Divide-and-conquer verification method for noisy intermediate-scale quantum computation

Yuki Takeuchi[1], Yasuhiro Takahashi[1,2], Tomoyuki Morimae[3], and Seiichiro Tani[1,4]

[1]NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
[2]Faculty of Informatics, Gunma University, 4-2 Aramakimachi, Maebashi, Gunma 371-8510, Japan
[3]Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto 606-8502, Japan
[4]International Research Frontiers Initiative (IRFI), Tokyo Institute of Technology, Japan

Several noisy intermediate-scale quantum computations can be regarded as logarithmic-depth quantum circuits on a sparse quantum computing chip, where two-qubit gates can be directly applied on only some pairs of qubits. In this paper, we propose a method to efficiently verify such noisy intermediate-scale quantum computation. To this end, we first characterize small-scale quantum operations with respect to the diamond norm. Then by using these characterized quantum operations, we estimate the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$ between an actual n-qubit output state $\hat{\rho}_{\rm out}$ obtained from the noisy intermediate-scale quantum computation and the ideal output state (i.e., the target state) $|\psi_t\rangle$. Although the direct fidelity estimation method requires $O(2^n)$ copies of $\hat{\rho}_{\rm out}$ on average, our method requires only $O(D^3 2^{12D})$ copies even in the worst case, where D is the denseness of $|\psi_t\rangle$. For logarithmic-depth quantum circuits on a sparse chip, D is at most $O(\log n)$, and thus $O(D^3 2^{12D})$ is a polynomial in n. By using the IBM Manila 5-qubit chip, we also perform a proof-of-principle experiment to observe the practical performance of our method.

1 Introduction

Universal quantum computers are expected to efficiently solve several hard problems that are intractable for classical counterparts. However, to exploit their full potential, quantum error correction (QEC) is necessary. For current technologies, QEC is highly demanding because it requires precise state preparations, quantum operations, and measurements. That is why the potential of quantum computation without QEC is being actively explored. Such non-fault-tolerant quantum computation is called noisy intermediate-scale quantum (NISQ) computation [1], and several quantum algorithms tailored for it have already been proposed [2, 3, 4] and experimentally evaluated [5, 6].

Although several error mitigation techniques have been proposed [7, 8, 9, 10, 11, 12, 13, 14, 15, 16], NISQ computation should be finished in at most logarithmic time due to the lack of fault-tolerance. Note that when an error occurs with a constant probability in each time step, logarithmic-depth quantum circuits succeed with a probability of the inverse of a polynomial. Furthermore, some current quantum computing chips are sparse in the sense that they can be separated into two parts by removing a small number of connections between two qubits. For example, IBM's 53-qubit chip [17, 18, 19, 20, 21, 22, 23, 24] in Fig. 1 can be separated into two parts ($0-27$ and $28-52$) by removing only two connections between the 21st and 28th qubits and between the 25th and 29th qubits. In short, several NISQ computations can be regarded as shallow (i.e., at most logarithmic-depth) quantum circuits on a sparse chip, and we focus on such NISQ computations.

Since the performance of NISQ computations is strongly affected by noise, it is necessary to efficiently check whether a given NISQ computer works as expected. This task is known as the verification of quantum computation. Although various efficient verification methods [25, 26, 27,

Yuki Takeuchi: yuki.takeuchi.yt@hco.ntt.co.jp

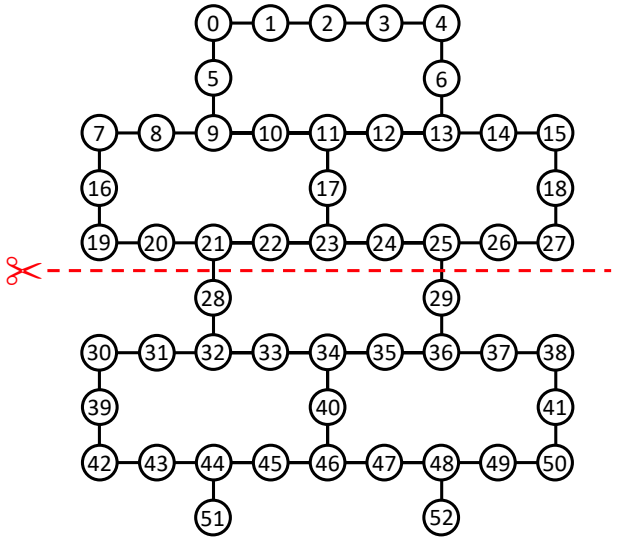

Figure 1: The connectivity of qubits within the IBM Rochester 53-qubit chip. Two-qubit operations can be directly applied on only pairs of two qubits connected by a line. This chip can be separated into two parts ($0-27$ and $28-52$) by removing only two connections between the 21st and 28th qubits and between the 25th and 29th qubits.

28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41] have been proposed so far, they all assume (fault-tolerant) universal quantum computations. Particularly, some of these methods [25, 26, 27, 29, 30, 32, 35, 36, 39, 41] are based on measurement-based quantum computation (MBQC) [42], which consumes at least one qubit to apply a single elementary quantum gate. Therefore, MBQC requires more qubits than the quantum circuit model. Since the number of available qubits is limited in NISQ computations, the MBQC is inadequate for it. The method of Fitzsimons *et al.* [31] requires a prover (i.e., a quantum computer to be verified) to generate a Feynman-Kitaev history state whose generation seems to be hard for NISQ computations. Other methods [34, 37, 38, 40] require the prover to compute classical functions in a superposition, where the functions are constructed from the learning-with-errors problem [43]. This task also seems to be beyond the capability of NISQ computations. Furthermore, since NISQ computers are expected to be used to solve several problems such as optimizations, classifications, and simulations of materials, a verification method should be developed for general problems other than decision problems, which can be answered by YES or NO.

It is highly nontrivial whether an n-qubit NISQ computer can be efficiently verified by using a quantum measurement device that is strictly smaller than n qubits [44]. In this paper, we solve this problem affirmatively. More precisely, let $|\psi_t\rangle$ be any target state, i.e., any n-qubit pure state generated from an ideal logarithmic-depth quantum circuit on a sparse chip. We propose an efficient method (Algorithm 1) to estimate the fidelity between $|\psi_t\rangle$ and the actual state $\hat{\rho}_{\rm out}$ [45] generated from an actual NISQ computer. Our method needs a $(m+1)$-qubit measurement device, where $n/2+1 \leq m+1 < n$. Since our method estimates the fidelity between the actual and ideal quantum states, it can be used for any problems beyond decision problems. Our method is constructed as follows (see also Fig. 2): first, we obtain an upper bound on the diamond norms between the ideal quantum operations achieved in the $(m+1)$-qubit measurement device and its actual ones. Our method works even if the $(m+1)$-qubit measurement device is somewhat noisy, i.e., the upper bound is non-zero but sufficiently small. Then we measure m qubits of $\hat{\rho}_{\rm out}$ and an ancillary qubit $|0\rangle$ by using the noisy $(m+1)$-qubit operators. The remaining $n-m$ qubits of $\hat{\rho}_{\rm out}$ are also similarly measured with another ancillary qubit $|0\rangle$, where $n-m \leq m$. We repeat these procedures by generating a polynomial number of copies of $\hat{\rho}_{\rm out}$. Finally, by classically post-processing all measurement outcomes, we estimate the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$. Since we divide $\hat{\rho}_{\rm out}$ into two parts and measure each of them separately, our verification method can be considered as a divide-and-conquer method.

Our verification method is superior to existing methods in terms of the number of required copies, which we call the sample complexity. The sample complexity of our method is $O(D^3 2^{12D})$ that is a polynomial in n for NISQ computations because the denseness D of $|\psi_t\rangle$ is at most $O(\log n)$ (for the definition of the denseness, see Definition 2). As an existing fidelity estimation method, the quantum state tomography [46, 47, 48] can estimate the fidelity by reconstructing the matrix representation of $\hat{\rho}_{\rm out}$. Since any n-qubit state can be identified using $O(4^n)$ complex numbers, the quantum state tomography requires at least the same number of copies of $\hat{\rho}_{\rm out}$. To improve the efficiency, Flammia and Liu proposed a direct fidelity estimation

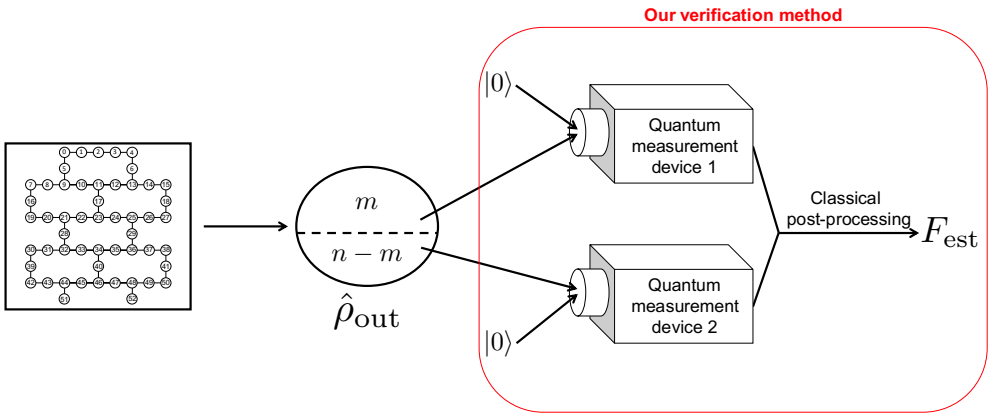

Figure 2: Diagram of our verification method. The n-qubit quantum state $\hat{\rho}_{\rm out}$ is the output from a sparse chip. m and other $n-m$ qubits of $\hat{\rho}_{\rm out}$ are measured by noisy quantum measurement devices 1 and 2 with an ancillary qubit $|0\rangle$, respectively. Our method repeats these procedures polynomially many times. Then by classically post-processing all measurement outcomes, we obtain an estimate $F_{\rm est}$ of the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$. Although we depict the quantum measurement devices 1 and 2 as different devices for simplicity, they can be treated as a single $(m+1)$-qubit device by sequentially measuring m and the other $n-m$ qubits of $\hat{\rho}_{\rm out}$.

method that estimates the fidelity without reconstructing $\hat{\rho}_{\rm out}$ [49]. Their method requires $\Omega(2^n)$ copies of $\hat{\rho}_{\rm out}$ on average. Although their method improved on the quantum state tomography in terms of the number of required copies, the number is still exponential in n. On the other hand, as mentioned above, our method requires only a polynomial number of copies even in the worst case.

