Fine-grained quantum supremacy based on Orthogonal Vectors, 3-SUM and All-Pairs Shortest Paths

早川龍[1,a)]　森前智行[1,b)]　玉置卓[2,c)]

概要：Fine-grained quantum supremacy is a study of proving (nearly) tight time lower bounds for classical simulations of quantum computation under "fine-grained complexity" assumptions. We show that under conjectures on Orthogonal Vectors (OV), 3-SUM, All-Pairs Shortest Paths (APSP) and their variants, strong and weak classical simulations of quantum computation are impossible in certain exponential time with respect to the number of qubits. Those conjectures are widely used in classical fine-grained complexity theory in which polynomial time hardness is conjectured. All previous results of fine-grained quantum supremacy are based on ETH, SETH, or their variants that are conjectures for SAT in which exponential time hardness is conjectured. We show that there exist quantum circuits which cannot be classically simulated in certain exponential time with respect to the number of qubits first by considering a Quantum Random Access Memory (QRAM) based quantum computing model and next by considering a non-QRAM model quantum computation. Finally, we show that there exists a hierarchy of fine-grained lower bounds for classical simulations of quantum computation based on k-OV, which is the generalized version of OV.

1. Introduction

Quantum computation is believed to have advantages in its computing time over classical computing and there are several approaches to show these advantages. One way is to show that a quantum algorithm can solve a problem faster than the best known classical algorithm, such as Shor's factoring algorithm [1]. However, the best record could be renewed [2]. Another approach is based on query complexity, such as Grover's search algorithm [3]. In query complexity, the advantage can be unconditionally proven but we do not know the real time of computation.

The third approach, which has been actively studied recently, is to consider sampling problems. Classically sampling output probability distributions of quantum computation is called a weak simulation. In contrast, exactly calculating output probability distributions of quantum computation is called a strong simulation. A weak simulation within a multiplicative error is defined as follows:

Definition 1 *We say that an output probability distribution $\{p_z\}_{z\in\{0,1\}^n}$ of a quantum computer is classically sampled in time T within a multiplicative error ϵ if there exists a T-time classical probabilistic algorithm that outputs z with probability q_z such that $|p_z - q_z| \leq \epsilon p_z$ for all $z \in \{0,1\}^n$.*

Meanwhile, a weak simulation within an additive error ϵ in total variation distance is defined by replacing $|p_z - q_z| \leq \epsilon$ of the above definition with $\sum_z |p_z - q_z| \leq \epsilon p_z$. In this paper, we mainly focus on a weak simulation of multiplicative accuracy. A strong simulation is defined as follows:

Definition 2 *We say that an n-qubit quantum circuit C is strongly simulated in time T within an error $\epsilon(n)$ if for every $z \in \{0,1\}^n$, there exists a T-time classical algorithm that can calculate an amplitude $\langle z|C|0^n\rangle$ within an additive error $\epsilon(n)$.*

In this paper, we take $\epsilon(n)$ to $2^{-n}/2$.

It is known that output probability distributions of several sub-universal quantum computing models cannot be classically sampled in polynomial time within a multiplicative error $\epsilon < 1$ unless the polynomial-time hierarchy (PH) collapses to the third level or the second level [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. Several sub-universal models that exhibit such "quantum supremacy" have

[1] 京都大学基礎物理学研究所
[2] 兵庫県立大学 社会情報科学部
[a)] ryu.hayakawa@yukawa.kyoto-u.ac.jp
[b)] tomoyuki.morimae@yukawa.kyoto-u.ac.jp
[c)] tamak@sis.u-hyogo.ac.jp

been found such as the depth-four model [4], the Boson Sampling model [5], the IQP model [6], [7], the one-clean-qubit model (DQC1 model) [8], [9], [10], [11], the random circuit model [12], [13], [14], and the HC1Q model [15].

In the argument of the quantum supremacy based on the PH, the non-collapse of the PH to its third level was first used with the complexity class postBQP and postBPP [6]. If a classical sampler can simulate a quantum computation which is universal under the post-selection within a multiplicative error, it can be shown that postBQP⊆postBPP. Then the PH collapses to its third level because postBQP=PP [16] and by the Toda's theorem [17],

$$\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}} = \mathrm{P}^{\mathrm{postBQP}} \subseteq \mathrm{P}^{\mathrm{postBPP}} \subseteq \Delta_3, \qquad (1)$$

where Δ_3 is the third level of the PH. Later, quantum supremacy results based on the second level of the PH was shown in Ref. [10], [11]. There, $\mathrm{coC_{=}P}$ or equally NQP [18] is considered instead of postBQP. If $\mathrm{NQP} = \mathrm{coC_{=}P} \subseteq \mathrm{NP}$ holds, then

$$\mathrm{PH} \subseteq \mathrm{BP}\cdot\ \mathrm{coC_{=}P} = \mathrm{BP}\cdot\mathrm{NP} = \mathrm{AM}, \qquad (2)$$

and the PH collapses to its second level. (Our results are based on fine-grained assumptions of $\mathrm{coC_{=}P} \subseteq \mathrm{NP}$, which will be explained later.)

