Verifying commuting quantum computations via fidelity estimation of weighted graph states

Masahito Hayashi\textsuperscript{1,2,3,}\textsuperscript{*} and Yuki Takeuchi\textsuperscript{4,}\textsuperscript{†}

\textsuperscript{1}Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan
\textsuperscript{2}Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
\textsuperscript{3}Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2 117542, Singapore
\textsuperscript{4}NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan

The instantaneous quantum polynomial time model (or the IQP model) is one of promising models to demonstrate a quantum computational advantage over classical computers. If the IQP model can be efficiently simulated by a classical computer, an unlikely consequence in computer science can be obtained (under some unproven conjectures). In order to experimentally demonstrate the advantage using medium or large-scale IQP circuits, it is inevitable to efficiently verify whether the constructed IQP circuits faithfully work. There exists two types of IQP models, each of which is the sampling on hypergraph states or weighted graph states. For the first-type IQP model, polynomial-time verification protocols have already been proposed. In this paper, we propose verification protocols for the second-type IQP model. To this end, we propose polynomial-time fidelity estimation protocols of weighted graph states for each of the following four situations where a verifier can (i) choose any measurement basis and perform adaptive measurements, (ii) only choose restricted measurement bases and perform adaptive measurements, (iii) choose any measurement basis and only perform non-adaptive measurements, and (iv) only choose restricted measurement bases and only perform non-adaptive measurements. In all of our verification protocols, the verifier’s quantum operations are only single-qubit measurements. Since we assume no i.i.d. property on quantum states, our protocols work in any situation.

I. INTRODUCTION

Quantum computing is believed to be able to perform several computational tasks faster than classical computing. Indeed, some efficient quantum algorithms that outperform the best known classical algorithms have been found for the integer factorization \cite{1}, approximations of Jones polynomials \cite{2, 3}, and simulations of quantum many-body dynamics \cite{4}. In addition, quantum computational advantages have been shown in terms of the query complexity \cite{5, 6} and the communication complexity \cite{7, 8}.

Recently, the quantum computational advantage has also been shown in terms of sampling problems, which is called the quantum (computational) supremacy \cite{9}. If an appropriately designed quantum computing model can be efficiently simulated by a classical computer, an unlikely consequence in computer science can be obtained under some unproven conjectures (for details, see Sec. VIII B). So far, to demonstrate the quantum supremacy, several quantum computing models have been proposed \cite{10–20}. As an advantage of this approach, the quantum computing model do not have to be universal one. Because of this advantage, this approach is considered to be well suited to demonstrate the quantum computational advantage using near-term quantum technologies. Several proof-of-principal small-scale experiments have already been performed towards the demonstration of the quantum supremacy \cite{21–26}.

In order to extend these experimental demonstrations of the quantum supremacy to medium or large-scale ones, efficient methods of verifying whether the target sub-universal model is faithfully realized are inevitable (see Fig. 1). From this importance, several efficient verification protocols have been proposed for various sub-universal quantum computing models \cite{27–31}. However, there is a possibility that conjectures making classical simulations of these verifiable sub-universal models intractable will be rejected. Therefore, it is theoretically and experimentally important to investigate the verifiability of other sub-universal models.

In this paper, we focus on the instantaneous quantum polynomial time (IQP) model \cite{32}. Simply speaking, this model can be considered as a non-adaptive measurement-based quantum computation (MBQC) \cite{33, 34}. In other
words, in the IQP model, an entangled resource state is prepared, and then each of all qubits is simultaneously measured (for details, see Sec. VIII). By appropriately designing the resource state, the IQP model can generate the output probability distribution whose simulation seems to be hard for any classical sampler. More precisely, if the IQP model can be efficiently simulated by a classical computer, the polynomial-time hierarchy would collapse to its third level, which is an unlikely consequence in computer science, under some unproven conjectures. In Ref. [13], two types of IQP circuits have also been shown under different conjectures. The proven conjectures. In Ref. [13], two types of IQP circuits have already been proposed via the efficiency protocols can also be used for the verification of the IQP model. Section IX is devoted to the construction of verification protocols for weighted graph states. In this paper, we affirmatively solve this open problem.

The rest of this paper is organized as follows: In Sec. II, as preliminaries, we review the definition of weighted graph states and explain some terminologies that are necessary to understand our result. In Sec. III, we review some known mathematical facts that are used in proofs of our theorems. In Secs. IV, V, VI, VII, as the main result, we propose four kinds of verification protocols for weighted graph states. In Sec. VIII, we apply our verification protocols to verify the MBQC and the IQP model. Section IX is devoted to the conclusion and discussion.

II. WEIGHTED GRAPH STATES

In this section, we review the definition of weighted graph states [35,37].

Definition 1 (Weighted graph states) Let \( G \equiv (V, E, \Theta) \) be a weighted graph, i.e., a triple of a set \( V \) of vertices, a set \( E \) of edges, and a set \( \Theta \equiv \{ \theta_{jk} \}_{j,k=1}^{n} \) of weights, where \( n \equiv |V| \). Here, \(|V|\) represents the number of vertices, and \( \theta_{jk} \in \mathbb{R} \) represents the weight of the edge \((j,k)\). Note that if \((j,k) \notin E\), \( \theta_{jk} = 0 \). A weighted graph state \( |G\rangle \) corresponding to \( G \) is defined as

\[
|G\rangle \equiv \left( \prod_{(j,k) \in E} \Lambda_{jk}(\Theta_{jk}) \right) |\cdot\rangle^{\otimes n},
\]

where each \( |\cdot\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} \) state is placed on each vertex, and

\[
\Lambda_{jk}(\theta_{jk}) \equiv |0\rangle\langle 0| \otimes I_k + |1\rangle\langle 1| \otimes (|0\rangle\langle 0| \otimes e^{i\theta_{jk}} |1\rangle\langle 1|_k)
\]

is the controlled-Z rotation gate acting on the \( j \)-th and \( k \)-th qubits. Here, \( I_k(j) \) is the two-dimensional identity operator on the \( k \) \text{(}j\text{)}-th qubit.

A subset of \( V \) is called an independent set if no two vertices are connected to each other. A set \( \mathcal{A} = \{ A_1, A_2, \ldots, A_m \} \) of independent sets of \( V \) is called an independence cover if \( \bigcup_{i=1}^{n} A_i = V \). The cover \( \mathcal{A} \) also defines a coloring of \( G \) with \( m \) colors when \( \mathcal{A} \) forms a partition of \( V \), that is, when \( A_i \) are pairwise disjoint (assuming no \( A_i \) is empty). Hereafter, we consider the independence cover whose entries are pairwise disjoint. A weighted graph \( G \) is \( m \)-colorable if its vertices can be colored using \( m \) different colors such that any two adjacent vertices are assigned with different colors. The chromatic number \( \chi(G) \) of \( G \) is the minimal number of colors in any coloring of \( G \) or, equivalently, the minimal number of elements in any independence cover of \( G \). In particular, a two-colorable graph is also called a bipartite graph.