Prior to our work, as far as we know, only two types of verification methods were developed for NISQ computers [50, 51, 52]. Our method can estimate the fidelity between ideal and actual output states, unlike the methods in Refs. [50, 51], which can estimate the total variation distance between an actual output probability distribution and the ideal one. In this sense, our method is superior to theirs. Note that theirs can also be used to estimate lower and upper bounds on the probability that the target quantum circuit is afflicted by errors. By using the upper bound, a lower bound on the fidelity can be obtained, which may be loose. The method in Refs. [52] achieves both verifiability and the security, i.e., it enables us to securely and verifiably delegate quantum computing to a remote server even if the server's quantum computer is noisy. Its error robustness is promising. However, their method is based on the MBQC, which seems to be inadequate for NISQ computers as we have mentioned, whereas our method is not.

Efficient verification methods have already been proposed for several quantum states such as graph states [26, 41, 35], hypergraph states [30, 32, 39], weighted graph states [36], and Dicke states [53]. Since these previous methods are tailored for the specific classes of states, they cannot be used for our purpose. Our method can efficiently estimate the fidelity for any pure state generated by shallow quantum circuits on a sparse chip.

The rest of this paper is organized as follows. In Sec. 2, we formally define a class of quantum states, which will be proved to be efficiently verifiable with our method. In Sec. 3, we construct our verification method and derive its sample complexity. In Sec. 4, we provide an observation on the practical performance of our method by performing a proof-of-principle experiment on the IBM Manila 5-qubit chip. Section 5 is devoted to the conclusion and discussion.

2 Target state: sparse quantum state

In this section, we formally define a class of quantum states to be efficiently verified by our method. More precisely, we define sparse quantum states as output states of shallow quantum circuits implemented on a sparse quantum computing chip. To this end, we define a sparse quantum computing chip. Quantum computing chips are often represented by graphs whose vertices and edges represent qubits and the connectivity between qubits (i.e., the applicability of two-qubit gates), respectively. Two-qubit gates can

be directly applied on two qubits whose corresponding vertices are connected by an edge. By using this graph representation, sparse quantum computing chips are defined as follows:

Definition 1 (Sparse quantum computing chip) *An n-qubit quantum computing chip $\mathcal{C}$ is a graph such that n qubits are located on each vertex, and each edge represents the connectivity between the qubits (i.e., the applicability of two-qubit gates). $\mathcal{C}$ is called sparse if it can be divided into two subgraphs with $\Theta(n)$ vertices by removing a constant number of edges.*

As a simple example, when $\mathcal{C}$ is a one-dimensional graph, it is sparse. This is because, a one-dimensional graph can be divided into two subgraphs by removing only one edge.

We also define the denseness of pure states as follows:

Definition 2 (Denseness of pure states) *Let us consider a gate set composed of all single-qubit gates and the controlled-Z (CZ) gate $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes Z$, where I and Z are the two-dimensional identity gate and the Pauli-Z gate, respectively. Let U be any n-qubit quantum circuit that consists of a polynomial number of quantum gates chosen from the gate set. When the set of the n qubits are partitioned into two sets A and B of $\Theta(n)$ qubits, let $CUT(A:B)$ be the number of CZ gates that act across A and B in the quantum circuit U. For every such circuit U, the denseness D of the pure state $U|0^n\rangle$ with respect to U is the minimum number of $CUT(A:B)$ over all partitions $A:B$ of the set of the n qubits that U acts on. When U is clear from the context, we may just write "the denseness D of the pure state $|\psi\rangle$ ", where $|\psi\rangle = U|0^n\rangle$.*

From Definition 1, when an n-qubit quantum circuit U is a d-depth quantum circuit on a sparse chip, the denseness D of $|\psi_t\rangle \equiv U|0^n\rangle$ is $O(d)$. Therefore, when we consider NISQ computations satisfying $d = O(\log n)$, the denseness D is also $O(\log n)$.

3 Divide-and-conquer verification method

In this section, we give our main result. We explain our construction step by step. In Sec. 3.1, we introduce generalized stabilizer operators and explain how to estimate the fidelity by using them. In Sec. 3.2, we decompose n-qubit generalized stabilizer operators into linear combinations of tensor products of m-qubit and $(n-m)$-qubit operators. Then we give an $(n+1)$-qubit quantum circuit to measure each term of the linear combinations. In Sec. 3.3, we show that the $(n+1)$-qubit quantum circuit can be replaced with $(m+1)$-qubit and $(n-m+1)$-qubit quantum circuits. This means that the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$ can be estimated using the resultant $(m+1)$-qubit and $(n-m+1)$-qubit quantum circuits. We also summarize the procedures of our verification method as Algorithm 1. Finally, in Sec. 3.4, we derive the sample complexity, i.e., the required number of copies of $\hat{\rho}_{\rm out}$ to estimate the fidelity. This sample complexity is summarized as Theorem 1.

3.1 Generalized stabilizer operators

Our final goal is to estimate the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$ with the ideal sparse quantum state $|\psi_t\rangle \equiv U|0^n\rangle$. To this end, we first introduce generalized stabilizer operators $\{g_i\}_{i=1}^n$ for $|\psi_t\rangle$, where $g_i \equiv UZ_iU^\dagger$, and Z_i is the Pauli-Z gate applied on the ith qubit [32]. For any $1 \le i \le n$, the equality $g_i|\psi_t\rangle = |\psi_t\rangle$ holds. Furthermore, for any distinct i and j, the operators g_i and g_j commute. This is why we call these operators generalized stabilizer operators. Unlike ordinary stabilizer operators, they cannot generally be written as a tensor product of Pauli operators.

By using the generalized stabilizer operators $\{g_i\}_{i=1}^n$, we obtain

$$|\psi_t\rangle\langle\psi_t| = \prod_{i=1}^n \frac{I^{\otimes n}+\hat{g}_i}{2} = \frac{1}{2^n}\sum_{\mathbf{k}\in\{0,1\}^n}\hat{s}_{\mathbf{k}},$$

where $\hat{s}_{\mathbf{k}} \equiv \prod_{i=1}^n \hat{g}_i^{k_i}$, and $\mathbf{k} \equiv k_1\dots k_n \in \{0,1\}^n$. Therefore,

$$\begin{aligned}\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle &= {\rm Tr}\left[\hat{\rho}_{\rm out}|\psi_t\rangle\langle\psi_t|\right] \\ &= \frac{1}{2^n}\sum_{\mathbf{k}\in\{0,1\}^n}{\rm Tr}\left[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}\right] \\ &= \frac{1}{2^n}\sum_{\mathbf{k}\in\{0,1\}^n}{\rm Re}\left[{\rm Tr}\left[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}\right]\right], \quad (1)\end{aligned}$$

where ${\rm Re}[c]$ is the real part of the complex number c, and in the last equality, we have used the fact that $\hat{s}_{\mathbf{k}}$ is Hermitian for any $\mathbf{k}$. Eq. (1) means

that we can estimate the fidelity as follows: first, a verifier generates an n-bit string $\mathbf{k}$ uniformly at random and then measures $\hat{s}_{\mathbf{k}}$ on $\hat{\rho}_{\rm out}$. The verifier repeats this procedure polynomially many times. A problem of this estimation method is that the measurement of $\hat{s}_{\mathbf{k}}$ generally requires an n-qubit operation.

3.2 Division with respect to the space

Our goal is to show that Eq. (1) can be efficiently estimated using noisy $(m+1)$-qubit and $(n-m+1)$-qubit measurements, where we assume $n/2 \leq m$, implying that $(n-m+1)$-qubit measurements can be implemented by using an $(m+1)$-qubit measurement device. As the first step toward this goal, in this section, we give $(n+1)$-qubit quantum circuits to estimate Eq. (1).

By supposing that the shallow quantum circuit U on a sparse chip is composed of a polynomial number of single-qubit gates and CZ gates, it can be decomposed as shown in Fig. 3:

$$\begin{aligned} U &= \left(\hat{v}^{(D+1)} \otimes \hat{w}^{(D+1)}\right) CZ_{c_D,t_D} \left(\hat{v}^{(D)} \otimes \hat{w}^{(D)}\right) \\ &\quad CZ_{c_{D-1},t_{D-1}} \cdots \left(\hat{v}^{(1)} \otimes \hat{w}^{(1)}\right) \\ &\equiv \left(\hat{v}^{(D+1)} \otimes \hat{w}^{(D+1)}\right) \prod_{i=D}^{1} CZ_{c_i,t_i} \left(\hat{v}^{(i)} \otimes \hat{w}^{(i)}\right), \end{aligned}$$

where $\hat{v}^{(i)}$ and $\hat{w}^{(i)}$ are m-qubit and $(n-m)$-qubit quantum gates for any $1 \leq i \leq D+1$, respectively. Here, D is the denseness of $U|0^n\rangle$. The quantum gate CZ_{c_i,t_i} is the CZ gate applied on the c_ith and t_ith qubits for any $1 \leq i \leq D$, where $1 \leq c_i \leq m < t_i \leq n$.