All these quantum supremacy results, however, prohibit only polynomial-time classical simulations: these models could be classically simulated in exponential time. To show (nearly) tight time lower bounds for classical simulations of quantum computation, the study of more "fine-grained" quantum supremacy has been started based on fine-grained (classical) complexity. In Refs. [19], [20], impossibilities of some exponential-time strong simulations were shown based on the exponential-time hypothesis (ETH) and the strong exponential-time hypothesis (SETH) [21], [22], [23]. Refs. [24], [25] showed that output probabilities of the IQP model, the QAOA model [26], and the Boson Sampling model cannot be classically sampled in some exponential time within a multiplicative error $\epsilon < 1$ under some SETH-like conjectures. Ref. [27] showed similar results for the one-clean-qubit model and the HC1Q model. Refs. [20], [27] also studied fine-grained quantum supremacy of Clifford-T quantum computation, and Ref. [27] studied Hadamard-classical quantum computation. We summarize the previous results of fine-grained quantum supremacy in table 1. In addition to those summarized in this table, fine-grained quantum supremacy in the additive-error precision is studied in Ref. [24], [28].

In (not fine-grained) complexity theory, it is often considered that whether a problem can be solved in polynomial time or not. For example, the "P ≠ NP conjecture" states that a NP-complete problem, such as 3-SAT problem, cannot be solved in deterministic polynomial time. In fine-grained complexity theory, stronger assumptions are conjectured. For example, the Exponential Time Hypothesis (ETH) states that 3-SAT problem cannot be solved in $2^{o(n)}$ time and the Strong Exponential Time Hypothesis (SETH) states that there exists k-SAT problem which cannot be solved in $2^{(1-\delta)n}$ time for any $\delta > 0$, where n is the number of variables.

In fine-grained complexity theory, not only conjectures in exponential time but also conjectures for problems which can be solved in polynomial time are explored. A fine-grained assumption for polynomial time problem, which is known to be solved in n^m time for some integer m, is usually in the form that this problem cannot be solved in $n^{m-\delta}$ time for any $\delta > 0$. Hardness results based on such conjectures are sometimes referred to as "Hardness in P [29]" because such problems are in P.

All previous results [19], [20], [24], [25], [27] on fine-grained quantum supremacy are based on ETH, SETH, or their variants in which exponential time hardness for SAT problems is conjectured. Conjectures used for strong simulation results are fine-grained assumptions of $\mathrm{P} \not\subseteq \mathrm{NP}$ while conjectures used for the weak simulation results are fine-grained assumptions of $\mathrm{coC_{=}P} \not\subseteq \mathrm{NP}$.

In this paper, we show fine-grained quantum supremacy results (in terms of the qubit-scaling) based on Orthogonal Vectors (OV) [30], 3-SUM [31], All-Pairs Shortest Paths (APSP) [32] and their variants, in which polynomial time hardness is conjectured. OV, 3-SUM and APSP are widely used in classical fine-grained complexity theory as the basis of many other conditional hardness results for problems within P as summarized in Ref. [29].

Among those three conjectures, OV is known to be reduced from SETH [30]. On the other hand, no reduction is known from OV to SETH. This means that the results based on OV are more stable than the results based on SETH in the sense that the results based on OV remain valid even if SETH is refuted. The results based on 3-SUM conjecture and APSP conjecture are independent of SETH (up to currently known reductions) and also remain valid even if SETH is refuted. This is one advantage of considering other conjectures than SETH. APSP is known to be equivalent to Negative Weight Triangle (NWT) [32], and therefore we use the conjecture of NWT to show fine-grained quantum supremacy instead of that of APSP.

For each conjecture, we first show fine-grained quantum supremacy results in the case when the Quantum Random Access Memory (QRAM) [33] is available. The QRAM is the

表 1 A summary of previous results of fine-grained quantum supremacy and our results. N is the number of qubits in the quantum computation (photons in Boson sampling). n is some function of N s.t. $N = poly(n)$. t is the number of T-gates. The conjectures of 1,2,3,4,5,6 and 9 are *exponential-time* versions of NQP = coC$_=$P $\subseteq$ NP.