III. FUNDAMENTAL FACTS

First, we review fundamental facts for a conventional testing protocol based on a non-negative operator \( \Omega \) satisfying \( I \geq \Omega \) on the single copy system as follows.

Definition 2 The verifier randomly chooses \( N \) copies from \( N + 1 \) copies and apply the same POVM \( \{ \Omega, I - \Omega \} \) to each of the \( N \) copies. Then, if all outcomes correspond to \( \Omega \), the verifier accepts the remaining single copy \( \sigma \). Otherwise, the verifier rejects it. This test is called the \( N \)-random sampling test of \( \Omega \). When we employ the \( N \)-random sampling test, the operator \( \Omega \) is called the test operator.

We here note that no independent and identically distributed (i.i.d.) property is assumed for \( N + 1 \) copies.
When a positive operator $\Omega$ satisfies the condition
$$\Omega \geq \ket{G}\bra{G},$$
we define the spectral gap $\nu(\Omega) := 1 - \|\Omega - \ket{G}\bra{G}\|$, where $\|A\| := \lambda_{\max}(\{A\})$, $|A| := \sqrt{A^*A}$, and $\lambda_{\max}(\{A\})$ is the maximum eigenvalue of $|A|$. Here, we consider the test operator $\Omega := \sum \lambda_i \Pi_i$, where $\{\Pi_i\}$ are mutually orthogonal rank-one projectors with $\Pi_1 = \ket{G}\bra{G}$. Since $\Omega(\leq I)$ is a positive semidefinite operator and satisfies Eq. 2, $\lambda_i = 1$ and $\{\lambda_i\}_{i \neq 1}$ are non-negative reals less than or equal to one. Therefore, $\nu(\Omega) = \lambda_1 - (\max_{i \neq 1} \lambda_i)$ is indeed the gap. Hereafter, we only consider the case that $\nu(\Omega) > 0$ holds. Then, the paper [30] showed the following.

**Proposition 1 ([30, Theorem 1])** Assume that $\Omega$ satisfies Eq. 2 and $\beta \geq \frac{1}{N\nu(\Omega) + 1}$. When the $N$-random sampling test of $\Omega$ is passed, the resultant state $\sigma$ satisfies
$$\langle G|\sigma|G \rangle \geq 1 - \frac{1 - \beta}{N\beta\nu(\Omega)}$$
with significance level $\beta$.

As the special case with $\nu(\Omega) = 1$, we have the following proposition.

**Proposition 2** Assume that $\beta \geq \frac{1}{m}$. We consider $N + 1$ binary variables $X_1, \ldots, X_{N+1}$. We randomly choose $N$ variables from the above. When all the $N$ values are zero, the remaining variable $X'$ satisfies
$$\Pr \{X' = 1\} \leq \frac{1 - \beta}{\beta N}$$
with significance level $\beta$.

Notice that Proposition 2 holds for any $N + 1$ binary variables $X_1, \ldots, X_{N+1}$ whatever physical device generates the variables $X_1, \ldots, X_{N+1}$. This is because Proposition 2 is a statement with respect to the joint distribution among the variables $X_1, \ldots, X_{N+1}$.

**IV. ADAPTIVE PROTOCOL WITH PERFECT MATCH**

First, we assume that the verifier can choose the measurement basis dependently on the previous measurement outcomes. Also, it is assumed that the verifier can choose any basis with the form $\{\ket{\alpha}, \ket{\alpha + \pi}\}$, where
$$\ket{\alpha} := \frac{1}{\sqrt{2}} (\ket{0} + e^{i\alpha} \ket{1}).$$

Based on an independence cover $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of $V$, we construct the test operator $\Omega(\mathcal{A})$ satisfying Eq. 2 as
$$\Omega(\mathcal{A}) := \sum_{l=1}^{m} \frac{P_l}{m}.$$  

The definition of the projection $P_l$ is given as follows. First, the verifier measures any vertex $j \in A'_l$ in the $Z$ basis and obtains the outcome $Z_j$. Here, the superscript $c$ represents the complementary set. By using the outcomes $Z_l := (Z_j)_{j \in A'_l}$, the expected state on the vertex $k \in A_l$ is given as $|\alpha_k(Z_l)|$, where
$$\alpha_k(Z_l) := \sum_{j \in C_k} \theta_{j,k} Z_j$$
and $C_k$ is the set of vertices connected to the vertex $k$. Then, the verifier measures any vertex $k \in A_l$ in the basis $\{|\alpha_k(Z_l)|, |\alpha_k(Z_l) + \pi\}$. When all the outcomes in $A_l$ correspond to $\otimes_{k \in A_l} |\alpha_k(Z_l)|$, the verifier accepts the resultant state $\sigma$. That is, using $Q_k := \oplus_{z_i} |\alpha_k(z_i)\rangle_k \langle \alpha_k(z_i)| \otimes \sigma_i$, we define $P_l := \prod_{k \in A_l} Q_k$.

Hence, the operator $\Omega(\mathcal{A})$ satisfies Eq. 2. For a subset $B \subset [m] := \{1, \ldots, m\}$, we define the projection $P(B) := \prod_{l \in B} (I - P_l) (\prod_{j \in B} P_j)$. Since $P([m]) = |G\rangle\langle G|$, we have
$$\|\Omega(\mathcal{A}) - |G\rangle\langle G|\| = \sum_{l=1}^{m} \frac{1}{m} \left( P_l - |G\rangle\langle G| \right) = \sum_{B \subset [m]} \frac{|B|}{m} P(B) = \frac{m - 1}{m},$$
which implies that
$$\nu(\Omega(\mathcal{A})) = \frac{1}{m}.$$

Here, $|B|$ represents the number of elements of $B$. Hence, applying Proposition 2 we have the following theorem.

**Theorem 1** The state $|G\rangle^{\otimes (N+1)}$ passes the $N$-random sampling test of $\Omega(\mathcal{A})$ with probability 1. When the test is passed, the resultant state $\sigma$ satisfies
$$\langle G|\sigma|G \rangle \geq 1 - \frac{m(1 - \beta)}{N\beta}$$
with significance level $\beta$.

**V. ADAPTIVE PROTOCOL WITH IMPERFECT MATCH**

Next, we assume that while the verifier can choose the measurement basis dependently on the previous measurement outcomes, available bases for the verifier are limited to the following $h$ bases $\{\ket{\frac{\pi}{h}}, \ket{\frac{\pi}{h} + \pi}\}, \{\ket{\frac{2\pi}{h}}, \ket{\frac{2\pi}{h} + \pi}\}, \ldots, \{\ket{\frac{h\pi}{h}}, \ket{\frac{h\pi}{h} + \pi}\}$ for a positive integer $h$.