To use the space-dividing technique of Bravyi *et al.* [54], which replaces two-qubit gates with combinations of single-qubit gates, we further decompose CZ as follows:

$$CZ = \frac{1}{2} \sum_{i,j \in \{0,1\}} (-1)^{ij} \hat{\sigma}(i) \otimes \hat{\sigma}(j),$$

where $\hat{\sigma}(0) \equiv I$ and $\hat{\sigma}(1) \equiv Z$. Let

$$V_{\mathbf{i}} \equiv \hat{v}^{(D+1)} \prod_{k=D}^{1} \hat{\sigma}_{c_k}(i_k) \hat{v}^{(k)}, \tag{2}$$

where $\mathbf{i} \equiv i_1 \dots i_D \in \{0,1\}^D$. Let

$$W_{\mathbf{j}} \equiv \hat{w}^{(D+1)} \prod_{k=D}^{1} \hat{\sigma}_{t_k}(j_k) \hat{w}^{(k)}. \tag{3}$$

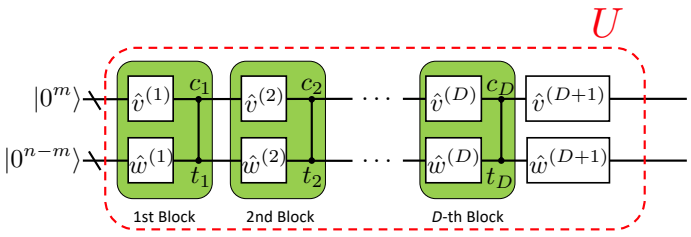

Figure 3: The shallow quantum circuit U on a sparse chip. Since any single-qubit gates and the CZ gate constitute a universal gate set, U can be decomposed as this figure. For all $1 \leq i \leq D+1$, $\hat{v}^{(i)}$ and $\hat{w}^{(i)}$ are m-qubit and $(n-m)$-qubit quantum gates, respectively. Here, D is the denseness of $U|0^n\rangle$. For all $1 \leq i \leq D$, the labels c_i and t_i indicate on which two qubits the corresponding CZ gate is applied, where $1 \leq c_i \leq m < t_i \leq n$.

By using Eqs. (2) and (3), the quantum gate U is represented as

$$U = \frac{1}{2^D} \sum_{\mathbf{i},\mathbf{j} \in \{0,1\}^D} (-1)^{\mathbf{i}\cdot\mathbf{j}} V_{\mathbf{i}} \otimes W_{\mathbf{j}}, \tag{4}$$

where $\mathbf{i} \cdot \mathbf{j} = \oplus_{k=1}^{D} i_k j_k$.

We define an n-qubit gate $Q_{\mathbf{i},\mathbf{j}}^{\dagger} \equiv V_{\mathbf{i}} \otimes W_{\mathbf{j}}$. From Eq. (4),

$$\begin{aligned} \hat{s}_{\mathbf{k}} &= U \left(\prod_{i=1}^{n} Z_i^{k_i}\right) U^{\dagger} \\ &= \frac{1}{4^D} \sum_{\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}' \in \{0,1\}^D} (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} \left[Q_{\mathbf{i},\mathbf{j}}^{\dagger} \left(\prod_{i=1}^{n} Z_i^{k_i}\right) Q_{\mathbf{i}',\mathbf{j}'}\right]. \end{aligned} \tag{5}$$

Therefore, $\mathrm{Re}[\mathrm{Tr}[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}]]$ can be estimated by estimating the real part of

$$(-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} \mathrm{Tr}\left[\hat{\rho}_{\rm out}\left[Q_{\mathbf{i},\mathbf{j}}^{\dagger}\left(\prod_{i=1}^{n} Z_i^{k_i}\right) Q_{\mathbf{i}',\mathbf{j}'}\right]\right]. \tag{6}$$

By using the quantum circuit in Fig. 4 (a), we can estimate the real part of Eq. (6). Let $b \in \{0,1\}$ and $\mathbf{z} \in \{0,1\}^n$ be outputs of the quantum circuit in Fig. 4 (a). $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}') \in \{1,-1\}$ is a random variable such that $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}') = 1$ if and only if $\oplus_{i=1}^{n} z_i k_i = \mathbf{i}\cdot\mathbf{j} \oplus \mathbf{i}'\cdot\mathbf{j}' \oplus b$. When we repeatedly run the quantum circuit in Fig. 4 (a), the mean value of $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$ converges to the real part of Eq. (6) as shown in Ref. [54]. For the completeness of our paper, we show it in Appendix A.

3.3 Division with respect to the time

The quantum circuit in Fig. 4 (a) cannot be split into two small circuits because a common ancillary qubit $|0\rangle$ is used for the first m and other

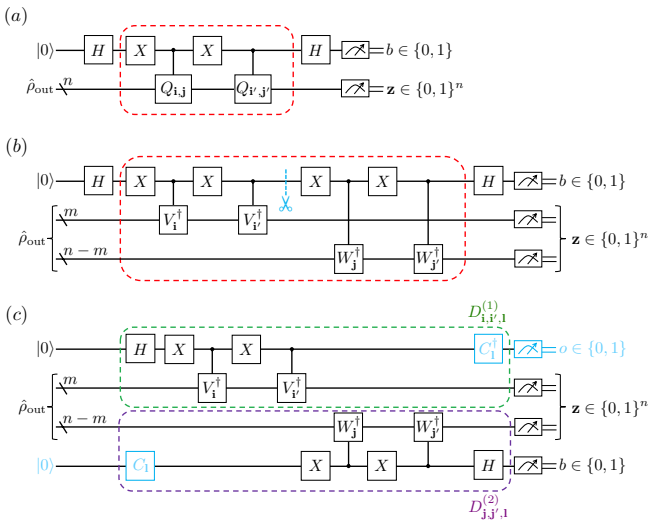

Figure 4: The quantum circuits to estimate the real part of Eq. (6). (a) The $(n+1)$-qubit quantum circuit used in Sec. 3.2. The meter symbols represent measurements in the computational basis. (b) The quantum circuit in (a) can be rewritten as this circuit. The difference is depicted by a dotted red box. Since a common ancillary qubit $|0\rangle$ is used for the first m and other $(n-m)$ qubits, this circuit cannot be split into two small circuits. (c) The quantum circuit in (b) can be divided into $(m+1)$- and $(n-m+1)$-qubit quantum circuits. The dotted blue vertical line in (b) is replaced with blue operations in (c). The Clifford operations $\{C_{\mathbf{l}}\}_{\mathbf{l}\in\{0,1\}^3}$ are defined in Eq. (7). The operations enclosed by the green (upper) and purple (lower) boxes are denoted by $D^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $D^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$, respectively.

$(n-m)$ qubits (see Fig. 4 (b)). To solve this problem, we utilize the time-dividing technique of Peng *et al.* [55], which replaces the identity gate with a combination of single-qubit measurements and preparations.

We replace the identity gate (the dotted blue vertical line in Fig. 4 (b)) with Pauli-basis measurements $\{C_{\mathbf{l}}|0\rangle\langle 0|C_{\mathbf{l}}^\dagger, C_{\mathbf{l}}|1\rangle\langle 1|C_{\mathbf{l}}^\dagger\}_{\mathbf{l}\in\{0,1\}^3}$ and the preparation of Pauli-basis states $\{C_{\mathbf{l}}|0\rangle\}_{\mathbf{l}\in\{0,1\}^3}$ (blue parts in Fig. 4 (c)). Here,

$$C_{\mathbf{l}} \equiv S^{\delta_{l_1,1}\delta_{l_2,0}} H^{\delta_{l_1+l_2,1}} X^{l_3} \tag{7}$$

is the Clifford operation, where $S \equiv \sqrt{Z}$, H is the Hadamard gate, X is the Pauli-X gate, and $\delta_{i,j} = 1$ if and only if $i = j$. Due to this replacement, we can divide the quantum circuit in Fig. 4 (b) into $(m+1)$- and $(n-m+1)$-qubit quantum circuits as shown in Fig. 4 (c).

Algorithm 1 Divide-and-conquer verification method

Purpose: For desired $0 < \epsilon, \delta < 1$, and any n-qubit sparse state $|\psi_t\rangle = U|0^n\rangle$, output F_{est} such that with probability of at least $1-\delta$, $|F_{\text{est}} - \langle\psi_t|\hat{\rho}_{\text{out}}|\psi_t\rangle| \leq \epsilon$.

Assumption: The actual output state $\hat{\rho}_{\text{out}}$ is identically and independently (i.i.d.) distributed, i.e., the actual quantum circuit always outputs $\hat{\rho}_{\text{out}}$. Any $(m+1)$-qubit unitary gate can be approximately achieved in the sense that the diamond norm [56] between its ideal operation and its actual one is at most $\epsilon/4^{D+2}$, where $n/2 \leq m < n-1$ and D is explained later.

Procedures:

1. For a target quantum gate U that is supposed to be implemented by the ideal quantum circuit, divide n input qubits into m and $(n-m)$ qubits such that the number of CZ gates between them is $D = O(\log n)$. This division is possible because of the sparsity of $|\psi_t\rangle$.

2. Under the division obtained in step 1, decompose U as Eq. (4).

3. Choose $\mathbf{k} \in \{0,1\}^n$ T_1 times uniformly at random, and then perform the following steps for each $\mathbf{k}$.

   (a) Calculate the generalized stabilizer operator $\hat{s}_{\mathbf{k}}$ (see Eq. (5)).

   (b) Choose quadruples $(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$ T_2 times uniformly at random. Then, perform the following step for each quadruple $(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$.

      (α) Estimate the expected value of $\sum_{\mathbf{l}\in\{0,1\}^3} \beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})/2$ as an estimated value of the real part of Eq. (6). To this end, run the quantum circuit in Fig. 4 (c) T_3 times for each $\mathbf{l} \in \{0,1\}^3$.

   (c) By averaging the T_2 estimated values of the real part of Eq. (6) obtained in step (α), derive an estimated value of $\text{Tr}[\hat{\rho}_{\text{out}}\hat{s}_{\mathbf{k}}]$.

4. By averaging the T_1 estimated values of $\text{Tr}[\hat{\rho}_{\text{out}}\hat{s}_{\mathbf{k}}]$, obtain F_{est}.

We define a random variable $\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l}) \equiv (-1)^{(1+\delta_{l_1,0}\delta_{l_2,0})o}\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$, where o is the outcome of the first qubit in Fig. 4 (c). The sum $\sum_{\mathbf{l}\in\{0,1\}^3}\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})/2$ converges to the real part of Eq. (6) as shown in Ref. [55]. For the completeness of our paper, we show it in Appendix B.

The procedures of our verification method are summarized as Algorithm 1. In Algorithm 1, the values of T_1, T_2, and T_3 remain free, which determine the sample complexity of our method. These values depend on the accuracy ϵ and the success probability $1-\delta$ and will be derived in the next subsection.

