Additive-error fine-grained quantum supremacy

Tomoyuki Morimae\textsuperscript{1,2,}\textsuperscript{*} and Suguru Tamaki\textsuperscript{3,}\textsuperscript{†}

\textsuperscript{1}Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa Oiwakecho, Sakyoku, Kyoto 606-8502, Japan
\textsuperscript{2}JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan
\textsuperscript{3}School of Social Information Science, University of Hyogo, 8-2-1, Gakuennishi-machi, Nishi-ku, Kobe, Hyogo 651-2197, Japan

(Dated: December 16, 2019)

Abstract

It is known that several sub-universal quantum computing models, such as the IQP model, the Boson sampling model, the one-clean qubit model, and the random circuit model, cannot be classically simulated in polynomial time under certain conjectures in classical complexity theory. Recently, these results have been improved to “fine-grained” versions where even exponential-time classical simulations are excluded assuming certain classical fine-grained complexity conjectures. All these fine-grained results are, however, about the hardness of strong simulations or multiplicative-error sampling. It was open whether any fine-grained quantum supremacy result can be shown for additive-error sampling. In this paper, we show the additive-error fine-grained quantum supremacy. As examples, we consider the IQP model, a mixture of the IQP model and log-depth Boolean circuits, and Clifford+T circuits. Similar results should hold for other sub-universal models.

\textsuperscript{*}tomoyuki.morimae@yukawa.kyoto-u.ac.jp
\textsuperscript{†}tamak@sis.u-hyogo.ac.jp
I. INTRODUCTION

Classically sampling output probability distributions of sub-universal quantum computing models is known to be impossible under certain classical complexity conjectures. The depth-four model [1], the Boson Sampling model [2], the IQP model [3, 4], the one-clean qubit model [5–9], the HC1Q model [10], and the random circuit model [11–13] are known examples. These results prohibit only polynomial-time classical sampling, but recently, impossibilities of some exponential-time classical simulations have been shown based on classical fine-grained complexity conjectures [14–19].

These “fine-grained” quantum supremacy results are, however, only for exact computations (i.e., strong simulations) or multiplicative-error sampling of output probability distributions. Here, we say that a quantum probability distribution \{p_z\}_z is classically sampled in time \(T\) within a multiplicative error \(\epsilon\) if 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 \(z\). It was open whether fine-grained quantum supremacy is shown for additive-error sampling. Here, we say that a quantum probability distribution \{p_z\}_z is classically sampled in time \(T\) within an additive error \(\epsilon\) if there exists a classical \(T\)-time probabilistic algorithm that outputs \(z\) with probability \(q_z\) such that \(\sum_z |p_z - q_z| \leq \epsilon\).

In this paper, we show additive-error fine-grained quantum supremacy based on certain classical fine-grained complexity conjectures. As examples, we consider the IQP model (Sec. II), a mixture of the IQP model and log-depth Boolean circuits (Sec. III), and Clifford+\(T\) circuits (Sec. IV). Similar results should hold for other sub-universal models.

The second result (IQP plus log-depth Boolean circuit) needs more complicated quantum circuit than the first one, but the conjecture seems to be more reliable. The first and second results are about the scaling for the number of qubits, while the third result is about the scaling for the number of \(T\) gates.

Proofs are basically the same as the standard proof of the additive-error quantum supremacy [2, 4], namely, the combination of Markov inequality, Stockmeyer theorem, and the anticoncentration lemma. Markov inequality and the anticoncentration lemma can be directly used, because they are independent of the time complexity of classical simulations. Stockmeyer theorem should be, on the other hand, modified because it is for polynomial-time probabilistic computing. We extend Stockmeyer theorem to exponential-time probabilistic
II. IQP

In this section, we show additive-error fine-grained quantum supremacy of the IQP model. The IQP model is defined as follows.

**Definition 1** An $N$-qubit IQP model is the following quantum computing model:

1. The initial state is $|0^N\rangle$. (Here, $|0^N\rangle = |0\rangle^\otimes N$.)
2. $H^\otimes N$ is applied, where $H$ is the Hadamard gate.
3. Z-diagonal gates (such as $e^{i\theta Z}$, $Z$, $CZ$, and $CCZ$) are applied. (In this paper, we consider only $Z$, $CZ$, and $CCZ$.)
4. $H^\otimes N$ is applied.
5. All qubits are measured in the computational basis.