For an independence cover $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of $V$, we define the test operator $\Omega_h(\mathcal{A})$ by modifying the test operator $\Omega(\mathcal{A})$ as follows. First, we define $\alpha^h_k(Z_l)$ as $\frac{\pi}{h} \otimes \frac{\pi}{h}$ satisfying $\frac{h \pi}{h} - \frac{\pi}{h} \leq \alpha_k(Z_l) < \frac{h \pi}{h} + \frac{\pi}{h}$. Then, we define the operator $\Omega_h(\mathcal{A})$ and $P_{ih}$ by replacing the basis $\{|\alpha_k(Z_l)|, |\alpha_k(Z_l) + \pi\}$ by the basis $\{|\alpha^h_k(Z_l)|, |\alpha^h_k(Z_l) + \pi\}$ in the definitions of $\Omega(\mathcal{A})$ and $P_l$ in Sec. IV.

Unfortunately, the operator $\Omega_h(\mathcal{A})$ does not necessarily satisfy Eq. 2. Instead, we have the following lemma.
Lemma 1 Let $|A_i|$ be the number of elements of $A_i$. Then, we have the following evaluations.

$$\langle G|\Omega_h(\mathcal{A'})|G \rangle \geq \left(1 - \sin^2 \frac{\pi}{\sqrt{4h}}\right)^{\max_l |A_i|}$$ (11)

$$\|\Omega_h(\mathcal{A}) - \Omega(\mathcal{A'})\| \leq \left(\sum_{l=1}^{m} \frac{|A_l|}{m}\right) \sin \frac{\pi}{\sqrt{4h}}$$ (12)

Proof: Since $|\alpha_k^h(Z_l)|^2 \geq 1 - \sin^2 \frac{\pi}{\sqrt{4h}}$, using $P_{Z_l}(Z_l) := \text{Tr}(G|Z_l)A_l^\dagger A_l^\dagger|G\rangle$, we have

$$\langle G|\Omega_h(\mathcal{A'})|G \rangle = \sum_{l=1}^{m} \frac{1}{m} \langle G|P_{Z_l}|G \rangle$$

$$= \sum_{l=1}^{m} \frac{1}{m} \sum_{z_l} P_{Z_l}(Z_l) \prod_{k \in A_i} |\langle \alpha_k^h(z_l)|\alpha_k(z_l)\rangle|^2$$

$$\geq \sum_{l=1}^{m} \frac{1}{m} \left(1 - \sin^2 \frac{\pi}{\sqrt{4h}}\right)^{|A_l|} \geq \left(1 - \sin^2 \frac{\pi}{\sqrt{4h}}\right)^{\max_l |A_i|}$$.

Also, since

$$\|\alpha_k(Z_l)\rangle \langle \alpha_k(Z_l)| - |\alpha_k^h(Z_l)\rangle \langle \alpha_k^h(Z_l)|\| \leq \sin \frac{\pi}{\sqrt{4h}}$$ (14)

we have

$$\|P_l - P_{l,h}\|$$

$$\leq \|\sum_{z_l} P_{Z_l}(Z_l) \prod_{k \in A_i} |\langle \alpha_k^h(z_l)|\alpha_k(z_l)\rangle|^2$$

$$= \sup_{z_l} \|\sum_{k \in A_i} |\langle \alpha_k^h(z_l)|\alpha_k(z_l)\rangle|^2$$

$$\leq \sup_{z_l} \sum_{k \in A_i} \|\alpha_k^h(z_l)\rangle \langle \alpha_k(z_l)| - |\alpha_k^h(z_l)\rangle \langle \alpha_k(z_l)|\|$$

$$\leq \sup_{z_l} \sum_{k \in A_i} \sin \frac{\pi}{\sqrt{4h}} = |A_i| \sin \frac{\pi}{\sqrt{4h}}.$$ (15)

Hence,

$$\|\Omega_h(\mathcal{A'}) - \Omega(\mathcal{A'})\| \leq \sum_{l=1}^{m} \frac{1}{m} \|P_l - P_{l,h}\|$$

$$\leq \left(\sum_{l=1}^{m} \frac{|A_l|}{m}\right) \sin \frac{\pi}{\sqrt{4h}}.$$ (16)

Using Proposition 2 and Eqs. (9), (11), and (12), we have the following theorem.

Theorem 2 Assume that $\beta \geq 1/N + 1$. The state $|G\rangle^{\otimes(N+1)}$ passes the $N$-random sampling test of $\Omega_h(\mathcal{A'})$ with probability at least $1 - \sin^2 \frac{\pi}{\sqrt{4h}} N \max_l |A_i|$. When the test is passed, the resultant state $\sigma$ satisfies

$$\langle G|\sigma|G \rangle \geq 1 - \frac{m(1 - \beta)}{\beta N} + n \sin \frac{\pi}{\sqrt{4h}}$$ (17)

with significance level $\beta$.

Before giving the proof of Theorem 2 we consider the asymptotic case to evaluate our adaptive protocol. When $N \max_l |A_i| \to 0$, the passing probability with the correct state $|G\rangle$ converges to one as

$$\left(1 - \sin^2 \frac{\pi}{\sqrt{4h}}\right) N \max_l |A_i| \geq 1 - N \max_l |A_i| \sin^2 \frac{\pi}{\sqrt{4h}}$$

$$\geq 1 - N \max_l |A_i| \frac{\pi^2}{16h^2} \to 1,$$ (18)

which implies that the verifier does not mistakenly reject the correct state $|G\rangle$. For example, when $m = n$, i.e., each color has only one vertex, we have $|A_i| = 1$. In this case, when $N = an$ and $h = bn$ with positive constants $a$ and $b$, Eq. (18) holds, and

$$\frac{m(1 - \beta)}{\beta N} + n \sin \frac{\pi}{\sqrt{4h}} \to \frac{1 - \beta}{a \beta} + \frac{\pi}{4b}.$$ (19)

That is, in the asymptotic regime, we can guarantee

$$\langle G|\sigma|G \rangle \geq 1 - \left(\frac{1 - \beta}{a \beta} + \frac{\pi}{4b}\right)$$ (20)

with significance level $\beta$.

To realize $\langle G|\sigma|G \rangle \geq 1 - \epsilon$, $a$ and $b$ need to satisfy $\frac{1 - \beta}{a \beta} + \frac{\pi}{4b} = \epsilon$, i.e.,

$$a = \frac{1 - \beta}{\beta} \left(\epsilon - \frac{\pi}{4b}\right)^{-1},$$ (21)

which requires the condition $\epsilon > \frac{\pi}{4b}$.

Now, we give the proof of Theorem 2 as follows.