3.4 Sample complexity

In this section, we derive the sample complexity of our method under the assumption that any $(m+1)$-qubit gate can be achieved with the diamond distance at most $\epsilon/4^{D+2}$, and $T_1 = T_2 = T_3$. The sample complexity is the number of copies of $\hat{\rho}_{\rm out}$ required to obtain $F_{\rm est}$ such that with probability of at least $1-\delta$, $|F_{\rm est} - \langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle| \leq \epsilon$. More precisely, we show the following theorem:

Theorem 1 *Let $|\psi_t\rangle \equiv U|0^n\rangle$ be an n-qubit sparse state, where U consists of a polynomial number of CZ gates and single-qubit quantum gates. Suppose that n qubits are divided into m and $(n-m)$ qubits, where $n/2 \leq m$, $m = \Theta(n)$, and $n-m = \Theta(n)$, such that the number of CZ gates between them is $D = O(\log n)$. We assume that $T_1 = T_2 = T_3 = T$, and the diamond norm between any ideal and actual $(m+1)$-qubit gates is upper bounded by $\epsilon/4^{D+2}$. Then for any n-qubit state $\hat{\rho}_{\rm out}$, Algorithm 1 outputs $F_{\rm est}$ such that with probability of at least $1-\delta$, $|F_{\rm est} - \langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle| \leq \epsilon$, by performing $(m+1)$-qubit measurements on*

$$8T^3 = O\left(\frac{2^{12D}}{\epsilon^6}\left(D + \log\frac{1}{\delta\epsilon^4}\right)^3\right)$$

copies of $\hat{\rho}_{\rm out}$, where $0 < \epsilon, \delta < 1$.

Proof. Our verification method consist of three parts: steps 1-4, steps (a)-(c), and step (α).

First, we consider step (α). The ideal functionalities of green and purple dotted boxes in Fig. 4 (c) are represented by $D^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $D^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$, respectively. The actual functionalities somewhat deviate from the ideal ones. We represent the actual functionalities by completely positive trace-preserving (CPTP) maps $\mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$, respectively. Without loss of generality, we can assume that Z-basis measurements and the initialization to $|0\rangle$ in Fig. 4 (c) can be perfectly implemented, because their imperfections can be treated as imperfections on quantum gates $D^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $D^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$. For convenience, we define a superoperator $\mathcal{U}(\cdot) \equiv U(\cdot)U^\dagger$ for any unitary operator U. From the assumption in Algorithm 1, there exists $\epsilon_\diamond (\leq \epsilon/4^{D+2})$ such that

$$\left|\left|\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} - \mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\right|\right|_\diamond \leq \epsilon_\diamond$$
$$\left|\left|\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right|\right|_\diamond \leq \epsilon_\diamond$$

for all $\mathbf{i}$, $\mathbf{i}'$, $\mathbf{j}$, $\mathbf{j}'$, and $\mathbf{l}$.

Let $\Pi_{\beta=1}$ and $\Pi_{\beta=-1}$ be projectors onto the space satisfying $\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l}) = 1$ and $\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l}) = -1$, respectively. We define an observable $B \equiv \Pi_{\beta=1} - \Pi_{\beta=-1}$. We also define $\hat{\rho}'_{\rm out} \equiv |0\rangle\langle 0| \otimes \hat{\rho}_{\rm out} \otimes |0\rangle\langle 0|$. By using them, we show that the expected value of B obtained in the actual case is close to that in the ideal case. More formally, we obtain

$$\begin{aligned}
&\left|\mathrm{Tr}\left[\left(\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right)(\hat{\rho}'_{\rm out})B\right]\right| \\
\leq& \sum_{a\in\{1,-1\}} \\
&\left|\mathrm{Tr}\left[\left(\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right)(\hat{\rho}'_{\rm out})\Pi_{\beta=a}\right]\right| \\
\leq& \left|\left|\left(\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right)(\hat{\rho}'_{\rm out})\right|\right|_1 \\
\leq& \left|\left|\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right|\right|_\diamond \\
\leq& \left|\left|\left(\mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} - \mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\right)\otimes\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right|\right|_\diamond \\
&+ \left|\left|\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\otimes\left(\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right)\right|\right|_\diamond \\
=& \left|\left|\mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} - \mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\right|\right|_\diamond \left|\left|\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right|\right|_\diamond \\
&+ \left|\left|\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}\right|\right|_\diamond \left|\left|\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}} - \mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}\right|\right|_\diamond \\
\leq& 2\epsilon_\diamond,
\end{aligned} \tag{8}$$

where $||\cdot||_1$ and $||\cdot||_\diamond$ are the Schatten 1-norm and the diamond norm, respectively. We have used the triangle inequality to derive the first and fourth inequalities. The second and third inequalities come from Theorem 9.1 in Ref. [57] and the definition of the diamond norm, respectively. The fifth equality is the multiplicativity of

the diamond norm with respect to tensor products [58].

A verifier repeatedly runs the quantum circuit in Fig. 4 (c) T times for each of chosen $\mathbf{i},\mathbf{i}',\mathbf{j},\mathbf{j}',\mathbf{l}$. Note that the verifier can implement only an approximated quantum circuit, i.e., the circuit in Fig. 4 (c) with $\mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $\mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$. Let $\beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})$ be the kth random variable obtained from such approximated quantum circuit for $1 \leq k \leq T$. From the Hoeffding inequality [59],

$$\left| \frac{\sum_{k=1}^{T} \beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})}{T} - \mathrm{Tr}\left[\mathcal{E}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} \otimes \mathcal{E}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}(\hat{\rho}'_{\mathrm{out}})B\right] \right| \leq \epsilon_h$$

holds with probability of at least $1 - 2e^{-T\epsilon_h^2/2}$, where $\epsilon_h > 0$. Therefore, from Eq. (8), with probability of at least $1 - 2e^{-T\epsilon_h^2/2}$,

$$\left| \frac{\sum_{k=1}^{T} \beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})}{T} - \mathrm{Tr}\left[\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} \otimes \mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}(\hat{\rho}'_{\mathrm{out}})B\right] \right| \leq \epsilon_h + 2\epsilon_\diamond. \tag{9}$$

Since $\sum_{\mathbf{l}\in\{0,1\}^3} \beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})/2$ obtained from the ideal circuit in Fig. 4 (c) converges to the real part of Eq. (6) as shown in Appendix B, from Eq. (9),

$$\begin{aligned}
&\left| \sum_{\mathbf{l}\in\{0,1\}^3} \frac{\sum_{k=1}^{T} \beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})}{2T} - \mathrm{Re}\left[(-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'}\mathrm{Tr}\left[\hat{\rho}_{\mathrm{out}}\left[Q^\dagger_{\mathbf{i},\mathbf{j}}\left(\prod_{i=1}^{n} Z_i^{k_i}\right)Q_{\mathbf{i}',\mathbf{j}'}\right]\right]\right] \right| \\
&= \left| \sum_{\mathbf{l}\in\{0,1\}^3} \frac{\sum_{k=1}^{T} \beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})}{2T} - \frac{1}{2}\sum_{\mathbf{l}\in\{0,1\}^3} \mathrm{Tr}\left[\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} \otimes \mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}(\hat{\rho}'_{\mathrm{out}})B\right] \right| \\
&\leq \frac{1}{2}\sum_{\mathbf{l}\in\{0,1\}^3} \left| \frac{\sum_{k=1}^{T} \beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})}{T} - \mathrm{Tr}\left[\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}} \otimes \mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}(\hat{\rho}'_{\mathrm{out}})B\right] \right| \\
&\leq 4\epsilon_h + 8\epsilon_\diamond
\end{aligned} \tag{10}$$

with probability of at least $(1 - 2e^{-T\epsilon_h^2/2})^8$.

Second, we consider steps (a)-(c). In these steps, the verifier chooses quadruples $(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$ T times. Let $(\mathbf{i}^{(i)},\mathbf{j}^{(i)},\mathbf{i}'^{(i)},\mathbf{j}'^{(i)})$ be the ith quadruple for $1 \leq i \leq T$. For simplicity, we define

$$\begin{aligned}
&q(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{k}) \\
&\equiv \mathrm{Re}\left[(-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'}\mathrm{Tr}\left[\hat{\rho}_{\mathrm{out}}\left[Q^\dagger_{\mathbf{i},\mathbf{j}}\left(\prod_{i=1}^{n} Z_i^{k_i}\right)Q_{\mathbf{i}',\mathbf{j}'}\right]\right]\right].
\end{aligned}$$

From the Hoeffding inequality and Eq. (5),

$$\left| \frac{1}{T}\sum_{i=1}^{T} q(\mathbf{i}^{(i)},\mathbf{j}^{(i)},\mathbf{i}'^{(i)},\mathbf{j}'^{(i)},\mathbf{k}) - \frac{\mathrm{Tr}[\hat{\rho}_{\mathrm{out}}\hat{s}_{\mathbf{k}}]}{4^D} \right| \leq \epsilon_h \tag{11}$$

with probability of at least $1 - 2e^{-T{\epsilon_h}^2/2}$.

Let $\tilde{\beta}(\mathbf{i},\mathbf{i}',\mathbf{j},\mathbf{j}') \equiv \sum_{\mathbf{l}\in\{0,1\}^3}\left(\sum_{k=1}^{T}\beta'_k(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})\right)/(2T)$. By using the triangle inequality with Eqs. (10) and (11),

$$\left| 4^D \frac{\sum_{i=1}^{T}\tilde{\beta}(\mathbf{i}^{(i)},\mathbf{i}'^{(i)},\mathbf{j}^{(i)},\mathbf{j}'^{(i)})}{T} - \mathrm{Tr}[\hat{\rho}_{\mathrm{out}}\hat{s}_{\mathbf{k}}] \right| \leq 4^D\left(5\epsilon_h + 8\epsilon_\diamond\right)$$

with probability of at least $(1 - 2e^{-T{\epsilon_h}^2/2})^{8T+1}$.

Finally, we consider steps 1-4. In these steps, the verifier chooses the bit string $\mathbf{k}$ T times. Let $\mathbf{k}^{(i)}$ be the ith chosen bit string for $1 \leq i \leq T$. From the Hoeffding inequality and Eq. (1),

$$\Pr\left[\left| \frac{\sum_{i=1}^{T}\mathrm{Tr}\left[\hat{\rho}_{\mathrm{out}}\hat{s}_{\mathbf{k}^{(i)}}\right]}{T} - \langle\psi_t|\hat{\rho}_{\mathrm{out}}|\psi_t\rangle \right| \leq \epsilon_h\right] \geq 1 - 2e^{-T{\epsilon_h}^2/2}.$$

Let $f \equiv 4^D\left(\sum_{i=1}^{T}\tilde{\beta}(\mathbf{i}^{(i)},\mathbf{i}'^{(i)},\mathbf{j}^{(i)},\mathbf{j}'^{(i)})\right)/T$. We also define $f^{(i)}$ as the random variable f obtained in the case of $\mathbf{k}^{(i)}$. Therefore, by using the triangle inequality, with the probability of at least

$(1-2e^{-T{\epsilon_h}^2/2})^{8T^2+T+1}$,

$$\left|\frac{\sum_{i=1}^{T} f^{(i)}}{T} - \langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle\right| \leq 4^D\left(5\epsilon_h + 8\epsilon_\diamond\right) + \epsilon_h.$$

By setting $F_{\rm est} = (\sum_{i=1}^{T} f^{(i)})/T$, we can estimate the value of the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$.

