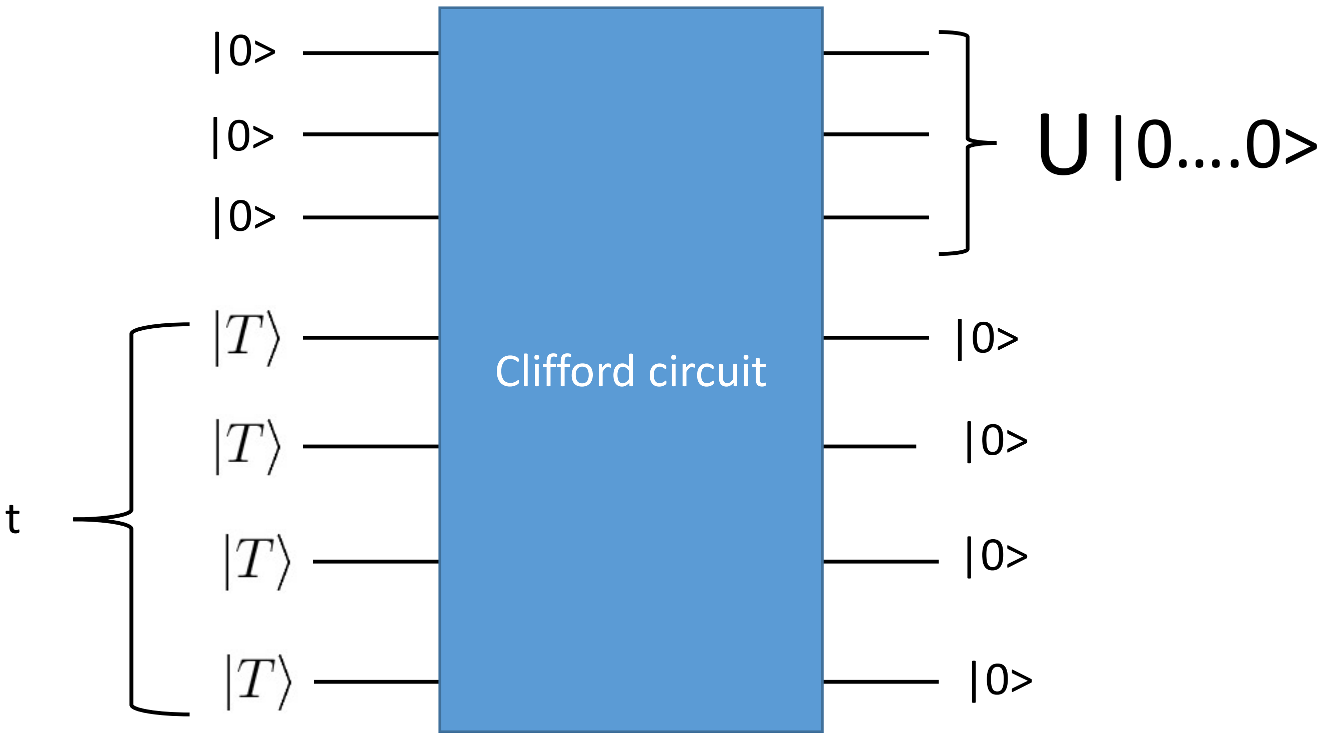
Classical calculation of Clifford and t T gates:

Trivial upperbound: 2^t time (brute force)

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

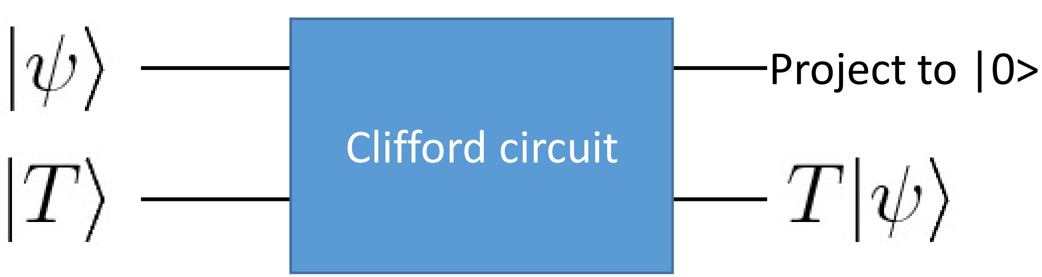
Non-trivial 2^{0.468t} time simulation [Bravyi-Smith-Smolin-Gosset].

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-Smith-Smolin-Gosset algorithm

Clifford circuit

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

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

Clifford and
t T-gates

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

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.

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 $2^{o(n)}$.

(Huang-Newman-Szegedy also showed similar result independently)

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

Proof idea:

ETH

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

$\Downarrow$ Sparcification lemma [Impagliazzo, Paturi, Zane]

ETH

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

f: 3-CNF with m clauses

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

If <0^N|U|0^N> is computed in time 2^{o(t)}=2^{o(m)}, ETH is refuted!

# Stabilizer rank conjecture

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-Gosset

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

Known best lowerbound

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

Stabilizer-rank conjecture:

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

Consider only decompositions such that c_j and phi_j are efficiently computable.