Proof: The first statement immediately follows from Eq. (11). Let $\widehat{F}$ be the fidelity between $\sigma$ and $|G\rangle$. Then,

$$\text{Tr} \sigma \Omega_h(\mathcal{A'}) \leq \text{Tr} \sigma |\mathcal{A'}\rangle \langle \mathcal{A'}| + \text{Tr} \sigma |\Omega_h(\mathcal{A'}) - \Omega(\mathcal{A'})|$$

$$\leq \text{Tr} \sigma \left|\langle G|G\rangle + \left(1 - \frac{1}{m}\right) (I - |G\rangle \langle G|)\right|$$

$$+ \left(\sum_{l=1}^{m} \frac{|A_l|}{m}\right) \sin \frac{\pi}{\sqrt{4h}}$$

$$= F + (1 - F) \left(1 - \frac{1}{m}\right) + \left(\sum_{l=1}^{m} \frac{|A_l|}{m}\right) \sin \frac{\pi}{\sqrt{4h}}$$

$$= 1 - \frac{1 - F}{m} + \left(\sum_{l=1}^{m} \frac{|A_l|}{m}\right) \sin \frac{\pi}{\sqrt{4h}}.$$ (22)

where (a) follows from the combination of Eqs. (9) and (12).

We virtually consider the case when we apply the two-valued POVM $\{\Omega_h(\mathcal{A}), I - \Omega_h(\mathcal{A})\}$ to all the $N + 1$ systems. Then, we define the variable $X_i$ as the outcome of the $i$-th system. Here, the outcome 0 corresponds to the POVM $\Omega_h(\mathcal{A})$ and the outcome 1 does to the POVM $I - \Omega_h(\mathcal{A})$. Now, we apply Proposition 2 to the $N + 1$ binary variables $X_1, \ldots, X_{N+1}$ defined here. Under this application, we have

$$\text{Pr}[X_{N+1} = 1|X'_1 = \ldots = X'_{N} = 0] = \text{Tr} \sigma (I - \Omega_h(\mathcal{A})).$$

Hence, when the test is passed, Proposition 2 guarantees that

$$\text{Tr} \sigma \Omega_h(\mathcal{A'}) \geq 1 - \frac{1 - \beta}{\beta N}.$$ (23)
holds with significance level $\beta$. Hence, solving the inequality
\[
1 - \frac{1 - F}{m} + \left(\sum_{l=1}^{\lfloor \frac{m}{\beta} \rfloor} \sin \frac{\pi}{4h} \right)^2 \geq 1 - \frac{1 - \beta}{\beta N},
\]
we have
\[
1 - F \leq m \left(1 - \frac{\beta N}{\beta N} + \left(\sum_{l=1}^{\lfloor \frac{m}{\beta} \rfloor} \sin \frac{\pi}{4h} \right)^2 \right) = m \left(1 - \frac{\beta N}{\beta N} + n \sin \frac{\pi}{4h} \right)
\]
with significance level $\beta$, which is the desired statement.

**VI. NON-ADAPTIVE PROTOCOL WITH PERFECT MATCH**

To consider a verification method without adaptive basis choice, we consider another type of test. Given integers $h = \{h(k)\}_{k \in [n]}$ and an independence cover $\mathcal{A} = \{A_1, A_2, \ldots, A_m\} \subseteq \mathcal{V}$, we define the test operator
\[
\tilde{P}_l := \prod_{k \in A_l} \left( \frac{1}{h(k)} Q_k + \frac{h(k) - 1}{h(k)} \right).
\]
Then, we define the operator
\[
\tilde{\Omega}(\mathcal{A})_h := \sum_{l=1}^{m} \frac{1}{m} \tilde{P}_l,
\]
which satisfies Eq. (27). We have the following lemma.

**Lemma 2** The spectral gap of $\tilde{\Omega}(\mathcal{A})_h$ is calculated as
\[
\nu(\tilde{\Omega}(\mathcal{A})_h) = \frac{1}{m \max_{k \in [n]} h(k)}.
\]

**Proof:** For a subset $B \subseteq A_l$, we define the projection $Q(B) := \prod_{k \in A_l \setminus B} \left(I - Q_k\right) \prod_{j \in B} Q_j$. Then,
\[
\tilde{P}_l = \prod_{k \in A_l} Q_k + \frac{h(k) - 1}{h(k)}(I - Q_k)
\]
\[
= P_l + \sum_{B \subseteq A_l, k \in A_l \setminus B} \prod_{h(k) - 1\over h(k)} Q(B).
\]
Hence,
\[
\|\tilde{\Omega}(\mathcal{A})_h - |G\rangle \langle G|\| = \max_l \left( \frac{m - 1}{m} + \frac{1}{m} \sum_{B \subseteq A_l, k \in A_l \setminus B} \left| \prod_{h(k) - 1\over h(k)} Q(B) \right| \right)
\]
\[
= \max_l \left( \frac{m - 1}{m} + \frac{1}{m} \max_{k \in A_l} h(k) \right).
\]
Hence, using the relation $\max_l \max_{k \in A_l} h(k) = \max_{k \in [n]} h(k)$, we obtain Eq. (28).

Therefore, combining Proposition 1 and Lemma 2 we have the following theorem.

**Theorem 3** The state $|G\rangle^{\otimes (N+1)}$ passes the $N$-random sampling test of $\tilde{\Omega}(\mathcal{A})_h$ with probability 1. When this test is passed, the resultant state $\sigma$ satisfies
\[
\langle G| \sigma|G\rangle \geq 1 - \frac{m(1 - \beta) \max_{k \in [n]} h(k)}{N\beta}
\]
with significance level $\beta$.

Next, we discuss a test whose measurement basis cannot be chosen dependently on the obtained outcomes. Also, we assume that possible values of $\alpha_k(z_l)$ for $k \in A_l$ belongs to one of $c(k)$ bases $\{\{\alpha_k,1\}, \{\alpha_k,1 + \pi\}, \{\alpha_k,2\}, \{\alpha_k,2 + \pi\}, \ldots, \{\alpha_k(c(k)), \{\alpha_k(c(k) + \pi)\}\}$, where $0 \leq \alpha_k < \pi$ for $j = 1, \ldots, c(k)$. In this case, we consider the following protocol by modifying $\tilde{\Omega}(\mathcal{A})_h$.

When the verifier chooses $A_l$, the verifier randomly chooses a measurement basis $\{\{\alpha_k,F_k\}, \{\alpha_k,F_k + \pi\}\}$ from $c(k)$ bases $\{\{\alpha_k,1\}, \{\alpha_k,1 + \pi\}, \{\alpha_k,2\}, \{\alpha_k,2 + \pi\}, \ldots, \{\alpha_k(c(k)), \{\alpha_k(c(k) + \pi)\}\}$ with probability $1/c(k)$ and measures each of vertices in $A_l$ in this measurement basis while the verifier measures the remaining vertices in the $Z$ bases. Then, given $F_k$ and $z_l$, we define the subset $A_l,F_k,k \subseteq A_l$ as the set of vertices $k \in A_l$ satisfying the condition that the chosen basis $\{\{\alpha_k,F_k\}, \{\alpha_k,F_k + \pi\}\}$ is correct. The verifier considers that the test is passed when the measurement outcome at any vertex $k \in A_l,F_k,k$ corresponds to $\{\alpha_k(z_l)\}$. Note that when $A_l,F_k,k = \emptyset$, the test is always passed.