The remaining task is to calculate the value of $8T^3$ under two conditions

$$4^D\left(5\epsilon_h + 8\epsilon_\diamond\right) + \epsilon_h \leq \epsilon \tag{12}$$

$$(1-2e^{-T{\epsilon_h}^2/2})^{8T^2+T+1} \geq 1-\delta. \tag{13}$$

From $\epsilon_\diamond \leq \epsilon/4^{D+2}$, we can set $\epsilon_h = \epsilon/[2(5\cdot 4^D+1)]$ to satisfy Eq. (12). Therefore, we have

$$\begin{aligned}
&(1-2e^{-T{\epsilon_h}^2/2})^{8T^2+T+1}\\
&\geq 1-2(8T^2+T+1)e^{-T{\epsilon_h}^2/2}\\
&\geq 1-20T^2e^{-T{\epsilon_h}^2/2}\\
&\geq 1-\frac{640}{{\epsilon_h}^4}e^{-T{\epsilon_h}^2/4},
\end{aligned}$$

where we have used $T \geq 1$ and $T^2 \leq 32e^{T{\epsilon_h}^2/4}/{\epsilon_h}^4$ to derive the second and third inequalities, respectively. To satisfy Eq. (13), it is sufficient to set $\delta = 640/({\epsilon_h}^4 e^{T{\epsilon_h}^2/4})$. As a result,

$$\begin{aligned}
T &= \frac{4}{{\epsilon_h}^2}\log\frac{640}{\delta{\epsilon_h}^4}\\
&= \frac{16(5\cdot 4^D+1)^2}{\epsilon^2}\log\frac{10240(5\cdot 4^D+1)^4}{\delta\epsilon^4}\\
&= O\left(\frac{2^{4D}}{\epsilon^2}\left(D+\log\frac{1}{\delta\epsilon^4}\right)\right).
\end{aligned}$$

This completes the proof of Theorem 1. ■

4 Proof-of-principle experiment

In the previous section, we have assumed $\epsilon_\diamond \leq \epsilon/4^{D+2}$. It implies that high-precision quantum gates are necessary to construct $\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$. As a concrete example, suppose that the quantum chip is linear, the required precision ϵ is 0.1, and the target state $|\psi_t\rangle$ is the n-qubit linear graph state $\prod_{i=1}^{n-1} CZ_{i,i+1}(|+\rangle^{\otimes n})$ with n being even. Here, $|+\rangle \equiv (|0\rangle+|1\rangle)/\sqrt{2}$. In this case, each of $\mathcal{D}^{(1)}_{\mathbf{i},\mathbf{i}',\mathbf{l}}$ and $\mathcal{D}^{(2)}_{\mathbf{j},\mathbf{j}',\mathbf{l}}$ can be constructed by using $(13n-15)$ single-qubit gates and $(8n-10)$ CZ's. Therefore, the diamond distance between ideal and actual elementary gates must be at most $1/[640(21n-25)]$. Even when $n=2$, this value $\sim 0.009\%$ is extremely low. Note that for simplicity, we assume that Z-basis measurements and the initialization to $|0\rangle$ are perfectly implemented.

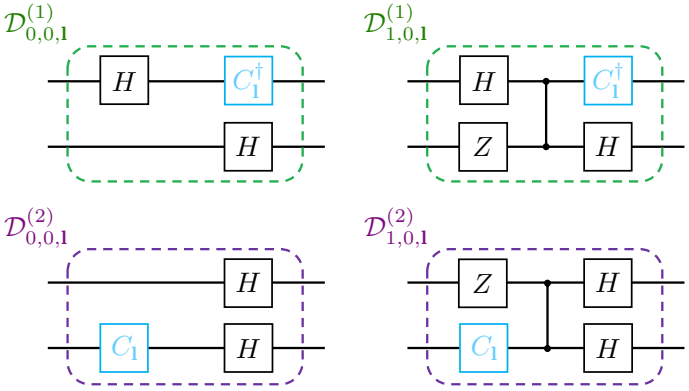

Figure 5: Circuit diagrams of $\mathcal{D}^{(1)}_{i,0,\mathbf{l}}$ and $\mathcal{D}^{(2)}_{j,0,\mathbf{l}}$ for $i,j \in \{0,1\}$ in the case of $|\psi_t\rangle = CZ|+\rangle^{\otimes 2}$. Here, H is the Hadamard gate. These circuits are obtained by simplifying circuits in Fig. 4 (c). To this end, we use two equalities $(I\otimes X)CZ(Z\otimes X) = CZ$ and $CH(X\otimes I)CH(X\otimes I) = I\otimes H$, where $CH \equiv |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes H$.

However, the above analysis is too pessimistic in several situations. Our analysis does not take an actual error model into account (e.g., see calculations to derive Eq. (8)). Furthermore, once $|\psi_t\rangle$ is fixed, we may be able to use properties of $|\psi_t\rangle$ to simplify quantum circuits in Fig. 4 (c). To observe the actual performance of our method, we perform a 4-qubit experiment on the IBM Manila 5-qubit chip. The target state is $|\psi_t\rangle = CZ|+\rangle^{\otimes 2}$. In this case, the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$ can be written as

$$\frac{1}{4}\sum_{i,j\in\{0,1\}}(-1)^{ij}{\rm Re}\left[{\rm Tr}\left[\hat{\rho}_{\rm out}\left[Q^\dagger_{i,j}\left(Z_1^j\otimes Z_2^i\right)Q_{0,0}\right]\right]\right], \tag{14}$$

where we have used

$$\begin{aligned}
&Q^\dagger_{i,j}\left(Z_1^{k_1}\otimes Z_2^{k_2}\right)Q_{i',j'}\\
&= (-1)^{i'k_1+j'k_2}Q^\dagger_{i\oplus i',j\oplus j'}\left(Z_1^{k_1}\otimes Z_2^{k_2}\right)Q_{0,0}
\end{aligned}$$

for any $i,j,i',j' \in \{0,1\}$ and $\mathbf{k} \in \{0,1\}^2$. In our experiment, we estimate each term by running quantum circuits in Fig. 4 (c) $T = 1024$ times for each $\mathbf{l} \in \{0,1\}^3$. In other words, we calculate

$$F_{\rm est} = \frac{1}{4}\sum_{i,j\in\{0,1\}}\sum_{\mathbf{l}\in\{0,1\}^3}\frac{\sum_{k=1}^{1024}\beta'_k(i,j,0,0,\mathbf{l})}{2048}$$

as an estimated value of Eq. (14). To this end, we simplify $\mathcal{D}^{(1)}_{i,0,\mathbf{l}}$ and $\mathcal{D}^{(2)}_{j,0,\mathbf{l}}$ as given in Fig. 5.

Depending on $\mathbf{l}$, we further simplify the circuits in Fig. 5. For example, when $\mathbf{l} = 000$, the CZ gate in $\mathcal{D}^{(2)}_{1,0,\mathbf{l}}$ can be removed because $C_{000}|0\rangle = |0\rangle$. By running these simplified circuits on the IBM Manila 5-qubit chip, we obtain $F_{\rm est} \simeq 0.789$. The experimental data is given in Appendix C.

To check the accuracy of $F_{\rm est}$, a true value $F \equiv \langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$ is necessary. However, in principle, it should be hard to derive F. Therefore, we alternatively compare $F_{\rm est}$ with another estimated value $\tilde{F}_{\rm est}$ that is obtained by directly estimating $\mathrm{Re}[\mathrm{Tr}[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}]]$ for each $\mathbf{k} \in \{0,1\}^2$ (see Eq. (1)). We expect that $\tilde{F}_{\rm est}$ tends to be closer to F than $F_{\rm est}$ is because quantum circuits used to obtain $\tilde{F}_{\rm est}$ are simpler than those used to obtain $F_{\rm est}$ (see Appendix C). In the case of $|\psi_t\rangle = CZ|+\rangle^{\otimes 2}$, we obtain $\hat{s}_{00} = I^{\otimes 2}$, $\hat{s}_{01} = Z \otimes X$, $\hat{s}_{10} = X \otimes Z$, and $\hat{s}_{11} = Y \otimes Y$, where Y is the Pauli-Y operator. Note that since $\hat{s}_{00} = I^{\otimes 2}$, we can set $\mathrm{Re}[\mathrm{Tr}[\hat{\rho}_{\rm out}\hat{s}_{00}]] = 1$ without performing experiments. By measuring the observable $\hat{s}_{\mathbf{k}}$ 1024 times for each $\mathbf{k} \in \{01, 10, 11\}$, we obtain $\tilde{F}_{\rm est} \simeq 0.865$ (see also Appendix C). Contrary to the expectation from the above pessimistic analysis, we conclude that our method faithfully works when $n = 2$ because $|F_{\rm est} - \tilde{F}_{\rm est}| < 0.076$ is sufficiently small (compared with $\epsilon = 0.1$). It would be interesting to explore in which cases our method becomes particularly practical. We leave it as a future work.

5 Conclusion and Discussion

We have proposed and experimentally performed an efficient divide-and-conquer method to verify noisy intermediate-scale quantum (NISQ) computers. Although we have simply divided a verification circuit into two small circuits (see Fig. 4 (c)), our idea can be straightforwardly generalized so that a verification circuit is divided into M circuits for any natural number M. In this case, the sample complexity grows at least exponentially with $\Theta(\tilde{D})$, where $\tilde{D}$ is the number of CZ gates across the M small circuits. Therefore, to make the sample complexity some polynomial in n, $M = O(\log n)$ is required because $M - 1 \leq \tilde{D}$.