Let us consider an $n$-variable degree-3 polynomial, $f : \{0, 1\}^n \rightarrow \{0, 1\}$, over $\mathbb{F}_2$ defined by

$$f(x_1, ..., x_n) \equiv \sum_{i=1}^{n} \alpha_i x_i + \sum_{i>j} \beta_{i,j} x_i x_j + \sum_{i>j>k} \gamma_{i,j,k} x_i x_j x_k$$

for any $x \equiv (x_1, x_2, ..., x_n) \in \{0, 1\}^n$, where $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \{0, 1\}$. If we say that we randomly choose $f$, it means that we randomly choose each $\alpha_i, \beta_{i,j}, \gamma_{i,j,k}$ uniformly and independently.

The conjecture on which additive-error fine-grained quantum supremacy of the IQP model is based is stated as follows.

**Conjecture 1** Let $f$ be an $n$-variable degree-3 polynomial over $\mathbb{F}_2$. Let us define $\text{gap}(f) \equiv \sum_{x \in \{0,1\}^n} (-1)^{f(x)}$. There exist positive constants $a$ and $n_0$ such that for every $n > n_0$ the following holds. Computing $[\text{gap}(f)]^2$ within a multiplicative error $\frac{26}{100}$ for at least $\frac{1}{24}$ fraction of $f$ cannot be done with a classical probabilistic $O(2^a n)$-time algorithm that makes queries of length $O(2^a n)$ to an NTIME[$n^2$] oracle with a success probability at least $\frac{31}{32}$. 

3
Note that the parameters $\frac{26}{100}$, $\frac{1}{24}$, $\frac{31}{32}$ can be adjustable to some extent. (See the proof.) We do not know whether this conjecture is true or false, but at least at this moment we do not know how to refute it.

Based on Conjecture \( \Pi \) we show the following result.

**Theorem 1** If Conjecture \( \Pi \) is true, then there exists an \( N \)-qubit IQP circuit whose output probability distribution cannot be classically sampled in \( O(2^{\frac{2}{3}N}) \)-time within an additive error \( \epsilon \leq \frac{1}{192} \).

For simplicity, we consider degree-3 polynomials, but it is clear from the following proof that a similar result holds for degree-\( k \) polynomials for any constant \( k \geq 3 \). (The anticoncentration lemma holds for any degree-\( k \) polynomial with \( k \geq 2 \), but the degree-2 case is classically simulatable because it is a Clifford circuit, so \( k \geq 3 \) is necessary.) If we consider Conjecture \( \Pi \) for degree-\( k \) polynomials, it becomes more stable for larger \( k \) \[20\].

**Proof of Theorem \( \Pi \)** Given an \( n \)-variable degree-3 polynomial \( f \), we can construct an \( n \)-qubit IQP circuit such that the probability \( p_z(f) \) of outputting \( z \in \{0, 1\}^n \) satisfies

\[
p_z(f) = \frac{(\text{gap}(f_z))^2}{2^n},
\]

where

\[
f_z(x_1, \ldots, x_n) \equiv f(x_1, \ldots, x_n) + \sum_{i=1}^{n} z_ix_i.
\]

Assume that there exists a \( T \)-time classical probabilistic algorithm that outputs \( z \in \{0, 1\}^n \) with probability \( q_z(f) \) such that

\[
\sum_{z \in \{0,1\}^n} |p_z(f) - q_z(f)| \leq \epsilon
\]

for a certain \( \epsilon \) and any \( f \). From Markov inequality,

\[
\Pr_z \left[ \left| p_z(f) - q_z(f) \right| \geq \frac{\epsilon}{2^n} \right] \leq \delta
\]

for any \( f \) and \( \delta > 0 \). According to the exponential-time Stockmeyer theorem (see Appendix), a classical \( O(T^2) \)-time probabilistic algorithm that makes queries of \( O(T) \) length to the \( \text{NTIME}[n^2] \) oracle can compute \( \tilde{q}_z(f) \) such that

\[
|q_z(f) - \tilde{q}_z(f)| \leq \xi q_z(f),
\]

for 4
where
\[ \xi \equiv \frac{2^{\frac{1}{\alpha}} - 2^{-\frac{1}{\alpha}}}{2}, \]
for any \( f, \alpha \geq 1 \), and \( z \in \{0, 1\}^n \), with a success probability at least \( \frac{31}{32} \). Due to the anti-concentration lemma [4],
\[ \Pr_{z,f} \left[ p_z(f) \geq \frac{\tau}{2^n} \right] \geq \frac{(1 - \tau)^2}{3} \]
for any \( 0 < \tau < 1 \).