Since the verifier chooses the correct basis with probability $1/c(k)$ for any $k \in A_l$, the above test is given as the operator $\tilde{\Omega}(\mathcal{A})_h$, where $e = \{\{k\}\}_{k \in [n]}$. That is, Theorem 3 gives the performance of this test.

**VII. NON-ADAPTIVE PROTOCOL WITH IMPERFECT MATCH**

Next, we consider the case when adaptive basis choice is not allowed and possible values of $\alpha_k(z_l)$ cannot be limited to a subset with reasonable elements. Given an integer $h$ and an independence cover $\mathcal{A} = \{A_1, A_2, \ldots, A_m\} \subseteq \mathcal{V}$, by using the operators
\[
\tilde{P}_{l,h} := \prod_{k \in A_l} \left( \frac{1}{h} Q_{k,h} + \frac{h - 1}{h} I\right),
\]
\[
Q_{k,h} := \langle z_l|\alpha_k^h(z_l)|\alpha_k^h(z_l)\rangle \otimes |z_l\rangle A_l \langle z_l|,
\]
we define the test operator
\[
\tilde{\Omega}_h(\mathcal{A}) := \sum_{l=1}^{m} \frac{1}{m} \tilde{P}_{l,h},
\]
Then, we have the following lemma.
Lemma 3 When \( h(k) = h \) for any \( k \), we denote \( h \) by \( h \). Then, we have
\[
\langle G | \Omega_h(\mathcal{A}) | G \rangle \geq \left( 1 - \frac{1}{h} \sin^2 \frac{\pi}{4h} \right)^{\max_i |A_i|}, \tag{34}
\]
\[
\nu(\Omega(\mathcal{A})) = \frac{1}{mh}, \tag{35}
\]
\[
\|\Omega_h(\mathcal{A}) - \Omega(\mathcal{A})\|_h \leq \left( \sum_{l=1}^{m} \frac{|A_l|}{mh} \right) \sin \frac{\pi}{4h}. \tag{36}
\]

Proof: Eq. (34) can be shown as follows.
\[
\langle G | \Omega_h(\mathcal{A}) | G \rangle = \sum_{l=1}^{m} \frac{1}{m} \sum_{z_l} \langle z_l | \nu | G \rangle
\]
\[
\prod_{k \in A_l} \langle \alpha_k(z_l) | \left( \frac{1}{h} | \alpha_h^l(z_l) \rangle \langle \alpha_h^k(z_l) \rangle + \frac{h - 1}{h} I \right) | \alpha_k(z_l) \rangle
\]
\[
= \sum_{l=1}^{m} \frac{1}{m} \sum_{z_l} \prod_{k \in A_l} \left( \frac{h - 1}{h} + \frac{1}{h} | \langle \alpha_k(z_l) | \alpha_h^k(z_l) \rangle |^2 \right)
\]
\[
\geq \sum_{l=1}^{m} \frac{1}{m} \left( 1 - \frac{1}{h} \sin^2 \frac{\pi}{4h} \right)^{\max_i |A_i|} \tag{37}
\]

Since \( h(k) = h \), Lemma 2 implies Eq. (35) and
\[
\| \hat{P}_i - \hat{P}_{i,h} \|
\]
\[
= \sup_{z_i} \left\| \hat{P}_i | \hat{P}_{i,h} \rangle \right\|
\]
\[
= \sup_{z_i} \left\| \hat{P}_i | \hat{P}_{i,h} \rangle \right\|
\]
\[
\leq \sup_{z_i} \left\| \hat{P}_i | \hat{P}_{i,h} \rangle \right\|
\]

Hence,
\[
\|\Omega_h(\mathcal{A}) - \Omega(\mathcal{A})\|_h \leq \sum_{l=1}^{m} \frac{1}{m} \| \hat{P}_i - \hat{P}_{i,h} \|
\]
\[
\leq \left( \sum_{l=1}^{m} \frac{|A_l|}{mh} \right) \sin \frac{\pi}{4h}. \tag{39}
\]

Using Eqs. (34), (35), and (36) of Lemma 3, we can show the following theorem in the same way as Theorem 2. That is, it can be shown by replacing Eq. 11, 9, and 12 by the proof of Theorem 2 by Eq. 34, 35, and 36, respectively.

Theorem 4 Assume that \( \beta > \frac{1}{N + 1} \). The state \( |G\rangle^\otimes (N + 1) \) passes the \( N \)-random sampling test of \( \Omega_h(\mathcal{A}) \) with probability at least \( 1 - \frac{1}{\beta N} \sin^2 \frac{\pi}{4h} \max_i |A_i| \). When the test is passed, the resultant state \( \sigma \) satisfies
\[
\langle G | \sigma | G \rangle \geq 1 - \left[ \frac{mh(1 - \beta)}{\beta N} + n \sin \frac{\pi}{4h} \right] \tag{40}
\]

with significance level \( \beta \).

Now, we construct a protocol to realize the test operator \( \Omega_h(\mathcal{A}) \) without adaptive basis choice when possible values of \( \alpha_l(Z_l) \) cannot be limited to a subset with reasonable elements. The verifier randomly chooses a basis state \( |z_l\rangle \) from an independence cover \( \{ |1\rangle_{\mathbb{H}}, |1\rangle_{\mathbb{H}} + \pi \} \) from bases \( \{ |1\rangle_{\mathbb{H}}, |1\rangle_{\mathbb{H}} + \pi \} \). Since the verifier chooses the correct basis \( |\alpha_h^k(z_l)\rangle \) with probability \( 1/h \) and measures each of vertices in \( A_l \) in this measurement basis while the verifier measures the remaining vertices in the \( Z \) bases. Then, given \( F \) and \( Z_l \), we define the subset \( A_{l,h,f,z_l} \subset A_l \) as the set of vertices \( k \in A_l \) satisfying the condition that the chosen basis state \( |\alpha_h^k(z_l)\rangle \) or \( |\alpha_h^k(z_l) + \pi\rangle \) equals to the correct basis \( |\alpha_h^k(z_l)\rangle \). The verifier considers that the test is passed when the measurement outcome at any vertex \( k \in A_{l,h,f,z_l} \) corresponds to \( |\alpha_h^k(z_l)\rangle \). Since the verifier chooses the correct basis with probability \( 1/h \) for any \( k \in A_l \), this test is given as the test operator \( \Omega_h(\mathcal{A}) \).