Then, the stabilizer rank conjecture is true if ETH is true.

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

# Stabilizer rank conjecture is true

Stabilizer rank: smallest k such that

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

Complex numbers

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

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

Result

The stabilizer rank conjecture is true (if non-uniform ETH is true)

c_j and phi_j are given as advice. But |c_j| is 2^{o(t)}? -> we can show it!

# H-scaling

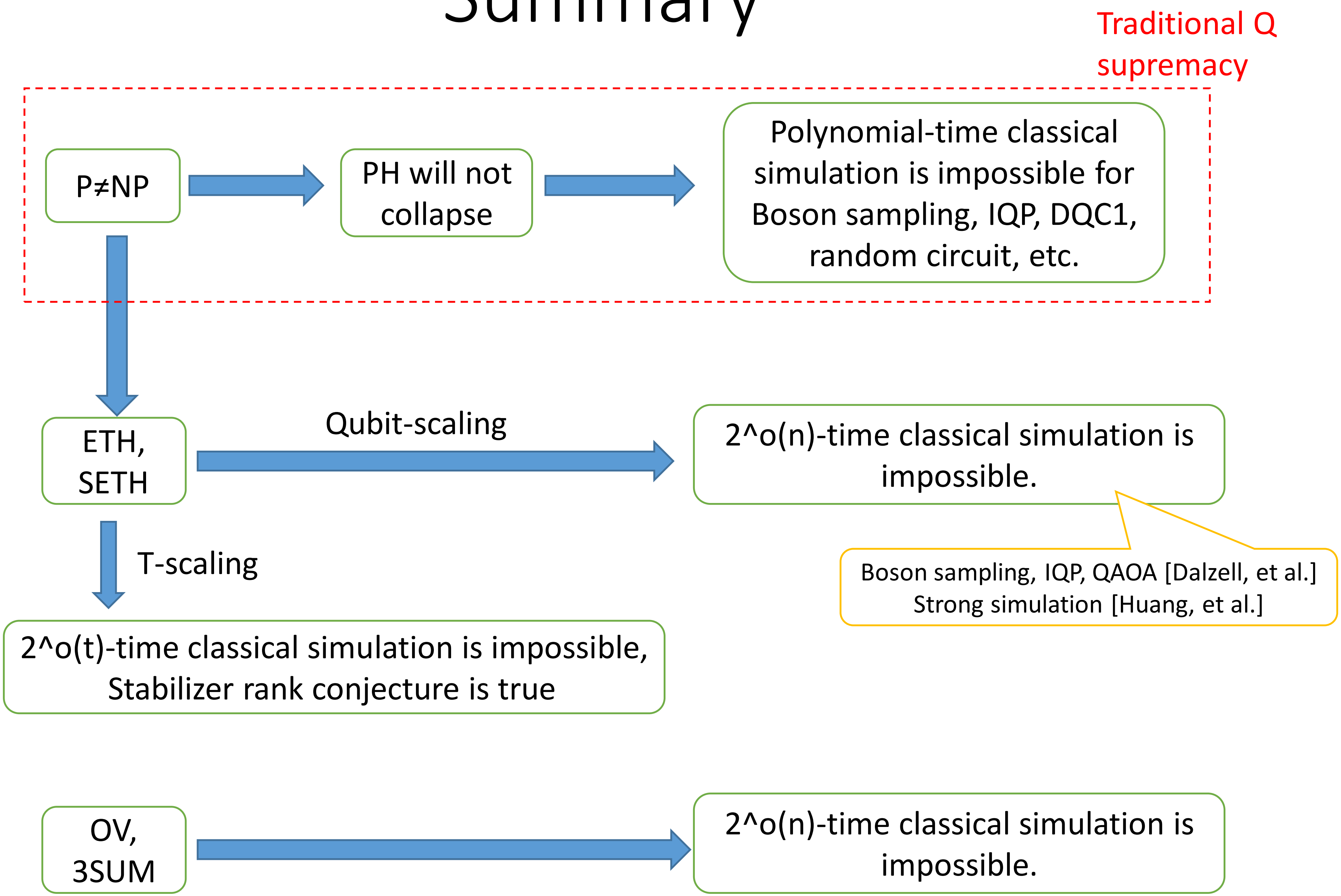
H + classical gates are universal [Aharonov, Shi]

Toffoli is classical universal → H is the ``resource” for quantum speedups

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

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 $\varepsilon < 1$

# Summary


Traditional Q supremacy
P≠NP
PH will not collapse
Polynomial-time classical simulation is impossible for Boson sampling, IQP, DQC1, random circuit, etc.
ETH, SETH
Qubit-scaling
2^o(n)-time classical simulation is impossible.
Boson sampling, IQP, QAOA [Dalzell, et al.]
Strong simulation [Huang, et al.]
T-scaling
2^o(t)-time classical simulation is impossible, Stabilizer rank conjecture is true
OV, 3SUM
2^o(n)-time classical simulation is impossible.

END