	Lower bound	Conjecture	Notion of simulation	Model of QC	Reference
1.	2^{aN} (for $0 \le a \le 1/2$)	degree-3-polynomial	Multiplicative error	IQP circuit	[24]
2.	$2^{\frac{aN}{2}}$ (for $0 \le a \le 1/2$)			QAOA circuit	
3.	$2^{(1-a)N}$ (for any $a > 0$)	permanent	Multiplicative error	Boson sampling	[24]
4.	$2^{(1-a)n}$ (for any $a > 0$)	general Boolean	Multiplicative error	DQC1, HC1Q	[27]
5.	$2^{(1-a)N}$ (for any $a > 0$)	log-depth Boolean			
6.	$2^{(1-a)N}$ (for any $a > 0$)	Reversible circuit			
7.	$2^{(1-a)N}$ (for any $a > 0$)	SETH	Strong Simulation	Universal	[19]
8.	$2^{o(t)}$ (for any $a > 0$)	3-CNF (ETH)	Strong Simulation	Clifford-T	[20], [27]
9.		3-CNF	Multiplicative error		[27]
10.	$2^{\frac{2-\delta}{3(c+1)}N}$ (for any $\delta > 0$, some $c > 0$)	OV	Strong Simulation	Universal	This paper
11.	$2^{\frac{2-\delta}{6(c+1)}N}$ (for any $\delta > 0$, some $c > 0$)		Multiplicative error		
12.	$2^{\frac{2-\delta}{13+3\eta}N}$ (for any $\delta, \eta > 0$)	3-SUM	Strong Simulation	Universal	This paper
13.	$2^{\frac{2-\delta}{2(13+3\eta)}N}$ (for any $\delta, \eta > 0$)		Multiplicative error		
14.	$2^{\frac{3-\delta}{4}N}$ (for any $\delta > 0$)	APSP(NWT)	Strong Simulation	Universal	This paper
15.	$2^{\frac{3-\delta}{8}N}$ (for any $\delta > 0$)		Multiplicative error		

quantum version of the Random Access Memory (RAM) and it can return a superposition of data in a single step as

$$\sum_i a_i|i\rangle \otimes |0^d\rangle \xrightarrow{QRAM} \sum_i a_i|i\rangle \otimes |D[i]\rangle, \qquad (3)$$

where $D[i]$ is the d-bit data stored in the memory of index i. Next, we show fine-grained quantum supremacy results of quantum circuits without the QRAM by constructing specific unitary operations which correspond to the QRAM operations.

In both cases, we show that there exist quantum circuits whose output probability distributions cannot be classically sampled in certain exponential time in terms of the number of qubits. In the case of the QRAM based quantum computation, the size of the quantum circuits is linear with respect to the number of qubits. Note that the usage of the QRAM is common in many quantum algorithms with classical data sets [34], [35].

We, however, also consider the non-QRAM model as well, because the QRAM model cannot be directly realized in real experiments. In the case of the non-QRAM model, the size of the quantum circuits is exponential with respect to the number of qubits. Then, this result can be seen as the comparison between the quantum computation without the QRAM power and the classical computation with the RAM power because fine-grained complexity conjectures are usually defined with the word RAM model, in which a d-bit word is assumed to be accessible in $O(1)$ time. The large size of the quantum circuit without the QRAM may seem as a drawback, however, the requirement of large size circuits without the QRAM is in common with many other quantum algorithms with classical data [34], which is inevitable in the currently known techniques. A more efficient treatment of the classical data sets can be said to be an important future problem.

Note that when we use ETH or SETH, we can construct efficient quantum circuits without the QRAM, because the inputs are some Boolean functions which can be encoded into quantum circuits efficiently and there are no large data to be stored in the QRAM.

Our results and previous results are summarized in TABLE 1. The lower bound times of our results are worse than that based on SETH-like conjectures although both are in exponential time. However, our results are also meaningful because the OV conjecture is more stable than SETH and the 3-SUM conjecture and the APSP conjecture are thought to be independent of SETH up to currently known reductions.

Finally, we show that there exists a hierarchy of fine-grained lower bounds for classical simulations of quantum computation based on the k-OV conjecture, which is the generalized version of the OV conjecture. By using the k-OV conjecture, we can derive a hierarchy of fine-grained quantum supremacy very naturally, which is another advantage of considering conjectures other than SETH.

2. Results

In this section, we introduce conjectures on OV, 3-SUM, NWT and k-OV and show fine-grained quantum supremacy results.