For example, when \( m = n \), i.e., each color has only one vertex, we have \( |A_l| = 1 \). In this case, when \( N = an^2 + bh \) with positive constants \( a \) and \( b \), the passing probability with the correct state \( |G\rangle \) is
\[
\left( 1 - \frac{1}{h} \sin^2 \frac{\pi}{4h} \right)^N = \left( 1 - \frac{1}{bn} \sin^2 \frac{\pi}{4bn} \right)^{an^2} \geq 1 - \frac{an^2}{bn} \sin^2 \frac{\pi}{4bn} \approx 1 - \frac{an^2}{16bn^2} = 1 - o \left( \frac{1}{n} \right). \tag{41}
\]

On the other hand,
\[
\frac{mh(1 - \beta)}{\beta N} + n \sin \frac{\pi}{4h} \rightarrow \frac{(1 - \beta)b}{a \beta} + \frac{\pi}{4b}. \tag{42}
\]

That is, in the asymptotic regime, we can guarantee
\[
\langle G | \sigma | G \rangle \geq 1 - \left[ \frac{(1 - \beta)b}{a \beta} + \frac{\pi}{4b} \right] \tag{43}
\]
with significance level $\beta$.

To realize $\langle G | \sigma | G \rangle \geq 1 - \epsilon$, $a$ and $b$ need to satisfy

$$a = \frac{1 - \beta}{\beta} \left( \epsilon - \frac{\pi}{4b^2} \right)^{-1}.$$  \hspace{1cm} (44)

The function $b \mapsto \left( \frac{c}{2} - \frac{\pi}{4b^2} \right)^{-1}$ realizes the minimum value $\frac{c}{2}$ when $b = \frac{1}{2\sqrt{\epsilon}}$. That is, when $\epsilon = \frac{c}{2\beta}$, $N = \frac{\pi(1-\beta)}{2\epsilon}$ is sufficient to guarantee $\langle G | \sigma | G \rangle \geq 1 - \epsilon$ with significance level $\beta$ in the asymptotic regime.

### VIII. Applications

In this section, we apply our verification protocols to verify several quantum computing models. In Sec. VIII A, we consider the verification of the MBQC [13, 34]. In Sec. VIII B, we consider the verification of IQP circuits [32]. Although all of our verification protocols can be applied to these purposes, for simplicity, we focus on our third protocol proposed in Sec. VI.

#### A. Verification of measurement-based quantum computing

MBQC [33, 34] is one of the most promising universal quantum computing models. In MBQC, quantum computing proceeds by adaptively measuring each qubits of an entangled state, a so-called universal resource state. So far, several universal resource states have been proposed [38–41]. Among them, the Mølmer-Sørensen (MS) graph state [40]

$$|G_{MS}\rangle := \left( \prod_{(i,j) \in E} e^{-i\theta_{ij}Z_i \otimes Z_j} \right) |+\rangle^\otimes n \hspace{1cm} (45)$$

with $\theta_{ij} \in \{ \frac{\pi}{2}, \frac{3\pi}{4} \}$ is particularly attractive. This is because only $X$ and $Z$-basis measurements are sufficient to perform MBQC on the MS graph state. From Eq. (45), MS graph states are weighted graph states up to local (single-qubit) unitary transformations $\prod_{i \in V} U_i$. Therefore, by transforming the measurement basis on the $i$-th vertex by $U_i^\dagger$ in our verification protocol, we can apply our protocol to estimate the fidelity between the MS graph state and a quantum state generated by experiment. In the case of the MS graph state, $\max_{k \in [n]} \epsilon(k) \leq 8$ and $m \leq n$. Hence,

$$N = \frac{8n(1-\beta)}{\epsilon \beta} \hspace{1cm} (46)$$

is sufficient to guarantee $\langle G_{MS} | \sigma | G_{MS} \rangle \geq 1 - \epsilon$ with significance level $\beta$.

#### B. Verification of instantaneous quantum polynomial time circuits

In this subsection, we consider the verification of quantum supremacy demonstrations with IQP circuits [32]. An $n$-qubit IQP circuit is defined as follows (see Fig. 2).

**Definition 3 (IQP)** An $n$-qubit IQP circuit is a quantum circuit that satisfies following conditions

1. The initial state is $|0\rangle^\otimes n$.
2. The $n$-qubit unitary $H^\otimes n D H^\otimes n$ is applied, where $H$ is the Hadamard gate, and $D$ is a unitary consisting of polynomial number of $Z$-diagonal gates.
3. Finally, all of $n$ qubits are measured in the $Z$ bases.

From Definition 3, the IQP circuit does not seem to be a universal quantum computing model. However, the hardness of classically simulating the IQP circuits has been shown under a certain unproven conjecture. To explain this fact in more detail, we use the following definition.

**Definition 4** Let $\{q_z\}_z$ be the output probability distribution of an $n$-qubit quantum circuit $Q_n$. If there exists a poly($n$)-time classical sampler whose output probability distribution $\{p_z\}_z$ satisfies

$$\sum_z |q_z - p_z| \leq \delta, \hspace{1cm} (47)$$

we say that the output probability distribution $\{q_z\}_z$ of $Q_n$ is classically simulated in poly($n$) time with an $l_1$-norm error $\delta$.

Bremner, Montanaro, and Shepherd have shown that, assuming a certain unproven conjecture, output probability distributions of IQP circuits cannot be classically simulated in poly($n$) time with a constant $l_1$-norm error unless the polynomial-time hierarchy (PH) collapses to its third level [13]. The PH is an infinite tower of complexity classes. In other words, when we write the $i$-th level of the PH as a complexity class $\Sigma_i P$, $PH = \cup_{i \geq 0} \Sigma_i P$ (for more formal definition, see Ref. [42]). If $PH \subseteq \Sigma_i P$, we say that the PH collapses to its $i$-th level (see Fig. 3). In the field of computer science, it is widely believed that the PH does not collapse. Therefore, their result suggests the quantum computational advantage of IQP circuits, a so-called quantum (computational) supremacy.

More precisely, they have shown the following theorem.


\[ \mathcal{P}H = \bigcup_{k \geq 1} \Sigma_k \mathcal{P} \]

\[ \text{FIG. 3: Illustration of the collapse of PH to its third level } \Sigma_3 \mathcal{P}. \]

The PH \( \mathcal{P}H = \bigcup_{k \geq 1} \Sigma_k \mathcal{P} \) is an infinite tower of complexity classes, where \( \Sigma_k \mathcal{P} \) represents the \( k \)-th level of the PH. If all levels above the third is contained in the third level, we say that the PH collapses to its third level.