For simplicity, we have assumed that $\hat{\rho}_{\rm out}$ is i.i.d. distributed. This assumption may be removed by using the quantum de Finetti theorem for the fully one-way local operations and classical communication (LOCC) norm [60] as in previous studies [30, 32]. Its rigorous analysis is left for future work.

We have also assumed that the quantum computing chip $\mathcal{C}$ is sparse. Our method is superior to the direct fidelity estimation method [49] even when $\mathcal{C}$ is not sparse but is a planar graph with a constant maximum degree. Since the graphs underlying almost all current physical chips are planar ones with constant maximum degrees, this assumption is quite natural. For example, the geometry of Google's Sycamore 53-qubit chip [61] is a planar graph with the maximum degree four, although it is not sparse. As a consequence of the planar separator theorem [62, 63], D is $O(\sqrt{n}\log n)$ for logarithmic-depth quantum circuits on any planar graph with a constant maximum degree. Therefore, the sample complexity of our method is $2^{O(\sqrt{n}\log n)}$, which is less than $O(2^n)$.

The core of our method is to divide a large quantum circuit into two small quantum circuits. By performing classical post-processing on their measurement outcomes, we estimate the value of the fidelity. Such a divide-and-conquer technique has already been used to embed a large problem into NISQ computers [64, 65] and reduce the number of two-qubit gates in quantum circuits [66, 67]. Furthermore, the technique was improved by Perlin *et al.* [68] and experimentally demonstrated by Ayral *et al.* [69]. Our results show that a similar technique can also be used to design an efficient verification method for NISQ computers. As a future work, it would be interesting to consider whether our verification method can be improved by using the result in Ref. [68]. At least, we can say that our construction seems to be more efficient than that using only the time-dividing technique in Ref. [55] in terms of the number of ancillary qubits. As stated in Ref. [44], when the target state is $|\psi_t\rangle = U|0^n\rangle$, the verification is possible by applying $U^\dagger$ to $\hat{\rho}_{\rm out}$. When we straightforwardly apply the time-dividing technique in Ref. [55] to $U^\dagger$, in the worst case, $O(\log n)$ ancillary qubits may be necessary because $D = O(\log n)$, while our construction requires only two ancillary qubits. In other words, although our method requires only $(m+1)$-qubit measurements, the direct use of Ref. [55] may require $(m + O(\log n))$-qubit ones.

A similar but different approach was also used in the Google team's supremacy experiment [61].

To characterize their 53-qubit chip, they divided qubis on it into two small sets, which are called patches, by actually removing all interactions between them. Their verification method was experimentally validated under their noise model. However, their method would not work in the general case. On the other hand, since our method "virtually" removes some two-qubit gates (see Eq. (4)), it works in any case.

Acknowledgments

We thank Samuele Ferracin for helpful discussions. We also thank anonymous reviewers for insightful comments. This work is supported by JST [Moonshot R&D – MILLENNIA Program] Grant Number JPMJMS2061 and the Grant-in-Aid for Scientific Research (A) No.JP22H00522 of JSPS. Y. Takeuchi is supported by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0118067394 and JPMXS0120319794. TM is supported by the JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT Q-LEAP, the Grant-in-Aid for Scientific Research (B) No.JP19H04066 of JSPS, and the Grant-in-Aid for Transformative Research Areas (A) No.JP21H05183. ST is supported by the Grant-in-Aid for Transformative Research Areas No.JP20H05966 of JSPS.

References

[1] J. Preskill, Quantum Computing in the NISQ era and beyond, Quantum **2**, 79 (2018).

[2] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, A variational eigenvalue solver on a photonic quantum processor, Nat. Commun. **5**, 4213 (2014).

[3] E. Farhi, J. Goldstone, and S. Gutmann, A Quantum Approximate Optimization Algorithm, arXiv:1411.4028.

[4] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, Quantum circuit learning, Phys. Rev. A **98**, 032309 (2018).

[5] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, Nature (London) **549**, 242 (2017).

[6] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandaka, J. M. Chow, and J. M. Gambetta, Supervised learning with quantum-enhanced feature spaces, Nature (London) **567**, 209 (2019).

[7] Y. Li and S. C. Benjamin, Efficient Variational Quantum Simulator Incorporating Active Error Minimization, Phys. Rev. X **7**, 021050 (2017).

[8] K. Temme, S. Bravyi, and J. M. Gambetta, Error Mitigation for Short-Depth Quantum Circuits, Phys. Rev. Lett. **119**, 180509 (2017).

[9] S. Endo, S. C. Benjamin, and Y. Li, Practical Quantum Error Mitigation for Near-Future Applications, Phys. Rev. X **8**, 031027 (2018).

[10] V. N. Premakumar and R. Joynt, Error Mitigation in Quantum Computers subject to Spatially Correlated Noise, arXiv:1812.07076.

[11] X. Bonet-Monroig, R. Sagastizabal, M. Singh, and T. E. O'Brien, Low-cost error mitigation by symmetry verification, Phys. Rev. A **98**, 062339 (2018).

[12] J. Sun, X. Yuan, T. Tsunoda, V. Vedral, S. C. Benjamin, and S. Endo, Mitigating Realistic Noise in Practical Noisy Intermediate-Scale Quantum Devices, Phys. Rev. Applied **15**, 034026 (2021).

[13] X.-M. Zhang, W. Kong, M. U. Farooq, M.-H. Yung, G. Guo, and X. Wang, Generic detection-based error mitigation using quantum autoencoders, Phys. Rev. A **103**, L040403 (2021).

[14] A. Strikis, D. Qin, Y. Chen, S. C. Benjamin, and Y. Li, Learning-Based Quantum Error Mitigation, PRX Quantum **2**, 040330 (2021).

[15] P. Czarnik, A. Arrasmith, P. J. Coles, and L. Cincio, Error mitigation with Clifford quantum-circuit data, Quantum **5**, 592 (2021).

[16] A. Zlokapa and A. Gheorghiu, A deep learning model for noise prediction on near-term quantum devices, arXiv:2005.10811.

[17] K. Yeter-Aydeniz, R. C. Pooser, and G. Siopsis, Practical quantum computation of chemical and nuclear energy levels using quantum imaginary time evolution and Lanczos

algorithms, npj Quantum Information **6**, 63 (2020).

[18] B. Tan and J. Cong, Optimality Study of Existing Quantum Computing Layout Synthesis Tools, IEEE Transactions on Computers **70**, 1363 (2021).

[19] M. R. Perelshtein, A. I. Pakhomchik, A. A. Melnikov, A. A. Novikov, A. Glatz, G. S. Paraoanu, V. M. Vinokur, and G. B. Lesovik, Solving Large-Scale Linear Systems of Equations by a Quantum Hybrid Algorithm, Ann. Phys. 2200082 (2022).

[20] A. Kondratyev, Non-Differentiable Learning of Quantum Circuit Born Machine with Genetic Algorithm, Wilmott **2021**, 50 (2021).

[21] S. Dasgupta, K. E. Hamilton, and A. Banerjee, Characterizing the memory capacity of transmon qubit reservoirs, arXiv:2004.08240.

[22] L. M. Sager, S. E. Smart, D. A. Mazziotti, Preparation of an exciton condensate of photons on a 53-qubit quantum computer, Phys. Rev. Research **2**, 043205 (2020).

[23] J. R. Wootton, A quantum procedure for map generation, in *Proc. of the 2020 IEEE Conference on Games* (IEEE, Osaka, 2020), p. 73.

[24] W.-J. Huang, W.-C. Chien, C.-H. Cho, C.-C. Huang, T.-W. Huang, and C.-R. Chang, Mermin's inequalities of multiple qubits with orthogonal measurements on IBM Q 53-qubit system, Quantum Engineering **2**, e45 (2020).

[25] T. Morimae, Verification for measurement-only blind quantum computing, Phys. Rev. A **89**, 060302(R) (2014).

[26] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. **115**, 220502 (2015).

[27] T. Morimae, Measurement-only verifiable blind quantum computing with quantum input verification, Phys. Rev. A **94**, 042301 (2016).

[28] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, Interactive Proofs for Quantum Computations, arXiv:1704.04487.

[29] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A **96**, 012303 (2017).

[30] T. Morimae, Y. Takeuchi, and M. Hayashi, Verification of hypergraph states, Phys. Rev. A **96**, 062321 (2017).

[31] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, *Post hoc* Verification of Quantum Computation, Phys. Rev. Lett. **120**, 040501 (2018).

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

[33] A. Broadbent, How to Verify a Quantum Computation, Theory of Computing **14**, 11 (2018).

[34] U. Mahadev, Classical Verification of Quantum Computations, in *Proc. of the 59th Annual Symposium on Foundations of Computer Science* (IEEE, Paris, 2018), p. 259.

[35] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound, npj Quantum Information **5**, 27 (2019).

[36] M. Hayashi and Y. Takeuchi, Verifying commuting quantum computations via fidelity estimation of weighted graph states, New J. Phys. **21**, 093060 (2019).

[37] A. Gheorghiu and T. Vidick, Computationally-Secure and Composable Remote State Preparation, in *Proc. of the 60th Annual Symposium on Foundations of Computer Science* (IEEE, Baltimore, 2019), p. 1024.

[38] G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung, Non-interactive Classical Verification of Quantum Computation, in *Proc. of Theory of Cryptography Conference* (Springer, Virtual, 2020), p. 153.

[39] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, Phys. Rev. Applied **12**, 054047 (2019).

[40] N.-H. Chia, K.-M. Chung, and T. Yamakawa, Classical Verification of Quantum Computations with Efficient Verifier, in *Proc. of Theory of Cryptography Conference* (Springer, Virtual, 2020), p. 181.

[41] D. Markham and A. Krause, A Simple Protocol for Certifying Graph States and Applications in Quantum Networks, Cryptography **4**, 3 (2020).

[42] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[43] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, Journal of the ACM **56**, 34 (2009).

[44] If n-qubit quantum operations are allowed, the efficient verification is trivially possible. Let U be a unitary operator such that $|\psi_t\rangle = U|0^n\rangle$ for an ideal output state $|\psi_t\rangle$. We apply $U^\dagger$ to a received state $\hat{\rho}$ and measure all qubits in the computational basis. Then, by estimating the probability of 0^n being observed, we can estimate the fidelity $\langle 0^n|U^\dagger\hat{\rho}U|0^n\rangle$ between $|\psi_t\rangle$ and $\hat{\rho}$.