2.1 Orthogonal Vectors

In this subsection, we show fine-grained quantum supremacy in terms of the qubit scaling based on Orthogonal Vectors and its variant. Let us introduce the following two conjectures:

Conjecture 1 (Orthogonal Vectors [29]) *For any $\delta > 0$, there is a c such that deciding whether $s > 0$ or $s = 0$ for given vectors, $u_1, ..., u_n, v_1, ..., v_n \in \{0,1\}^d$, with $d = c \log n$ cannot be done in time $n^{2-\delta}$. Here*

$$s \equiv |\{(i,j) \mid u_i \cdot v_j = 0\}|. \tag{4}$$

Conjecture 2 *For any $\delta > 0$, there is a c such that deciding whether $gap \neq 0$ or $gap = 0$ for given vectors, $u_1, ..., u_n, v_1, ..., v_n \in \{0,1\}^d$ and $u'_1, ..., u'_n, v'_1, ..., v'_n \in \{0,1\}^d$ with $d = c \log n$ cannot be done in non-deterministic time $n^{2-\delta}$. Here,*

$$\begin{aligned} gap \equiv\, & |\{(i,j,k,l) \mid u_i \cdot v_j = 0 \cap u'_k \cdot v'_l \neq 0\}| \\ & -|\{(i,j,k,l) \mid u_i \cdot v_j \neq 0 \cap u'_k \cdot v'_l = 0\}|. \end{aligned} \tag{5}$$

We use two different acceptance criteria, one is on #P functions, which is usually considered in fine-grained complexity theory, and the other is on gap functions. The argument of justification of conjecture 2 is given in the subsection 2.5. Note that we formulate Conjecture 2 through two instances of Orthogonal Vectors. The reason for such a formulation is also discussed in the subsection 2.5.

OV is reduced from SETH [30]. Let us introduce the following conjecture:

Conjecture 3 (SETH [21], [22], [23]) *Let A be any deterministic $T(n)$-time algorithm such that the following holds: given (a description of) a CNF, $f : \{0,1\}^n \rightarrow \{0,1\}$, with at most cn clauses, A accepts if $\#f > 0$ and rejects if $\#f = 0$, where*

$$\#f \equiv \sum_{x \in \{0,1\}^n} f(x). \tag{6}$$

Then, for any constant $a > 0$, there exists a constant $c > 0$ such that $T(n) > 2^{(1-a)n}$ holds for infinitely many n.

Then the following lemma hold:

Lemma 1 *([30]) If Conjecture 3 is true, then Conjecture 1 is true.*

A proof of Lemma 1 is given in Ref. [30].

Thinking of the QRAM model quantum computation, we can show the following two results based on the above two conjectures:

Theorem 1 (Strong simulation with QRAM) *Assume that Conjecture 1 is true. Then, for any $\delta > 0$, there is a c such that there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(2-\delta)(N-7)}{3(c+1)}}$.*

Theorem 2 (Weak simulation with QRAM) *Assume that Conjecture 2 is true. Then, for any $\delta > 0$, there is a c such that there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(2-\delta)(N-14)}{6(c+1)}}$.*

By constructing a unitary operation corresponding to the QRAM process, we can show the following two results based on the above two conjectures:

Theorem 3 (Strong simulation) *Assume that Conjecture 1 is true. Then, for any $\delta > 0$, there is a c such that there exists an N-qubit and $O(N^2 2^{\frac{N}{3(c+1)}})$-size quantum circuit which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(2-\delta)(N-7)}{3(c+1)}}$.*

Theorem 4 (Weak simulation) *Assume that Conjecture 2 is true. Then, for any $\delta > 0$, there is a c such that there exists an N-qubit and $O(N^2 2^{\frac{N}{6(c+1)}})$-size quantum circuit whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(2-\delta)(N-14)}{6(c+1)}}$.*

2.2 3-SUM

In this subsection, we show fine-grained quantum supremacy in terms of the qubit scaling based on 3-SUM and its variant. Let us introduce the following two conjectures:

Conjecture 4 (3-SUM [29]) *Given a set $S \subset \{-n^{3+\eta}, ..., n^{3+\eta}\}$ of size n, deciding $s > 0$ or $s = 0$ cannot be done in time $n^{2-\delta}$ for any $\eta, \delta > 0$. Here,*

$$s \equiv |\{(a,b,c) \in S \times S \times S \mid a+b+c = 0\}|. \tag{7}$$

Conjecture 5 *Given two sets $S, S' \subset \{-n^{3+\eta}, ..., n^{3+\eta}\}$ of size n each, deciding $gap \neq 0$ or $gap = 0$ cannot be done in non-deterministic time $n^{2-\delta}$ for any $\eta, \delta > 0$. Here,*

$$\begin{aligned} & gap \\ & \equiv |\{(a,b,c,a',b',c') \in S^3 \times S'^3 \mid a+b+c = 0 \cap a'+b'+c' \neq 0\}| \\ & - |\{(a,b,c,a',b',c') \in S^3 \times S'^3 \mid a+b+c \neq 0 \cap a'+b'+c' = 0\}|. \end{aligned} \tag{8}$$

