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
Outline

• Basic background 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 $\text{BQP} \neq \text{BPP}$. It is still open!

Showing $\text{BQP} \neq \text{BPP}$ will be extremely hard ($\text{BQP} \neq \text{BPP} \implies \text{P} \neq \text{PSPACE}$)
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
Query complexity

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

Let $U$ be an $n$-qubit quantum circuit

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

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

$$|p_z - q_z| \leq \varepsilon p_z$$

for all $z$

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

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

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

If a sub-universal model is classically sampled within a multiplicative error $\epsilon<1$, 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 $p_{acc}=0$

$$PH \subseteq BP \cdot coC_{=}P = BP \cdot NQP \subseteq BP \cdot NP \subseteq AM$$
Additive error sampling

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

\[ \sum_{z} |p_z - q_z| \leq \epsilon \]

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 \( 1/100 \) for at least \( 1/10 \) fraction of \( z \) is \#P-hard
- Computing \( f(z) \) within a multiplicative error \( 1/100 \) for at least \( 1/4 \) fraction of \( z \) is \#P-hard

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

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)

Bravyi-Gosset-Koenig 2018
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?
``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 $\text{poly}(n)$ time $\rightarrow$ $P \neq \text{NP}$ hypothesis

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

Almost $2^n$ time is necessary $\rightarrow$ Strong exponential time hypothesis (SETH)
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 $\text{gap}(f)\neq 0$ or $=0$ cannot be done in non-deterministic time $2^{(1-a)n}$

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

1: $k$-CNF $\rightarrow$ log-depth Boolean circuit
2: $\#f>0$ or $=0 \rightarrow \text{gap}(f)\neq 0$ or $=0$
3: deterministic time $\rightarrow$ non-deterministic time
Result

Modified SETH:

Let \( f \) be a log-depth Boolean circuit over \( n \) variables. Then for any \( a > 0 \), deciding \( \text{gap}(f) \neq 0 \) 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]

![Diagram]

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

$$\left| \langle 0^N | V | 0^N \rangle \right|^2 = \frac{\text{gap}(f)^2}{2^n}$$
With \( V \), construct the one-clean-qubit circuit

\[
\begin{array}{c}
|0\rangle \xrightarrow{X} |1\rangle \xrightarrow{V} |X\rangle \xrightarrow{V^\dagger} |0\rangle \\
\frac{I^m}{2^m} \xrightarrow{X} |X\rangle \xrightarrow{X} |X\rangle \xrightarrow{X} |X\rangle
\end{array}
\]

If gap(f) \neq 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) \neq 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) \neq 0 or =0 can be decided in non-deterministic \( 2^{(1-a)n} \) time

\( \rightarrow \) contradicts to the conjecture!
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 $d = \text{clog}(n)$. For any $\delta > 0$ there is a $c > 0$ such that deciding $\text{gap} \neq 0$ or $\text{gap} = 0$ cannot be done in non-deterministic time $n^{2-\delta}$.

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

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

OV is derived from SETH: even if SETH fails, OV can still survive
FG Q supremacy based on 3-SUM

Conjecture:

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

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

Result:

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

No relation is known between SETH and 3SUM A kind of risk hedge..
Additive-error FG supremacy

Let $f$ be an $n$-variable degree-3 polynomial over $F_2$. It is impossible to compute $\text{gap}(f)$ within a multiplicative error $1/100$ in $\text{PTIME}(2^{aN})^\text{NTIME}(m)$ 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
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. $T = \text{diag}(1, e^{i\pi/4})$

Clifford: easy
T: difficult

Near-term machines will have few T gates. $\rightarrow$ T-scaling is important!

Assuming BQP$\neq$BPP
poly($t$)

Assuming ETH
$2^{\Omega(t)}$

Bravyi-Smith-Smolin-Gosset
$2^{0.468t}$

Brute force
$2^t$

lowerbound

$?$

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

$$U |0, \ldots, 0\rangle$$

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

Magic state gadget

$|\psi\rangle$  Clifford circuit  Project to $|0\rangle$

$|T\rangle$  Clifford circuit  $T|\psi\rangle$
Classical simulation

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

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

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

\[ \chi \leq 2^{0.468t} \]

Therefore, U can be classically simulated in \(2^{0.468t}\) time. [Bravyi-Smith-Smolin-Gosset]
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)
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 \( 2^{o(m)} \).

\( f: 3\text{-CNF over } n \text{ variables. Number } m \text{ of clauses is } n^3 \)

\( 2m \text{ AND and } m-1 \text{ OR } \rightarrow 3m-1 \text{ Toffoli } \rightarrow 7(3m-1) \text{ T gates} \)

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

\( t=7(3m-1) \text{ T gates and Clifford gates} \)

\( < 0^N | U | 0^N > \text{ cannot be computable in } 2^{o(n)} = 2^{o(t^{1/3})} \text{ time} \)
Corollary: stabilizer rank conjecture is true (under ETH)

Stabilizer rank $\chi$: smallest $k$ such that

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

Complex numbers

Stabilizer state (Clifford gates on $|0...0\rangle$)

Bravyi-Smith-Smolin

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

Stabilizer-rank conjecture:

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

The stabilizer rank conjecture is true if ETH is true.

Known best (unconditional) lowerbound

$$\chi(|T\rangle \otimes t) \geq \Omega(\sqrt{t})$$
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 $\epsilon < 1$

Conjecture:

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