Therefore we have
\[
\begin{align*}
|p_z(f) - \tilde{q}_z(f)| &\leq |p_z(f) - q_z(f)| + |q_z(f) - \tilde{q}_z(f)| \\
&\leq |p_z(f) - q_z(f)| + \xi q_z(f) \quad \text{(with a success probability at least \( \frac{31}{32} \) for each \( f \) and \( z \))} \\
&\leq |p_z(f) - q_z(f)| + \xi (p_z(f) + |p_z(f) - q_z(f)|) \\
&= \xi p_z(f) + |p_z(f) - q_z(f)| (1 + \xi) \\
&\leq \xi p_z(f) + \frac{\epsilon}{2^n \delta} (1 + \xi) \quad \text{(for at least \( 1 - \delta \) fraction of \( z \))} \\
&\leq \xi p_z(f) + \frac{p_z(f)}{4} (1 + \xi) \quad \text{(for at least \( \frac{(1 - \frac{\epsilon}{3})^2}{3} \) fraction of \( (z, f) \))} \\
&= p_z(f) \left( \frac{1}{4} + \frac{5 \xi}{4} \right) \\
&\leq p_z(f) \left( \frac{1}{4} + \frac{1}{100} \right) \quad \text{(We take \( \xi \leq \frac{1}{125} \)).}
\end{align*}
\]
If we take \( \epsilon = \frac{1}{192} \) and \( \delta = 8 \epsilon \), the above inequality is correct for at least \( \frac{1}{24} \) fraction of \( (z, f) \). Hence, we obtain
\[
|(\text{gap}(f_z))^2 - 2^{2n} \tilde{q}_z(f)| \leq \frac{26}{100} (\text{gap}(f_z))^2
\]
for at least \( \frac{1}{24} \) fraction of \( (z, f) \). It means \( (\text{gap}(f))^2 \) is computable within the multiplicative error \( \frac{26}{100} \) for at least \( \frac{1}{24} \) fraction of \( f \), which contradict Conjecture [4].

III. IQP PLUS LOG-DEPTH BOOLEAN CIRCUIT

In this section, we show additive-error fine-grained quantum supremacy for the IQP plus log-depth Boolean circuit model.

Let us consider the following conjecture.
Conjecture 2 Let \( f : \{0,1\}^n \rightarrow \{0,1\} \) be an \( n \)-variable degree-2 polynomial over \( \mathbb{F}_2 \), and \( g : \{0,1\}^n \rightarrow \{0,1\} \) be an \( n \)-variable log-depth Boolean circuit. Define
\[
gap(f + g) \equiv \sum_{x \in \{0,1\}^n} (-1)^{f(x)+g(x)}.
\]
There exist positive constants \( a \) and \( n_0 \) such that for every \( n > n_0 \) the following holds. Computing \( [\gap(f + g)]^2 \) within a multiplicative error \( \frac{26}{100} \) for at least \( \frac{1}{24} \) fraction of \( f \) cannot be done with a classical probabilistic \( O(2^n) \)-time algorithm that makes queries of length \( O(2^{\frac{n}{2}}) \) to an \( \text{NTIME}[n^2] \) oracle with a success probability at least \( \frac{31}{32} \).

Conjecture 2 is “more stable” than Conjecture 1 because log-depth Boolean circuit is more general than constant-degree polynomials. For constant-degree polynomials, there is a non-trivial exponential time algorithm to count the number of solutions \( \text{[22]} \), but we do not know how to apply it to log-depth Boolean circuits. Furthermore, note that in Conjecture 2 the average case is considered only for \( f \), and \( g \) can be taken as the worst case one.

Based on Conjecture 2 we show the following result.

Theorem 2 If Conjecture 2 is true, then there exists an \( N \)-qubit \( \text{poly}(N) \)-size quantum circuit (consisting of an IQP circuit and a log-depth Boolean circuit) whose output probability distribution cannot be classically sampled in \( O(2^{\frac{3}{4}N}) \)-time within an additive error \( \epsilon \leq \frac{1}{192} \).

Proof of Theorem 2 Given a log-depth Boolean circuit \( g : \{0,1\}^n \rightarrow \{0,1\} \), we can construct an \( (n + 1) \)-qubit \( \text{poly}(n) \)-size quantum circuit \( U \) such that
\[
U(|x \rangle \otimes |0 \rangle) = e^{ih(x)}|x \rangle \otimes |g(x) \rangle
\]
for any \( x \in \{0,1\}^n \), where \( h \) is a certain function whose detail is irrelevant here \( \text{[23]} \). Let us consider the following circuit.