Thinking of the QRAM model quantum computation, we can show the following results based on these two conjectures:

Theorem 5 (Strong simulation with QRAM) *Assume that Conjecture 4 is true. Then for any $\eta, \delta > 0$, there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(2-\delta)(N-18)}{13+3\eta}}$.*

Theorem 6 (Weak simulation with QRAM) *Assume that Conjecture 5 is true. Then for any $\eta, \delta > 0$, there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(2-\delta)(N-36)}{2(13+3\eta)}}$.*

By constructing a specific unitary operation corresponding to the QRAM operation, we can show the following results based on the above two conjectures:

Theorem 7 (Strong simulation) *Assume that Conjecture 4 is true. Then for any $\eta, \delta > 0$, there exists an N-qubit and $O(N^2 2^{\frac{N}{13+3\eta}})$-size quantum circuit which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(2-\delta)(N-18)}{13+3\eta}}$.*

Theorem 8 (Weak simulation) *Assume that Conjecture 5 is true. Then for any $\eta, \delta > 0$, there exists an N-qubit and $O(N^2 2^{\frac{N}{2(13+3\eta)}})$-size quantum circuit whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(2-\delta)(N-36)}{2(13+3\eta)}}$.*

2.3 Negative Weight Triangle

In this subsection, we show fine-grained quantum supremacy in terms of the qubit scaling based on Negative Weight Triangle and its variant. Let us introduce the following two conjectures:

Conjecture 6 (Negative Weight Triangle [32]) *Given an edge-weighted n-vertex graph $G = (V, E)$ with integer weights from $\{-M, ..., M\}$, where M is a certain integer, deciding whether $s > 0$ or $s = 0$ needs $n^{3-\delta}$ time for any $\delta > 0$. Here,*

$$s \equiv \left|\{(i, j, k) \in V^3 | (i, j, k) \textit{ is good}\}\right|, \tag{9}$$

where we say (i, j, k) is good if it is a triangle and

$$W(e_{i,j}) + W(e_{j,k}) + W(e_{k,i}) < 0, \tag{10}$$

where $e_{i,j}$ is the edge between vertices i and j, and $W(e_{i,j})$ is the weight of it. Note that $W(e_{i,j}) = 0$ means that the edge $e_{i,j}$ has weight 0, which is different from no-edge.

Conjecture 7 *Given two edge-weighted n-vertex graph $G = (V, E)$ and $G' = (V', E')$ with integer weights from $\{-M, ..., M\}$, where M is a certain integer, deciding whether $gap \neq 0$ or $gap = 0$ needs non-deterministic $n^{3-\delta}$ time for any $\delta > 0$. Here,*

$$\begin{aligned} &gap \qquad (11)\\ &\equiv \left|\{(i, j, k, a, b, c) \in V^3 \times V'^3 | (i, j, k) \textit{ is good} \cap (a, b, c) \textit{ is not good}\}\right|\\ &- \left|\{(i, j, k, a, b, c) \in V^3 \times V'^3 | (i, j, k) \textit{ is not good} \cap (a, b, c) \textit{ is good}\}\right|. \end{aligned}$$

Thinking of the QRAM model quantum computation, we can show the following two results based on the above two conjectures:

Theorem 9 (Strong Simulation with QRAM) *Assume that Conjecture 6 is true. Then, for any $\delta > 0$, there is an M such that there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{3-\delta}{4}(N-4\log(2M+1)-22)}$.*

Theorem 10 (Weak Simulation with QRAM) *Assume that Conjecture 7 is true. Then, for any $\delta > 0$, there is an M such that there exists an N-qubit and $O(N)$-size quantum circuit with access to the QRAM whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{3-\delta}{8}(N-8\log(2M+1)-44)}$.*

By constructing a specific unitary operation corresponding to the QRAM process, we can show the following two results based on the above two conjectures:

Theorem 11 (Strong Simulation) *Assume that Conjecture 6 is true. Then, for any $\delta > 0$, there is an M such that there exists an N-qubit and $O(N^2 2^{\frac{N}{2}})$-size quantum circuit which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{3-\delta}{4}(N-4\log(2M+1)-22)}$.*

Theorem 12 (Weak Simulation) *Assume that Conjecture 7 is true. Then, for any $\delta > 0$, there is an M such that there exists an N-qubit and $O(N^2 2^{\frac{N}{4}})$-size quantum circuit whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{3-\delta}{8}(N-8\log(2M+1)-44)}$.*