**Theorem 5** (13) Assume either one of below two conjectures is true. If the output probability distribution of any IQP circuit can be classically simulated in polynomial time, up to an error of \( \frac{1}{192} \) in \( l_1 \) norm, then the PH would collapse to its third level.

**Conjecture 1** (13) Let

\[ Z_R := \sum_{z \in \{ \pm 1 \}^n} e^{i \pi / 8 (\sum_{j \leq k} w_{jk} z_j z_k + \sum_{v_1 \in v_2} v_1 v_2)}, \tag{48} \]

where \( j, k \in \{ 1, 2, \ldots, n \} \) and \( w_{jk}, v_1 \in \{ 0, 1, \ldots, 7 \} \). It is \#P-hard to approximate \(|Z_R|^2\) up to a multiplicative error \( \frac{1}{4} + O(1) \) for a \( \frac{1}{31} \) fraction of instances over the choice of \( \{ w_{jk} \}_{j < k} \) and \( \{ v_1 \}_{v_1 \in v_2} \).\newpage

**Conjecture 2** (13) Let \( f : \{ 0, 1 \}^n \rightarrow \{ 0, 1 \} \) be a uniformly random degree-three polynomial over \( \mathbb{F}_2 \). Then, it is \#P-hard to approximate \(|\text{gap}(f)|^2\) up to a multiplicative error \( \frac{1}{31} + O(1) \) for a \( \frac{1}{31} \) fraction of polynomials \( f \). Here, \( \text{gap}(f) := |\{ x : f(x) = 0 \}| - |\{ x : f(x) = 1 \}|. \)

\[ |\langle \sigma \rangle| = \frac{1}{\sqrt{n}} \]

Here, we say that a function \( g \) is approximated up to multiplicative error \( \delta \) if \( g' \) is obtained such that \( |g - g'| \leq \delta g \) holds.

\#P (43) is a class of function problems that can be solved by counting the number of solutions of arbitrary NP problems.

When we assume that Conjecture 2 is true, Theorem 5 holds for the IQP circuits whose diagonal gate \( D \) is composed of \( Z \), the controlled-\( Z \), and the controlled-controlled-\( Z \) gates. In this case, output states of IQP circuits (immediately before the \( Z \)-basis measurements) are hypergraph states (35), which are generalizations of graph states, up to local unitary transformations. Therefore, such IQP circuits can be verified using existing polynomial-time verification protocols for hypergraph states (29, 30).

However, since Conjecture 2 has not yet been shown, there is a possibility that Conjecture 2 is incorrect. That is why it is important to consider the case that Conjecture 1 is true.

When Conjecture 1 is true, Theorem 5 holds for the IQP circuits whose diagonal gate \( D \) is composed of \( T := |0\rangle\langle 0| + e^{i \pi / 4} |1\rangle\langle 1| + \Lambda(\frac{\pi}{2}) \). Therefore, the output state of the IQP circuit is

\[ |G_{\text{IQP}}\rangle := \left( \prod_{l=1}^n H_l T_l^{q_l} \right) \left( \prod_{j<k} T_j^{w_{jk}} T_k^{w_{jk}} \Lambda_{jk} \left( \frac{w_{jk} \pi}{2} \right) \right) |+\rangle^n \tag{49} \]

that is a weighted graph state up to local unitary transformations. Since the IQP model can be considered as MBQC with non-adaptive measurements, we should not use adaptive measurements to verify the output state \( |G_{\text{IQP}}\rangle \). Therefore, we focus on our third verification protocol in this subsection. Since \( \max_{k \in [n]} \epsilon(k) \leq 2 \) and \( m \leq n \), by using our third protocol,

\[ N = \frac{2n(1-\beta)}{e \beta} \tag{50} \]

is sufficient to guarantee \(|\langle G_{\text{IQP}}|\sigma\rangle| \geq 1 - \epsilon \) with significance level \( \beta \).

At the last of this subsection, we show that a quantum state \( \sigma \) that passes our verification protocol can be used to demonstrate the quantum supremacy. To this end, from Theorem 5 we show the following corollary.

**Corollary 1** Assume Conjecture 1 is true. If for any output state \( |G_{\text{IQP}}\rangle \), there exists an \( n \)-qubit quantum state \( \sigma \) such that \(|\langle G_{\text{IQP}}|\sigma\rangle| \geq 1 - \epsilon \) with \( \epsilon = \frac{1}{\text{poly}(n)} \), and the probability distribution \( \{ |z\langle\sigma|z\rangle \}_{z \in \{0,1\}^n} \) can be classically simulated in polynomial time, up to an error of \( \frac{1}{192} \) in \( l_1 \) norm, then the PH would collapse to its third level.

\[ \text{Proof: Let } F \text{ be the fidelity between } \sigma \text{ and } |G_{\text{IQP}}\rangle. \text{ Then, we have} \]

\[ \sum_{z \in \{0,1\}^n} |\langle z|G_{\text{IQP}}\rangle|^2 - |\langle z|\sigma|z\rangle| \leq 2\sqrt{1 - F} \]

\[ \leq 2\sqrt{\epsilon} = \frac{1}{\text{poly}(n)} \tag{51} \]

Let \( p_z \) be the probability of a classical sampler outputting \( z \). Then, if we assume that it is possible to classically simulate the probability distribution \( \{ |z\langle\sigma|z\rangle \}_{z \in \{0,1\}^n} \) in polynomial time, up to an error of \( \frac{1}{192} \) in \( l_1 \) norm, from the triangle inequality and Eq. (51),

\[ \sum_{z \in \{0,1\}^n} |\langle z|G_{\text{IQP}}\rangle|^2 - p_z \]

\[ \leq \sum_{z \in \{0,1\}^n} |\langle z|G_{\text{IQP}}\rangle|^2 - |\langle z|\sigma|z\rangle| + \sum_{z \in \{0,1\}^n} |\langle z|\sigma|z\rangle - p_z| \]

\[ \leq \frac{1}{\text{poly}(n)} + \frac{1}{193} \leq \frac{1}{192} \tag{52} \]

This consequence means that it is possible to classically simulate the output probability distribution of the IQP circuit in polynomial time, up to an error of \( \frac{1}{192} \) in \( l_1 \) norm. Therefore, from Theorem 5 the PH collapses to its third level. \( \blacksquare \)
From Theorem 3 using $N = \frac{2n(1-\beta)}{\epsilon^2}$ copies, with significance level $\beta$, we can prepare an $n$-qubit quantum state $\sigma$ whose fidelity with $|G_{\text{IQP}}\rangle$ is at least $1 - \epsilon$. When $\epsilon, \beta = \frac{1}{\text{poly}(n)}$, $N = \text{poly}(n)$, i.e., this preparation can be accomplished in polynomial time. Therefore, by measuring the quantum state $\sigma$ in the $Z$ basis, it is possible to generate the probability distribution $\{\langle z | \sigma | z \rangle \}_{z \in \{0,1\}^n}$ in polynomial time. On the other hand, from Corollary 1, when we assume that the PH does not collapse, this is impossible for any classical sampler. This means that the quantum state $\sigma$ that passes our (third) verification protocol can be used to demonstrate the quantum supremacy.