1. The initial state is \( |0^n \rangle \otimes |0 \rangle \).
2. Apply \( H^\otimes n \otimes I \) to obtain
\[
\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x \rangle \otimes |0 \rangle.
\]
3. Apply \( U \) to obtain
\[
\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} e^{ih(x)}|x \rangle \otimes |g(x) \rangle.
\]
4. Apply $Z$ on the last qubit to obtain
\[ \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} e^{ih(x)} (-1)^{g(x)} |x\rangle \otimes |g(x)\rangle. \]

5. Apply $U^\dagger$ to obtain
\[ \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{g(x)} |x\rangle \otimes |0\rangle. \]

6. Apply $Z$ and $CZ$ that correspond to $f$ to obtain
\[ \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{g(x)+f(x)} |x\rangle \otimes |0\rangle. \]

7. Apply $H^{\otimes n} \otimes I$ and measure the first $n$ qubits in the computational basis.

The probability of obtaining $z \in \{0,1\}^n$ is
\[ p_z(f + g) = \left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{g(x)+f(x)+\sum_{j=1}^{n} x_j z_j} \right|^2 \]
\[ = \frac{(\text{gap}(g + f_z))^2}{2^{2n}}. \]

Assume that there exists a $T$-time classical probabilistic algorithm that outputs $z \in \{0,1\}^n$ with probability $q_z(f + g)$ such that
\[ \sum_{z \in \{0,1\}^n} |p_z(f + g) - q_z(f + g)| \leq \epsilon. \]

From Markov inequality,
\[ \Pr_z \left[ |p_z(f + g) - q_z(f + g)| \geq \frac{\epsilon}{2^n \delta} \right] \leq \delta \]
for any $f$, $g$, and $\delta > 0$. According to the exponential-time Stockmeyer theorem, a classical $O(T^2)$-time probabilistic algorithm that makes queries of length $O(T)$ to the $\text{NTIME}[n^2]$ oracle can compute $\tilde{q}_z(f + g)$ such that
\[ |q_z(f + g) - \tilde{q}_z(f + g)| \leq \xi q_z(f + g), \]
where
\[ \xi = \frac{2^{\frac{1}{\alpha}} - 2^{-\frac{1}{\alpha}}}{2}. \]
for any $f, g, \alpha \geq 1$, and $z \in \{0,1\}^n$, with a success probability at least $\frac{31}{32}$. Due to the anticoncentration lemma [4]

\[
\Pr_{z,f}\left[ p_z(f + g) \geq \frac{\tau}{2^n} \right] \geq \frac{(1 - \tau)^2}{3}
\]

for any $0 < \tau < 1$.

Then we have

\[
|p_z(f + g) - q_z(f + g)| \leq |p_z(f + g) - q_z(f + g)| + |q_z(f + g) - q_z(f + g)|
\]

\[
\leq |p_z(f + g) - q_z(f + g)| + \xi q_z(f + g)
\]

\[
\leq |p_z(f + g) - q_z(f + g)| + \xi (p_z(f + g) + |p_z(f + g) - q_z(f + g)|)
\]

\[
= \xi p_z(f + g) + |p_z(f + g) - q_z(f + g)|(1 + \xi)
\]

\[
\leq \xi p_z(f + g) + \frac{\epsilon}{2^n}\delta (1 + \xi) \quad \text{(for at least } 1 - \delta \text{ fraction of } z)
\]

\[
\leq \xi p_z(f + g) + \frac{\epsilon}{4}\left(1 + \frac{\xi}{4}\right) \quad \text{(for at least } \frac{(1 - \delta^2)^2}{3} \text{ fraction of } (z, f))
\]

\[
= p_z(f + g) \left(\frac{1}{4} + \frac{5\xi}{4}\right)
\]

\[
\leq p_z(f + g) \left(\frac{1}{4} + \frac{1}{100}\right) \quad \text{(We take } \xi \leq \frac{1}{125})
\]

If we take $\epsilon = \frac{1}{192}$ and $\delta = 8\epsilon$, the above inequality is correct for at least $\frac{1}{24}$ fraction of $(z, f)$, which contradict Conjecture 2.

IV. CLIFFORD PLUS $T$

In this section, we finally show additive-error fine-grained quantum supremacy for Clifford+$T$ circuits. Let us consider the following conjecture.