2.4 Hierarchy of Fine-grained quantum supremacy

In this subsection, we show that there exists a hierarchy of fine-grained lower bounds for classical simulations of quantum computation. For this purpose, we consider the conjecture of classical fine-grained complexity theory called k-Orthogonal Vectors (k-OV) [40]. The k-OV problem and the k-OV conjecture are defined as follows:

Definition 3 (k-OV problem) *For an integer $k \geq 2$, given k sets $(U_1, ..., U_k)$ of n vectors from $\{0, 1\}^{d(n)}$ each, decide whether there exist $u_i \in U_i$ for each i such that over $\mathbb{Z}$,*

$$\sum_{l \in [d(n)]} u_1[l] \cdots u_k[l] = 0. \tag{12}$$

Conjecture 8 (k-OV Conjecture [40]) *For any $\delta > 0$, there exist $d = c \log n$ that any classical deterministic algorithm for the k-OV problem requires $n^{k-\delta}$ time.*

We slightly change this problem into the Gap-k-OV problem and define the Gap-k-OV Conjecture as follows:

Definition 4 (Gap-k-OV problem) *For an integer $k \geq 2$, the Gap-k-OV problem is to determine, given k sets $(U_1, ..., U_k)$ of n vectors from $\{0,1\}^{d(n)}$ each and k sets $(U'_1, ..., U'_k)$ of n vectors from $\{0,1\}^{d(n)}$ each, whether $gap(U_1, ..., U_k, U'_1, ..., U'_k) \neq 0$ or $= 0$, where*

$$\begin{aligned}
&gap(U_1, ..., U_k, U'_1, ..., U'_k)] \qquad (13)\\
&\equiv \Bigg|\Big\{(u_1, ..., u_k, u'_1, ..., u'_k)|\text{ s.t.} \sum_{l\in[d(n)]} u_1[l]\cdots u_k[l] = 0\\
&\quad \cap \sum_{l\in[d(n)]} u'_1[l]\cdots u'_k[l] \neq 0\Big\}\Bigg|\\
&-\Bigg|\Big\{(u_1, ..., u_k, u'_1, ..., u'_k)|\text{ s.t.} \sum_{l\in[d(n)]} u_1[l]\cdots u_k[l] \neq 0\\
&\quad \cap \sum_{l\in[d(n)]} u'_1[l]\cdots u'_k[l] = 0\Big\}\Bigg|.
\end{aligned}$$

Conjecture 9 (Gap-k-OV Conjecture) *For any $\delta > 0$, there exist $d = c \log n$ that the Gap-k-OV problem requires non-deterministic $n^{k-\delta}$ time.*

Those conjectures mean that there exists a time hierarchy for the hardness of k-OV problem or the Gap-k-OV problem because they can be solved in n^k time by the brute-force algorithm but requires $n^{k-\delta}$ time for any $\delta > 0$. The k-OV conjecture can also be reduced from SETH.

Lemma 2 *([30]) If Conjecture 3 is true, then Conjecture 8 is true.*

Reduction from k-OV to SETH is not known and therefore, the following theorems are more stable than the results based on SETH as in the case of OV.

Thinking of the QRAM model quantum computation, we can show the following results based on these two conjectures:

Theorem 13 *(**Hierarchy of Strong Simulation with QRAM**) Assume that Conjecture 8 is true, then for any $\delta > 0$ and every integer $k \geq 2$, there is a $c > 0$ such that there exists an N-qubit and $O(N)$-size quantum circuit with access to a QRAM, which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(k-\delta)(N-2k-3)}{(k+1)(c+1)}}$.*

Theorem 14 *(**Hierarchy of Weak Simulation with QRAM**) Assume that Conjecture 9 is true, then for any $\delta > 0$ and every integer $k \geq 2$, there is a $c > 0$ such that there exists an N-qubit and $O(N)$-size quantum circuit with access to a QRAM, whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(k-\delta)(N-4k-6)}{2(k+1)(c+1)}}$.*

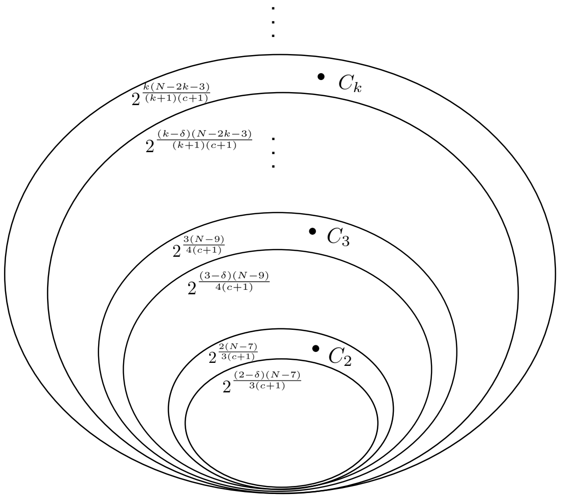
C_k
$2^{\frac{k(N-2k-3)}{(k+1)(c+1)}}$
$2^{\frac{(k-\delta)(N-2k-3)}{(k+1)(c+1)}}$
C_3
$2^{\frac{3(N-9)}{4(c+1)}}$
$2^{\frac{(3-\delta)(N-9)}{4(c+1)}}$
C_2
$2^{\frac{2(N-7)}{3(c+1)}}$
$2^{\frac{(2-\delta)(N-7)}{3(c+1)}}$