[45] For clarity, we use the notation $\hat{a}$ when the lowercase letter a is a quantum state or quantum operation. On the other hand, for any uppercase letter A, we omit $\hat{}$ even if A is a quantum state or quantum operation.

[46] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum, Phys. Rev. Lett. **70**, 1244 (1993).

[47] Z. Hradil, Quantum-state estimation, Phys. Rev. A **55**, R1561(R) (1997).

[48] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, Maximum-likelihood estimation of the density matrix, Phys. Rev. A **61**, 010304(R) (1999).

[49] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. **106**, 230501 (2011).

[50] S. Ferracin, T. Kapourniotis, and A. Datta, Accrediting outputs of noisy intermediate-scale quantum computing devices, New J. Phys. **21** 113038 (2019).

[51] S. Ferracin, S. T. Merkel, D. McKay, and A. Datta, Experimental accreditation of outputs of noisy quantum computers, Phys. Rev. A **104**, 042603 (2021).

[52] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, Verifying BQP Computations on Noisy Devices with Minimal Overhead, PRX Quantum **2**, 040302 (2021).

[53] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient Verification of Dicke States, Phys. Rev. Applied **12**, 044020 (2019).

[54] S. Bravyi, G. Smith, and J. A. Smolin, Trading Classical and Quantum Computational Resources, Phys. Rev. X **6**, 021043 (2016).

[55] T. Peng, A. Harrow, M. Ozols, and X. Wu, Simulating Large Quantum Circuits on a Small Quantum Computer, Phys. Rev. Lett. **125**, 150504 (2020).

[56] D. Aharonov, A. Kitaev, and N. Nisan, Quantum Circuits with Mixed States, in *Proc. of the 30th Annual ACM Symposium on Theory of Computing* (ACM, Dallas, 1998), p. 20.

[57] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).

[58] M. Fanciulli, ed., *Electron Spin Resonance and Related Phenomena in Low-Dimensional Structures* (Springer, Berlin, 2009).

[59] W. Hoeffding, Probability Inequalities for Sums of Bounded Random Variables, Journal of the American Statistical Association **58**, 13 (1963).

[60] K. Li and G. Smith, Quantum de Finetti Theorem under Fully-One-Way Adaptive Measurements, Phys. Rev. Lett. **114**, 160503 (2015).

[61] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung,

M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, Nature (London) **574**, 505 (2019).

[62] R. J. Lipton and R. E. Tarjan, A Separator Theorem for Planar Graphs, SIAM J. Appl. Math. **36**, 177 (1979).

[63] R. J. Lipton and R. E. Tarjan, Applications of a Planar Separator Theorem, SIAM J. Comput. **9**, 615 (1980).

[64] K. Fujii, K. Mizuta, H. Ueda, K. Mitarai, W. Mizukami, Y. O. Nakagawa, Deep Variational Quantum Eigensolver: A Divide-And-Conquer Method for Solving a Larger Problem with Smaller Size Quantum Computers, PRX Quantum **3**, 010346 (2022).

[65] W. Tang, T. Tomesh, M. Suchara, J. Larson, and M. Martonosi, CutQC: using small Quantum computers for large Quantum circuit evaluations, in *Proc. of the 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (ACM, Virtual, 2021), p. 473.

[66] K. Mitarai and K. Fujii, Constructing a virtual two-qubit gate by sampling single-qubit operations, New J. Phys. **23**, 023021 (2021).

[67] K. Mitarai and K. Fujii, Overhead for simulating a non-local channel with local channesl by quasiprobability sampling, Quantum **5**, 388 (2021).

[68] M. A. Perlin, Z. H. Saleem, M. Suchara, and J. C. Osborn, Quantum circuit cutting with maximum-likelihood tomography, npj Quantum Information **7**, 64 (2021).

[69] T. Ayral, F.-M. L Régent, Z. Saleem, Y. Alexeev, and M. Suchara, Quantum Divide and Compute: Hardware Demonstrations and Noisy Simulations, in *Proc. of the 2020 IEEE Computer Society Annual Symposium on VLSI* (IEEE, Limassol, 2020), p. 138.

A Estimation of the real part of Eq. (6)

In this appendix, we show that the mean value of α converges to the real part of Eq. (6). Note that for simplicity, we write $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}')$ by α. By using the spectral decomposition, we write $\hat{\rho}_{\rm out} = \sum_{i=1}^{2^n} p_i|\psi_i\rangle\langle\psi_i|$, where p_i is a non-negative real number for any i, and $\sum_{i=1}^{2^n} p_i = 1$. Therefore, the mean value $\mathbb{E}[\alpha \mid |0\rangle\langle 0| \otimes \hat{\rho}_{\rm out}]$ with the input state $|0\rangle\langle 0| \otimes \hat{\rho}_{\rm out}$ is written as $\sum_{i=1}^{2^n} p_i \mathbb{E}[\alpha \mid |0\rangle|\psi_i\rangle]$.

We explicitly calculate $\mathbb{E}[\alpha \mid |0\rangle|\psi_i\rangle]$. The quantum state immediately before the measurements in Fig. 4 (a) is

$$|\phi\rangle = \frac{|+\rangle \otimes Q_{\mathbf{i},\mathbf{j}}|\psi_i\rangle + |-\rangle \otimes Q_{\mathbf{i}',\mathbf{j}'}|\psi_i\rangle}{\sqrt{2}}$$

with $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. Remember that $\alpha = 1$ if and only if $\oplus_{i=1}^n z_i k_i = \mathbf{i}\cdot\mathbf{j} \oplus \mathbf{i}'\cdot\mathbf{j}' \oplus b$. We separately consider the cases of $b = 0$ and $b = 1$. The probability P_1 of obtaining $b = 0$ and $\mathbf{z}$ such that $\oplus_{i=1}^n z_i k_i = \mathbf{i}\cdot\mathbf{j} \oplus \mathbf{i}'\cdot\mathbf{j}'$ is

$$P_1 = \langle\phi| \left(|0\rangle\langle 0| \otimes \frac{I^{\otimes n} + (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} \prod_{i=1}^n Z_i^{k_i}}{2} \right) |\phi\rangle.$$

On the other hand, the probability P_2 of obtaining $b = 1$ and $\mathbf{z}$ such that $\oplus_{i=1}^n z_i k_i \neq \mathbf{i}\cdot\mathbf{j} \oplus \mathbf{i}'\cdot\mathbf{j}'$ is

$$P_2 = \langle\phi| \left(|1\rangle\langle 1| \otimes \frac{I^{\otimes n} - (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} \prod_{i=1}^n Z_i^{k_i}}{2} \right) |\phi\rangle.$$

By a straightforward calculation,

$$P_1 + P_2 = \frac{1 + (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} {\rm Re}\left[\langle\psi_i| Q_{\mathbf{i},\mathbf{j}}^\dagger \left(\prod_{i=1}^n Z_i^{k_i} \right) Q_{\mathbf{i}',\mathbf{j}'} |\psi_i\rangle \right]}{2},$$

where ${\rm Re}[c]$ represents the real part of the complex number c. Therefore,

$$\begin{aligned} \mathbb{E}[\alpha \mid |0\rangle|\psi_i\rangle] &= (P_1 + P_2)\cdot 1 + (1 - P_1 - P_2)\cdot(-1) \\ &= 2(P_1 + P_2) - 1 \\ &= (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} {\rm Re}\left[\langle\psi_i| Q_{\mathbf{i},\mathbf{j}}^\dagger \left(\prod_{i=1}^n Z_i^{k_i} \right) Q_{\mathbf{i}',\mathbf{j}'} |\psi_i\rangle \right]. \end{aligned} \tag{15}$$

From Eq. (15), the mean value $\mathbb{E}[\alpha \mid |0\rangle\langle 0| \otimes \hat{\rho}_{\rm out}]$ with the input state $|0\rangle\langle 0| \otimes \hat{\rho}_{\rm out}$ converges to

$$\sum_{i=1}^{2^n} p_i \mathbb{E}[\alpha \mid |0\rangle|\psi_i\rangle] = (-1)^{\mathbf{i}\cdot\mathbf{j}+\mathbf{i}'\cdot\mathbf{j}'} {\rm Re}\left[{\rm Tr}\left[\hat{\rho}_{\rm out} \left[Q_{\mathbf{i},\mathbf{j}}^\dagger \left(\prod_{i=1}^n Z_i^{k_i} \right) Q_{\mathbf{i}',\mathbf{j}'} \right] \right] \right].$$

B Conversion from Fig. 4 (b) to (c)

In this appendix, we show that $\sum_{\mathbf{l}\in\{0,1\}^3} \beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})/2$ converges to the real part of Eq. (6). Let $U \equiv \Lambda(V_{\mathbf{i}'}^\dagger) X \Lambda(V_{\mathbf{i}}^\dagger) X H$ and $V \equiv H \Lambda(W_{\mathbf{j}'}^\dagger) X \Lambda(W_{\mathbf{j}}^\dagger) X$, where $\Lambda(Q) \equiv |0\rangle\langle 0| \otimes I^{\otimes n'} + |1\rangle\langle 1| \otimes Q$ for any n'-qubit unitary Q and any natural number n'. For simplicity, we define super-operators $\mathcal{U}(\cdot) \equiv U(\cdot)U^\dagger$ and $\mathcal{V}(\cdot) \equiv V(\cdot)V^\dagger$. We also define $\Pi_{\alpha=1}$ and $\Pi_{\alpha=-1}$ as projectors onto the space satisfying $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}') = 1$ and $\alpha(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}') = -1$, respectively. From them, we can define an observable $A \equiv \Pi_{\alpha=1} - \Pi_{\alpha=-1}$.