**Conjecture 3** Let $g : \{0,1\}^n \to \{0,1\}$ be a 3-CNF with $m$ clauses, and $f : \{0,1\}^n \to \{0,1\}$ be an $n$-variable degree-2 polynomial over $\mathbb{F}_2$. Define

\[
gap(f + g) \equiv \sum_{x \in \{0,1\}^n} (-1)^{f(x) + g(x)}.
\]

There exist positive constants $a$ and $n_0$ such that for every $n > n_0$ the following holds. Computing $[\gap(f + g)]^2$ within a multiplicative error $\frac{26}{100}$ for at least $\frac{1}{24}$ fraction of $f$ cannot be done with a classical probabilistic $O(2^{an})$-time algorithm that makes queries of length $O(2^{an})$ to an NTIME[$n^2$] oracle with a success probability at least $\frac{31}{32}$.
Based on Conjecture 3, we show the following result.

**Theorem 3** If Conjecture 3 is true, then there exists a quantum circuit over Clifford gates and $t$ $T$ gates whose output probability distribution cannot be classically sampled in $O(2^{\frac{2(n+14)}{84}})$-time within an additive error $\epsilon \leq \frac{1}{192}$.

*Proof of Theorem 3.* Given a 3-CNF $g : \{0, 1\}^n \rightarrow \{0, 1\}$, we can construct a quantum circuit $U$ such that

$U(|x\rangle \otimes |0^\xi\rangle) = |g(x)\rangle \otimes |junk(x)\rangle$

for any $x \in \{0, 1\}^n$, where $\xi \equiv 3m - 1$, and $junk(x) \in \{0, 1\}^{n+\xi-1}$ is a certain bit string whose detail is irrelevant here. Note that $U$ consists of Clifford and $7(3m - 1)$ number of $T$ gates. (The 3-CNF $g$ contains $2m$ OR gates and $m - 1$ AND gates. Each AND and OR gate can be simulated with a single TOFFOLI gate by using a single ancilla qubit. A single TOFFOLI gate can be simulated with Clifford and 7 $T$ gates.) Let us consider the following circuit.

1. The initial state is $|0^n\rangle \otimes |0^\xi\rangle$.

2. Apply $H^{\otimes n} \otimes I^{\otimes \xi}$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \otimes |0^\xi\rangle.$$ 

3. Apply $U$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |g(x)\rangle \otimes |junk(x)\rangle.$$ 

4. Apply $Z \otimes I^{\otimes n+\xi-1}$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{g(x)} |g(x)\rangle \otimes |junk(x)\rangle.$$ 

5. Apply $U^\dagger$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{g(x)} |x\rangle \otimes |0^\xi\rangle.$$
6. Apply $Z$ and $CZ$ that correspond to $f$ to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{g(x)+f(x)} |x\rangle \otimes |0^\xi\rangle.$$ 

7. Apply $H^\otimes n \otimes I^\otimes \xi$ and measure all qubits in the first register in the computational basis.

This quantum computing uses $t \equiv 14(3m - 1)$ number of $T$ gates. The probability of obtaining $z \in \{0,1\}^n$ is

$$p_z(f + g) = \left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+\sum_{j=1}^n x_jz_j+g(x)} \right|^2.$$ 

Assume that there exists a $T$-time classical probabilistic algorithm that outputs $z \in \{0,1\}^n$ with probability $q_z(f + g)$ such that

$$\sum_{z \in \{0,1\}^n} |p_z(f + g) - q_z(f + g)| \leq \epsilon.$$ 

From Markov inequality,

$$\Pr_{z,f} \left[ |p_z(f + g) - q_z(f + g)| \geq \frac{\epsilon}{2n^2} \right] \leq \delta$$

for any $f$, $g$, and $\delta > 0$. According to the exponential-time Stockmeyer theorem, a classical $O(T^2)$-time probabilistic algorithm that makes queries of length $O(T)$ to the NTIME[$n^2$] oracle can compute $\tilde{q}_z(f + g)$ such that

$$|q_z(f + g) - \tilde{q}_z(f + g)| \leq \xi q_z(f + g),$$

where

$$\xi \equiv \frac{2^{\frac{1}{\alpha}} - 2^{-\frac{1}{\alpha}}}{2},$$

for any $f$, $g$, $\alpha \geq 1$, and $z \in \{0,1\}^n$, with a success probability at least $\frac{31}{32}$. Due to the anticoncentration lemma \[4\]

$$\Pr_{z,f} \left[ |p_z(f + g) \geq \frac{\tau}{2^n} \right] \geq \frac{(1 - \tau)^2}{3}$$

for any $0 < \tau < 1$. 