図 1 Hierarchy of fine-grained quantum supremacy. This figure means that quantum circuit C_k ($k = 2, 3, ...$) is in a class of circuits which can be simulated classically in $2^{\frac{k(N-k-2)}{(k+1)(c+1)}}$ time but not in a class which can be simulated classically in $2^{\frac{(k-\delta)N-k-2)}{(k+1)(c+1)}}$ time for any $\delta > 0$.

By constructing a specific unitary operation corresponding to the QRAM operation, we can show the following results based on the above two conjectures:

Theorem 15 *(**Hierarchy of Strong Simulation**) Assume that Conjecture 8 is true, then for any $\delta > 0$ and every integer $k \geq 2$, there is a $c > 0$ such that there exists an N-qubit and $O(N^2 2^{\frac{N}{(k+1)(c+1)}})$-size quantum circuit, which cannot be strongly simulated within an additive error 2^{-N} in time $T \equiv 2^{\frac{(k-\delta)(N-2k-3)}{(k+1)(c+1)}}$.*

Theorem 16 *(**Hierarchy of Weak Simulation**) Assume that Conjecture 9 is true, then for any $\delta > 0$ and every integer $k \geq 2$, there is a $c > 0$ such that there exists an N-qubit and $O(N^2 2^{\frac{N}{2(k+1)(c+1)}})$-size quantum circuit, whose acceptance probability cannot be classically sampled within a multiplicative error $\epsilon < 1$ in time $T \equiv 2^{\frac{(k-\delta)(N-4k-6)}{2(k+1)(c+1)}}$.*

Theorem 14 and 16 show that for each integer $k \geq 2$, there exists a quantum circuit C_k which could be sampled classically in $2^{\frac{k(N-2k-6)}{(k+1)(c+1)}}$ time but cannot be simulated in $2^{\frac{(k-\delta)(N-2k-6)}{(k+1)(c+1)}}$ time. This time lower bound grows as k increase. Therefore, those results show that there exists a hierarchy of fine-grained lower bounds for classical simulations of quantum computation (See Fig. 1).

2.5 Justification of conjectures

In this subsection, we argue about an "justification" of Conjecture 2, 5, 7 and 9 which are not standard form in the fine-grained complexity theory and defined in this paper. Let us take Conjecture 1 (OVC) and Conjecture 2 (Gap-N-OVC) for example. Gap-N-OVC is different from OVC in the point that Gap-N-OVC is defined through a variant of a gap function and the hardness even in non-deterministic time is conjectured.

First, note that in the definition of Gap-N-OVC, *gap* is defined through two instances of the OV problem as

$$\begin{aligned} gap \equiv\ & |\{(i,j,k,l) \mid u_i \cdot v_j = 0 \cap u'_k \cdot v'_l \neq 0\}| \\ & -|\{(i,j,k,l) \mid u_i \cdot v_j \neq 0 \cap u'_k \cdot v'_l = 0\}|. \end{aligned} \tag{14}$$

This is because if we define $gap' \equiv |\{(i,j) \mid u_i \cdot v_j = 0\}| - |\{(i,j) \mid u_i \cdot v_j \neq 0\}|$, the existence of an instance which satisfies $gap' = 0$ is unclear.

Then the important point is to consider whether a non-deterministic algorithm can decide whether $gap \neq 0$ or $= 0$ faster than a deterministic algorithm. Up to currently known algorithms, the only known way to decide $gap \neq 0$ or $= 0$ is to compute some #P functions (the number of acceptance paths and the number of rejection paths) and then compute the *gap*. In our case, this corresponds to the counting of $|\{(i,j,k,l) \mid u_i \cdot v_j = 0 \cap u'_k \cdot v'_l \neq 0\}|$ and $|\{(i,j,k,l) \mid u_i \cdot v_j \neq 0 \cap u'_k \cdot v'_l = 0\}|$. The currently known deterministic algorithm to compute #OV of Ref. [36] takes n^2 time as $n \to \infty$ and there is no known result that this can be substantially improved with the power of non-determinism. Those are the reason why our conjectures should be justified.

Similar arguments can be applied to Conjecture 5, 7 and 9.