By using the above definitions, from Appendix A, the real part of Eq. (6) can be written as

$${\rm Tr}[A\mathcal{V}\mathcal{U}(|0\rangle\langle 0| \otimes \hat{\rho}_{\rm out})]. \tag{16}$$

Since any quantum state can be expanded by Pauli operators,

$$\begin{aligned}\mathcal{U}(|0\rangle\langle 0|\otimes\hat{\rho}_{\rm out}) &= (\mathcal{U}\otimes\mathcal{I}^{\otimes n-m})(|0\rangle\langle 0|\otimes\hat{\rho}_{\rm out})\\ &= \sum_{i=1}^{4}\sum_{j=1}^{4^m}\sum_{k=1}^{4^{n-m}} c_{ijk}(\hat{\sigma}_i\otimes\hat{\tau}_j\otimes\hat{\chi}_k),\end{aligned} \tag{17}$$

where $\mathcal{I}(\cdot)=I(\cdot)I$, c_{ijk} is a real number, and $\hat{\sigma}_i$, $\hat{\tau}_j$, and $\hat{\chi}_k$ are 1-, m-, and $(n-m)$-qubit Pauli operators, respectively. Furthermore, for any $\hat{\sigma}_i$, we utilize the well-known equality

$$\hat{\sigma}_i = \frac{{\rm Tr}[\hat{\sigma}_i]I + {\rm Tr}[\hat{\sigma}_i X]X + {\rm Tr}[\hat{\sigma}_i Y]Y + {\rm Tr}[\hat{\sigma}_i Z]Z}{2}, \tag{18}$$

where Y is the Pauli-Y gate. From Eqs. (17) and (18), Eq. (16) is rewritten as

$$\begin{aligned}\sum_{i=1}^{4}\sum_{j=1}^{4^m}\sum_{k=1}^{4^{n-m}}\frac{c_{ijk}}{2}\{&{\rm Tr}[\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|0\rangle\langle 0|\otimes\hat{\chi}_k)]] + {\rm Tr}[\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|1\rangle\langle 1|\otimes\hat{\chi}_k)]]\\ &+{\rm Tr}[X\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|+\rangle\langle +|\otimes\hat{\chi}_k)]] - {\rm Tr}[X\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|-\rangle\langle -|\otimes\hat{\chi}_k)]]\\ &+{\rm Tr}[Y\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|+i\rangle\langle +i|\otimes\hat{\chi}_k)]] - {\rm Tr}[Y\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|-i\rangle\langle -i|\otimes\hat{\chi}_k)]]\\ &+{\rm Tr}[Z\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|0\rangle\langle 0|\otimes\hat{\chi}_k)]] - {\rm Tr}[Z\hat{\sigma}_i\otimes A[\hat{\tau}_j\otimes\mathcal{V}(|1\rangle\langle 1|\otimes\hat{\chi}_k)]]\},\end{aligned}$$

where $|\pm\rangle\equiv(|0\rangle\pm|1\rangle)/\sqrt{2}$ and $|\pm i\rangle\equiv(|0\rangle\pm i|1\rangle)/\sqrt{2}$.

By using Eq. (7), the above formula can be concisely represented by

$$\begin{aligned}&\sum_{\mathbf{l}=000,001}\frac{{\rm Tr}[(I\otimes A)[\mathcal{U}\otimes\mathcal{V}'(|0\rangle\langle 0|\otimes\hat{\rho}_{\rm out}\otimes C_{\mathbf{l}}|0\rangle\langle 0|C_{\mathbf{l}}^\dagger)]]}{2}\\ &+\sum_{\mathbf{l}\neq 000,001}\frac{{\rm Tr}[(C_{\mathbf{l}}ZC_{\mathbf{l}}^\dagger\otimes A)[\mathcal{U}\otimes\mathcal{V}'(|0\rangle\langle 0|\otimes\hat{\rho}_{\rm out}\otimes C_{\mathbf{l}}|0\rangle\langle 0|C_{\mathbf{l}}^\dagger)]]}{2}\\ &=\frac{1}{2}\sum_{\mathbf{l}\in\{0,1\}^3}\mathbb{E}\left[\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})\mid\ |0\rangle\langle 0|\otimes\hat{\rho}_{\rm out}\otimes|0\rangle\langle 0|\right],\end{aligned}$$

where $\mathcal{V}'\equiv V'(\cdot)V'^\dagger$, and $V'=U_{\rm perm}^\dagger V U_{\rm perm}$ with the permutation gate $U_{\rm perm}$ shifting the ith qubit to the $(i+1 \pmod{n-m+1})$th one for $1\le i\le n-m+1$ (see also Fig. 4 (c)). Note that the term $(-1)^{(1+\delta_{l_1,0}\delta_{l_2,0})o}$ in the definition of $\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})$ means that when $\mathbf{l}=000$ or 001, we ignore the measurement outcome o. This concludes that $\sum_{\mathbf{l}\in\{0,1\}^3}\beta(\mathbf{i},\mathbf{j},\mathbf{i}',\mathbf{j}',\mathbf{l})/2$ converges to the real part of Eq. (6).

C Experimental data

In this appendix, we give the data obtained from our experiment on the IBM Manila 5-qubit chip. This chip is represented by a one-dimensional graph with five vertices. We have used four qubits labeled by $Q0$, $Q1$, $Q2$, and $Q3$ and have performed the experiment in 30th April 2022.

For all $i,j\in\{0,1\}$ and $\mathbf{l}\in\{0,1\}^3$, we run simplified quantum circuits of those in Fig. 4 (c) and obtain measurement outcomes $(b,z_2,z_1,o)\in\{0,1\}^4$, where z_1 and z_2 are the 1st and 2nd bits of $\mathbf{z}$, respectively. The experimental results are summarized in Fig. 6. For comparison, we also directly estimate ${\rm Re}[{\rm Tr}[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}]]$ for $\mathbf{k}\in\{01,10,11\}$. The experimental results and quantum circuits used to obtain them are given in Figs. 7 (b) and (a), respectively.

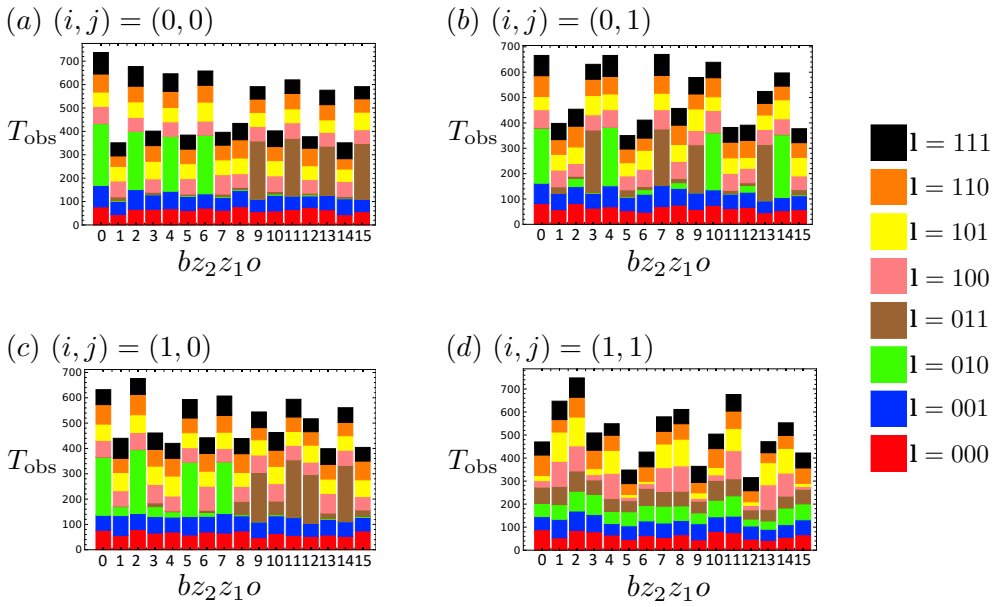

Figure 6: Experimental results of our method performed on the IBM Manila 5-qubit chip. $T_{\rm obs}$ counts how many times each of bz_2z_1o is observed. The labels of the horizontal axis denote the decimal numbers of bz_2z_1o, i.e., the values of $8b+4z_2+2z_1+o$. Note that since the circuits in the case of $\mathbf{l}=000$ and $\mathbf{l}=110$ are the same, we obtain $\beta'_k(i,j,0,0,000)$ and $\beta'_k(i,j,0,0,110)$ from the same experimental data. The same applies to the case of $\mathbf{l}=001$ and $\mathbf{l}=111$.

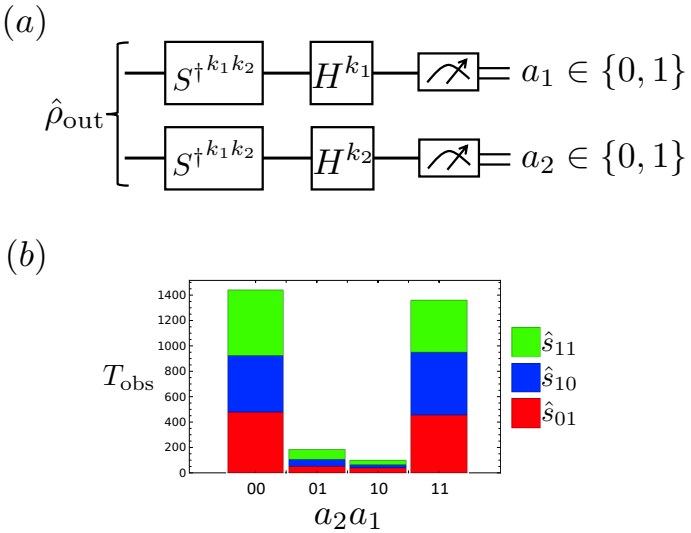

Figure 7: Quantum circuits used to directly estimate $\mathrm{Re}[\mathrm{Tr}[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}]]$ for $\mathbf{k}\in\{01,10,11\}$ and their measurement outcomes. (a) $S^\dagger\equiv|0\rangle\langle 0|-i|1\rangle\langle 1|$, and k_1 and k_2 are the 1st and 2nd bits of $\mathbf{k}$, respectively. Let $\gamma(a_1,a_2)\in\{1,-1\}$ be a random variable such that $\gamma(a_1,a_2)=1$ if and only if $a_1=a_2$. Since the expected value of $\gamma(a_1,a_2)$ is $\mathrm{Re}[\mathrm{Tr}[\hat{\rho}_{\rm out}\hat{s}_{\mathbf{k}}]]$, it can be estimated from a_1 and a_2. (b) We run the quantum circuit in (a) 1024 times for each $\mathbf{k}\in\{01,10,11\}$. As a result, we obtain this histogram. $T_{\rm obs}$ counts how many times each of a_2a_1 is observed.