10
Then we have
\[ |p_z(f + g) - \tilde{q}_z(f + g)| \leq |p_z(f + g) - q_z(f + g)| + |q_z(f + g) - \tilde{q}_z(f + g)| \]
\[ \leq |p_z(f + g) - q_z(f + g)| + \xi_q(f + g) \]
\[ \leq |p_z(f + g) - q_z(f + g)| + \xi(p_z(f + g) + |p_z(f + g) - q_z(f + g)|) \]
\[ = \xi p_z(f + g) + |p_z(f + g) - q_z(f + g)|(1 + \xi) \]
\[ \leq \xi p_z(f + g) + \frac{\epsilon}{2^n \delta}(1 + \xi) \quad \text{(for at least } 1 - \delta \text{ fraction of } z) \]
\[ \leq \xi p_z(f + g) + \frac{p_z(f + g)}{4}(1 + \xi) \quad \text{(for at least } (1 - \frac{4\epsilon}{3})^2 \text{ fraction of } (z, f)) \]
\[ = p_z(f + g)\left(\frac{1}{4} + \frac{5\xi}{4}\right) \]
\[ \leq p_z(f + g)\left(\frac{1}{4} + \frac{1}{100}\right) \quad \text{(We take } \xi \leq \frac{1}{125}). \]

If we take \( \epsilon = \frac{1}{192} \) and \( \delta = 8\epsilon \), the above inequality is correct for at least \( \frac{1}{24} \) fraction of \((z, f)\), which contradict Conjecture 3.

\[ \square \]

**ACKNOWLEDGMENTS**

TM thanks Yoshifumi Nakata for discussion. TM is supported by MEXT Q-LEAP, JST PRESTO No.JPMJPR176A, and the Grant-in-Aid for Young Scientists (B) No.JP17K12637 of JSPS. ST is supported by JSPS KAKENHI Grant Numbers 16H02782, 18H04090, and 18K11164.

**Appendix**

In this Appendix, we provide a proof of the exponential-time Stockmeyer theorem. The proof is a straightforward generalization of the one given in Ref. [21].

1. **A pairwise independent hash family and the leftover hash lemma**

To show the exponential-time Stockmeyer, we need the following two lemmas. Their proofs can be found in standard text books of complexity theory, such as Ref. [24].

**Lemma 1 (A pairwise independent hash family)** Let \( A \) be a random \( n \times m \) binary Toeplitz matrix, and \( b \) be a random \( m \)-dimensional binary vector. (Here, a Toeplitz matrix
is a matrix whose matrix elements satisfy $a_{i,j} = a_{i+1,j+1}$.) Then, the family $H \equiv \{ h_{A,b} \}_{A,b}$ of functions, $h_{A,b} : \{0,1\}^n \to \{0,1\}^m$, with $h_{A,b}(x) \equiv Ax + b$ satisfies

$$\Pr_{A,b}[h_{A,b}(x_1) = y_1 \land h_{A,b}(x_2) = y_2] = \frac{1}{2^{2m}}$$

for any $x_1 \neq x_2 \in \{0,1\}^n$ and $y_1, y_2 \in \{0,1\}^m$.

**Lemma 2 (The leftover hash lemma)** Let $S \subseteq \{0,1\}^n$ be a set of $n$-bit strings. Then

$$\Pr_{A,b}\left[\left|\{x \in S : h_{A,b}(x) = 0^m\}\right| - \frac{|S|}{2^m} \geq \epsilon \frac{|S|}{2^m}\right] \leq 2^{m-1} \epsilon^2 |S|.$$

2. **Algorithm $A_k$**

In this subsection, we define the algorithm $A_k$, which is used for the exponential-time Stockmeyer. Let $G$ be an $n$-time deterministic classical algorithm. Let $S \equiv \{ x \in \{0,1\}^n : G(x) = 1 \}$. Let $k$ be an integer such that $1 \leq k \leq n$. We construct a classical probabilistic $O(n)$-time algorithm $A_k$ that gets a description of $G$ as the input, and that makes queries of length $O(n)$ to the NTIME[$n^2$] oracle such that

- If $|S| \geq 2^{k+1}$ then $\Pr[A_k \text{ accepts}] \geq \frac{3}{4}$.
- If $|S| < 2^k$ then $\Pr[A_k \text{ accepts}] \leq \frac{1}{8}$.

The algorithm $A_k$ runs as follows.

1. If $k \leq 5$, query the NTIME[$n$] oracle whether $|S| \geq 2^{k+1}$ or not. (The query to the oracle is the description of $G$. Given the description of $G$, deciding $|S| \geq 2^{k+1}$ or not is in NTIME[$n$].) Accept if the oracle answer is yes. If the oracle answer is no, reject.