2.6 Proofs of Theorems

In this paper, we omit the proofs of Theorems. The proofs of Theorems are available at Ref. [43].

参考文献

[1] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994), p.124 (1994).

[2] E. Tang, A quantum-inspired classical algorithm for recommendation systems. Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019) Pages 217-228.

[3] L. K. Grover, Quantum mechanics helps in searching for a needle in haystack. Phys. Rev. Lett. **79**, 325 (1997).

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

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

[6] 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).

[7] 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).

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

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

[10] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits. ICALP 2016.

[11] 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).

[12] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling. Nat. Phys. **15**, pages159–163 (2019).

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

[14] 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

[15] 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).

[16] S. Aaronson, Quantum Computing, Postselection, and Probabilistic Polynomial-Time, Proc. R. Soc. A: **461**, 3473 (2005).

[17] S. Toda, PP Is as Hard as the Polynomial-Time Hierarchy, SIAM J. Comput. **20**, 865 (1991).

[18] S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy, In Proceedings of the 6th Italian Conference on Theoretical Computer Science, pages 241–252, (1998).

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

[20] 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

[21] R. Impagliazzo and R. Paturi, On the complexity of *k*-SAT. Journal of Computer and System Sciences **62**, 367 (2001).

[22] R. Impagliazzo, R. Paturi, and F. Zane, Which problems have strong exponential complexity? Journal of Computer and System Sciences **63**, 512 (2001).

[23] C. Calabro, R. Impagliazzo, and R. Paturi, The Complexity of Satisfiability of Small Depth Circuits. In: Chen J., Fomin F.V. (eds) Parameterized and Exact Computation. IWPEC 2009. Lecture Notes in Computer Science, vol 5917. Springer, Berlin, Heidelberg.

[24] A. M. Dalzell, A. W. Harrow, D. E. Koh, and R. L. La Placa, How many qubits are needed for quantum computational supremacy?, Quantum 4 (2020): 264.

[25] A. M. Dalzell, Lower bounds on the classical simulation of quantum circuits for quantum supremacy. Bachelor’s thesis, Massachusetts Institute of Technology, 2017.

[26] E. Farhi and A. W. Harrow, Quantum supremacy through the quantum approximate optimization algorithm, arXiv:1602.07674v1.

[27] T. Morimae and S. Tamaki, Fine-grained quantum computational supremacy. Quant. Inf. Comput. **19**, 1089-1115 (2019).

[28] T. Morimae and S. Tamaki, Additive-error fine-grained quantum supremacy, arXiv:1912.06336 (2020).

[29] V. V. Williams, Hardness of easy problems: Basing hardness on popular conjectures such as the strong exponential time hypothesis (invited talk). In LIPIcs-Leibniz International Proceedings in Informatics., volume 43, 2015.

[30] R. Williams, A new algorithm for optimal 2-constraint satisfaction and its implications. Ther. Comput. Sci. **348**, 357-365 (2005).

[31] A. Gajentaan and M. H. Overmars, On a class of $O(n^2)$ problems in computational geometry. Computational Geometry **5**, 165 (1995).

[32] Virginia Vassilevska Williams, and Ryan Williams, Subcubic Equivalences Between Path, Matrix, and Triangle Problems. Symposium on Foundations of Computer Science (FOCS), 645 (2010).

[33] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum Random Access Memory. Phys. Rev. Lett. **100**, 160501 (2008).

[34] S. Aaronson, Read the Fine Print, Nature Phys **11**, 291 (2015).

[35] A. Ambainis and N. Larka, Quantum Algorithms for Computational Geometry Problems, ArXiv:2004.08949 (2020).

[36] T. M. Chan and R. Williams, Deterministic APSP, Orthogonal Vectors, and More: Quickly Derandomizing Razborov-Smolensky. SODA 2016: 1246-1255.

[37] A. Barenco et al., Elementary gates for quantum computation. Phys. Rev. A **52**, 3457 (1995).

[38] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, A new quantum ripple-carry addition circuit. arXiv:0410184

[39] D. K. Park, F. Petruccione, and J.-K. K. Rhee, Circuit-Based Quantum Random Access Memory for Classical Data, Sci Rep 9, 3949 (2019).

[40] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, Average-case fine-grained hardness, Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing Pages 483-496 (2017).

[41] Goldreich, Oded, and Guy Rothblum. ”Counting t-cliques: Worst-case to average-case reductions and direct interactive proof systems.” 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2018.

[42] Abboud, Amir, and Kevin Lewi. ”Exact weight subgraphs and the k-sum conjecture.” International Colloquium on Automata, Languages, and Programming. Springer, Berlin, Heidelberg, 2013.

[43] 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 (2019).