### IX. CONCLUSION & DISCUSSION

We have proposed four kinds of verification protocols of weighted graph states for each of the following classes of measurements: (i) adaptive and all bases are available, (ii) adaptive and restricted bases are available, (iii) non-adaptive and all bases are available, (iv) non-adaptive and restricted bases are available. The comparison of Theorems 1 2 3 and 4 yields the relationships among these four protocols. As far as we know, so far, no efficient verification protocol has been proposed for weighted graph states. Applying our protocols, we have also shown that the MBQC and the IQP model can be efficiently verified.

In our verification protocols, we assume that the verifier’s single-qubit measurements are ideal. One possible solution to remove this assumption is to utilize the quantum error correction. In Ref. 44, the Raussendorf-Harrington-Goyal (RHG) lattice state 45 enables the verifier to do the topological quantum error correction with only physical single-qubit measurements during the verification of the universal MBQC. Unfortunately, such a scheme is known only for graph states. If a similar scheme is found for weighted graph states, we may be able to add the fault tolerance in our verification protocols.

As another possible solution to remove the assumption, we can consider a classical verification protocol that requires no quantum operation for the verifier. In Ref. 46, under some assumptions, Hangleiter et al. have shown that this approach requires exponentially many runs of the IQP circuit. To circumvent this no-go result, the self-testing approach may be helpful. So far, several self-testing protocols have been proposed for maximally entangled pair of qubits [47, 48], graph states [49, 50], the three-qubit W state [51], and all pure bipartite entangled states [52]. It is an interesting future work to propose a self-testing protocol for weighted graph states.

### ACKNOWLEDGMENTS

We thank Tomoyuki Morimae and Yasuhiro Takahashi for helpful discussions. M. H. is supported in part by Fund for the Promotion of Joint International Research (Fostering Joint International Research) Grant No. 15K0007, Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (A) No. 17H01280, (B) No. 16KT0017, and Kayamori Foundation of Informational Science Advancement. Y. T. is supported by MEXT QLEAP project.

[1] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26, 1484 (1997).

[2] D. Aharonov, V. Jones, and Z. Landau, A Polynomial Quantum Algorithm for Approximating the Jones Polynomial, Algorithmica 55, 395 (2009).

[3] D. Aharonov, I. Arad, E. Eban, and Z. Landau, Polynomial Quantum Algorithms for Additive approximations of the Potts model and other Points of the Tutte Plane, arXiv:quant-ph/0702008.

[4] I. M. Georgescu, S. Ashhab, and F. Nori, Quantum simulation, Rev. Mod. Phys. 86, 153 (2014).

[5] D. R. Simon, On the power of quantum computation, in Proceedings of the 35th Annual Symposium of Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, 1994), p. 116.

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

[7] H. Buhrman, R. Cleve, and A. Wiggins, Quantum vs. classical communication and computation, in Proceedings of the 30th Annual ACM Symposium on Theory of Computing (ACM Press, New York, 1998), p. 63.

[8] R. Raz, Exponential separation of quantum and classical communication complexity, in Proceedings of the 31st Annual ACM Symposium on Theory of Computing (ACM Press, New York, 1999), p. 358.

[9] A. W. Harrow and A. Montanaro, Quantum computational supremacy, Nature(London) 549, 203 (2017).

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

[11] M. Bremner, R. Jozsa, and D. Shepherd, Classical Simulation of Commuting Quantum Computations Implies Collapse of the Polynomial Hierarchy, Proc. R. Soc. A 467, 459 (2011).

[12] Y. Takeuchi and Y. Takahashi, Ancilla-Driven Instantaneous Quantum Polynomial Time Circuit for Quantum Supremacy, Phys. Rev. A 94, 062336 (2016).

[13] 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).

[14] S. Aaronson and A. Arkhipov, The Computational Complexity of Linear Optics, Theory Comput. 9, 143 (2013).

[15] 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).

[16] T. Morimae, Hardness of Classically Sampling the One-Clean-Qubit Model with Constant Total Variation Distance Error, Phys. Rev. A 96, 040302(R) (2017).

[17] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Quantum Supremacy and the Complexity of Random Circuit Sam-
[18] Y. Takahashi, T. Yamazaki, and K. Tanaka, Hardness of classically simulating quantum circuits with unbounded Toffoli and fan-out gates, Quant. Inf. Comput. 14, 1149 (2014).

[19] A. Bouland, J. F. Fitzsimons, and D. E. Koh, Complexity classification of conjugated Clifford circuits, 33rd Computational Complexity Conference (CCC 2018), Leibniz International Proceedings in Informatics (LIPIcs), edited by R. A. Servedio, Vol. 102 (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany), p. 21:1.

[20] 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).

[21] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Photonic Boson Sampling in a Tunable Circuit, Science 339, 794 (2013).

[22] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Experimental boson sampling, Nat. Photon. 7, 540 (2013).

[23] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brood, E. F. Galvao, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, Experimental scattershot boson sampling, Sci. Adv. 1, e1400255 (2015).

[24] H. Wang, Y. He, Y.-H. Li, Z.-E. Su, B. Li, H.-L. Huang, X. Ding, M.-C. Chen, C. Liu, J. Qin, J.-P. Li, Y.-M. He, C. Schneider, M. Kamp, C.-Z. Peng, S. Hoffling, C.-Y. Lu, and J.-W. Pan, High-efficiency multiphoton boson sampling, Nat. Photon. 11, 361 (2017).

[25] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, 12-Photon Entanglement and Scalable Scattershot Boson Sampling with Optimal Entangled-Photon Pairs from Parametric Down-Conversion, Phys. Rev. Lett. 121, 250505 (2018).

[26] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, Experimental Quantum Computing Without Entanglement, Phys. Rev. Lett. 101, 200501 (2008).

[27] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, Direct certification of a class of quantum simulations, Quant. Sci. Tech. 2, 015004 (2017).

[28] J. Miller, S. Sanders, and A. Miyake, Quantum supremacy in constant-time measurement-based computation: A unified architecture for sampling and verification, Phys. Rev. A 96, 062312 (2017).

[29] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X 8, 021060 (2018).

[30] H. Zhu and M. Hayashi, Efficient verification of hypergraph states, [arXiv:1806.05565]

[31] S. Ferracin, T. Kapourniotis, and A. Datta, Verifying quantum computations on noisy intermediate-scale quantum devices, [arXiv:1811.09709]

[32] D. Shepherd and M. J. Bremner, Temporally unstructured quantum computation, Proc. R. Soc. London A 465, 1413 (2009).