2. If $k \geq 6$, set $m \equiv k - 5$. Randomly choose an $n \times m$ binary Toeplitz matrix $A$, and an $m$-dimensional binary vector $b$. It takes $n + 2m - 1 = O(n)$ time. Define the function $h_{A,b} : \{0,1\}^n \to \{0,1\}^m$ by $h_{A,b}(x) \equiv Ax + b$. Query the NTIME[$n^2$] oracle whether $\{|x \in S : h_{A,b}(x) = 0^m\}| \geq 48$ or not. (The query to the oracle is the description of $G$, $A$, and $b$. Given the description of $G$, $A$, and $b$, deciding $\{|x \in S : h_{A,b}(x) = 0^m\}| \geq 48$ or not is in NTIME[$n^2$].) If the oracle answer is yes, accept. If the oracle answer is no, reject.
Assume that $k \leq 5$. Then, if $|S| \geq 2^{k+1}$, the probability that $A_k$ accepts is 1. If $|S| < 2^k$, the probability that $A_k$ accepts is 0.

Assume that $k \geq 6$. If $|S| \geq 2^{k+1}$, then $|S| \geq 2^{m+6}$ and therefore

$$\Pr[A_k \text{ rejects}] = \Pr_{A,b}\left[|\{x \in S : h_{A,b}(x) = 0^m\}| < 48\right]$$

$$\leq \Pr_{A,b}\left[|\{x \in S : h_{A,b}(x) = 0^m\}| \leq \frac{3|S|}{4^2m}\right]$$

$$= \Pr_{A,b}\left[-|\{x \in S : h_{A,b}(x) = 0^m\}| + \frac{|S|}{2^m} \geq \frac{1}{4^2m}\right]$$

$$\leq \Pr_{A,b}\left[|\{x \in S : h_{A,b}(x) = 0^m\}| - \frac{|S|}{2^m} \geq \frac{1}{4^2m}\right]$$

$$\leq \frac{2^{m+4}}{|S|} \leq \frac{1}{4}.$$  

If $|S| < 2^k$, define a superset $S' \supseteq S$ with $|S'| = 2^k$. Then,

$$\Pr[A_k \text{ accepts}] = \Pr_{A,b}\left[\{|x \in S : h_{A,b}(x) = 0^m\}| \geq 48\right]$$

$$\leq \Pr_{A,b}\left[\{|x \in S' : h_{A,b}(x) = 0^m\}| \geq 48\right]$$

$$= \Pr_{A,b}\left[\{|x \in S' : h_{A,b}(x) = 0^m\}| \geq \frac{3|S'|}{2^m}\right]$$

$$= \Pr_{A,b}\left[\{|x \in S' : h_{A,b}(x) = 0^m\}| \geq \frac{|S'|}{2^m} + \frac{1}{2} \frac{|S'|}{2^m}\right]$$

$$= \Pr_{A,b}\left[\{|x \in S' : h_{A,b}(x) = 0^m\}| - \frac{|S'|}{2^m} \geq \frac{1}{2} \frac{|S'|}{2^m}\right]$$

$$\leq \Pr_{A,b}\left[\{|x \in S' : h_{A,b}(x) = 0^m\}| - \frac{|S'|}{2^m} \geq \frac{1}{2} \frac{|S'|}{2^m}\right]$$

$$\leq \frac{2^{m+2}}{|S'|} = \frac{1}{8}.$$  

### 3. Exponential-time Stockmeyer theorem

**Theorem 4** For any classical probabilistic $T$-time algorithm that outputs $z \in \{0, 1\}^N$ with probability $q_z$, and any constant integer $\alpha \geq 1$, there exists a $O(T^2)$-time classical probabilistic algorithm that makes queries of length $O(T)$ to the NTIME[$n^2$] oracle that outputs $\tilde{q}_z$ such that

$$|q_z - \tilde{q}_z| \leq \frac{2^\frac{1}{\alpha} - 2^{-\frac{1}{\alpha}}}{2} q_z$$

with a success probability at least $\frac{2^\frac{1}{2}}{2^\frac{1}{2}}$ for any $z \in \{0, 1\}^N$.  

13
Proof of Theorem 4. Let $\mathcal{C}$ be a $T$-time deterministic classical algorithm such that
\[
\frac{\left| \{ r \in \{0, 1\}^T : \mathcal{C}(r) = z \} \right|}{2^T} = q_z
\]
for all $z \in \{0, 1\}^N$. For each $z \in \{0, 1\}^N$, let us define the set $S_z \subseteq \{0, 1\}^T$ by
\[
S_z \equiv \{ r \in \{0, 1\}^T : \mathcal{C}(r) = z \}.
\]
For any integer $\alpha \geq 1$, define
\[
S_{z}^{\times \alpha} \equiv \{ (r_1, \ldots, r_\alpha) \in (\{0, 1\}^T)^{\times \alpha} : \mathcal{C}(r_1) = \ldots = \mathcal{C}(r_\alpha) = z \}.
\]
For $S_{z}^{\times \alpha}$, run $\mathcal{A}_k$ for $k = 1, 2, \ldots, \alpha T$. It takes classical probabilistic $O(T^2)$-time that makes queries of length $O(T)$ to the NTIME[$n^2$] oracle. Assume that $\mathcal{A}_k$ accepts for $k = 1, 2, \ldots, \eta - 1$, and rejects for $k = \eta$ with a certain integer $\eta$. This means $2^{\eta - 1} < |S_{z}^{\times \alpha}| < 2^{\eta + 1}$ with a failure probability at most $1/32$. If we define $\sigma \equiv 2^\eta$, $\frac{1}{2} \sigma^\alpha < |S_z|^{\alpha} < 2 \sigma^\alpha$. Hence
\[
\left( \frac{1}{2} \right)^{\frac{1}{\alpha}} \sigma < |S_z| < 2^{\frac{1}{\alpha}} \sigma.
\]
If we define $\tilde{q}_z \equiv \sigma/2^T$, we obtain the result. □

[1] B. M. Terhal and D. P. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. Quant. Inf. Comput. 4, 134 (2004).

[2] S. Aaronson and A. Arkhipov, The computational complexity of linear optics. Theory of Computing 9, 143 (2013).

[3] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. R. Soc. A 467, 459 (2011).

[4] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations. Phys. Rev. Lett. 117, 080501 (2016).

[5] E. Knill and R. Laflamme, Power of one bit of quantum information. Phys. Rev. Lett. 81, 5672 (1998).

[6] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of classically simulating the one clean qubit model. Phys. Rev. Lett. 112, 130502 (2014).

[7] T. Morimae, Hardness of classically sampling one clean qubit model with constant total variation distance error. Phys. Rev. A 96, 040302(R) (2017).

[8] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Impossibility of classically simulating one-clean-qubit model with multiplicative error. Phys. Rev. Lett. 120, 200502 (2018).
[9] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits. Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016), pp.13:1-13:14 (2016).

[10] T. Morimae, Y. Takeuchi, and H. Nishimura, Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy. Quantum 2, 106 (2018).

[11] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling. Nature Phys. 15, 159 (2019).

[12] R. Movassagh, Efficient unitary paths and quantum computational supremacy: A proof of average-case hardness of Random Circuit Sampling. arXiv:1810.04681

[13] R. Movassagh, Cayley path and quantum computational supremacy: A proof of average-case \#P-hardness of Random Circuit Sampling with quantified robustness. arXiv:1909.06210

[14] A. M. Dalzell, A. W. Harrow, D. E. Koh, and R. L. La Placa, How many qubits are needed for quantum computational supremacy? arXiv:1805.05224

[15] A. M. Dalzell, Bachelor thesis, MIT (2017). https://dspace.mit.edu/handle/1721.1/111859

[16] C. Huang, M. Newman, and M. Szegedy, Explicit lower bounds on strong quantum simulation. arXiv:1804.10368

[17] C. Huang, M. Newman, and M. Szegedy, Explicit lower bounds on strong simulation of quantum circuits in terms of T-gate count. arXiv:1902.04764

[18] T. Morimae and S. Tamaki, Fine-grained quantum computational supremacy. Quant. Inf. Comput. 19, 1089 (2019).

[19] R. Hayakawa, T. Morimae, and S. Tamaki, Fine-grained quantum supremacy based on Orthogonal Vectors, 3-SUM and All-Pairs Shortest Paths. arXiv:1902.08382

[20] R. Williams, Counting solutions to polynomial systems via reductions. Proceedings of the 1st Symposium on Simplicity in Algorithms (SOSA 2018).

[21] L. Trevisan, Lecture notes on computational complexity.

[22] D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, and H. Yu, Beating brute force for systems of polynomial equations over finite fields. Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms, pp.2190-2202 (2017).

[23] A. Cosentino, R. Kothari, and A. Paetznick, Dequantizing read-once quantum formulas. arXiv:1304.5164

[24] O. Goldreich, Computational Complexity: a conceptual perspective. Cambridge University
Press (2008).