

Received: 18 April 2019 Accepted: 22 August 2019

Published online: 19 September 2019

OPEN Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements

Yuki Takeuchi¹, Tomoyuki Morimae^{2,3} & Masahito Hayashi^{4,5,6}

Measurement-based quantum computing is one of the most promising quantum computing models. Although various universal resource states have been proposed so far, it was open whether only two Pauli bases are enough for both of universal measurement-based quantum computing and its verification. In this paper, we construct a universal hypergraph state that only requires X and Z-basis measurements for universal measurement-based quantum computing. We also show that universal measurement-based quantum computing on our hypergraph state can be verified in polynomial time using only X and Z-basis measurements. Furthermore, in order to demonstrate an advantage of our hypergraph state, we construct a verifiable blind quantum computing protocol that requires only X and Z-basis measurements for the client.

Quantum computing is believed to solve several problems faster than classical computing 1-3. Toward realizations of universal quantum computers, several quantum computing models have been proposed, such as the quantum circuit model⁴, adiabatic quantum computing⁵, measurement-based quantum computing (MBQC)^{6,7}, and topological quantum computing. Among these, MBQC is one of the most promising models. In MBQC, quantum computing proceeds via adaptive single-qubit measurements on a highly entangled state, a so-called universal resource state. This important advantage of MBQC, namely, the fact that all multi-qubit operations can be done offline, fits MBQC to several physical systems such as photons^{9,10}, cold atoms¹¹, ion traps¹², and superconducting circuits¹³.

Finding fewer and simpler measurement bases is essential for realizations of MBQC, because measurements are only online operations. Furthermore, when MBQC is applied to cloud (blind) quantum computing 14, fewer and simpler measurement bases are more desirable for the client, who securely delegates his/her quantum computing to a remote quantum server.

In this paper, we propose a universal hypergraph state that only needs Pauli-X and Z basis measurements (for the definition of hypergraph states, see the "Hypergraph states" subsection in the Results section). Several previous universal resource states are summarized in Table 1. We can see that except for the Mølmer-Sørensen graph state 15, all previous universal resource states in Table 1 need at least three measurement bases. Our resource state is better than these resource states in the sense that our resource state only needs two Pauli-measurement bases. Although the Mølmer-Sørensen graph state also achieves two Pauli-measurement bases, i.e. Pauli X and Z bases, an important advantage of our universal resource state is that it is efficiently verifiable with only Pauli-X and Z basis measurements: we can check whether a given state is close to the ideal resource state or not by measuring each qubit in the X or Z basis (for details, see the "Verification of our universal hypergraph state" subsection in the Results section). The Mølmer-Sørensen graph state is, on the other hand, not known to be efficiently verifiable using only Pauli-X and Z basis measurements. More precisely, if other additional bases than the X and Z bases are allowed, weighted graph states are efficiently verifiable 16. These additional bases should be necessary.

¹NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa, 243-0198, Japan. ²Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto, 606-8502, Japan. ³JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan. ⁴Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan. ⁵Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055, China. 6Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore, 117543, Singapore. Correspondence and requests for materials should be addressed to Y.T. (email: yuki.takeuchi.yt@hco.ntt.co.jp) or T.M. (email: tomoyuki.morimae@yukawa.kyoto-u.ac.jp) or M.H. (email: masahito@math.naqoya-u.ac.jp)

| Resource state | Measurement basis | Class |
|---|----------------------------------|----------------------|
| Cluster state ³⁷ | X, Y, TXT ^{†38} | graph state |
| Brickwork state ⁴⁰ | $X, Y, TXT^{\dagger_{40}}$ | graph state |
| Triangular lattice state ⁴¹ | X, Z, H, XHX ⁴¹ | graph state |
| Raussendorf-Harrington-Goyal (RHG) lattice ^{42,43} | $X, Y, Z, TXT^{\dagger_{43,44}}$ | graph state |
| Decorated RHG lattice ⁴⁵ | X, Y, TXT ^{†45} | graph state |
| Affleck-Kennedy-Lieb-Tasaki (AKLT) state ^{46,47} | qutrit bases ⁴⁷ | matrix-product state |
| Union Jack state ³³ | X, Y, Z^{33} | hypergraph state |
| Three-uniform hypergraph state ³⁶ | X, Y, Z^{36} | hypergraph state |
| Mølmer-Sørensen graph state ¹⁵ | X, Z^{15} | weighted graph state |
| Our state | X, Z | hypergraph state |

Table 1. Required measurement bases for various universal resource states of MBQC. Here, $H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$ and $T \equiv |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. Operators X, Y, and Z are Pauli-X, Y, and Z operators, respectively. Hypergraph states are generalizations of graph states (for details, see the "Hypergraph states" subsection in the Results section). Weighted graph states are other generalizations of graph states³⁹.

This is because the stabilizer operators of weighted graph states are not linear combinations of tensor products of X and Z with real coefficients, and checking stabilizers seems to be the only way of efficiently verifying weighted graph states.

In summary, our universal resource state achieves both the universality and the verifiability at the same time with only X and Z-basis measurements. This result should also be contrasted with the graph state case: the verification of graph states can be done with only X and Z-basis measurements^{17–19}, but when we do MBQC on a graph state, an extra non-Clifford basis measurement is necessary due to the Gottesman-Knill theorem.

Our universal hypergraph state, which we denote $|G_n^d\rangle$, can simulate any n-qubit quantum circuit of depth d consisting of the Hadamard gate $H \equiv |+\rangle\langle 0|+|-\rangle\langle 1|$ and the controlled-controlled-Z (CCZ) gate $CCZ \equiv I^{\otimes 3} - 2|111\rangle\langle 111|$ with only adaptive X and Z-basis measurements, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$, and I is the two-dimensional identity gate. Since the gate set $\{H,CCZ\}$ is universal $[0,0]^2$, our state $[0,0]^2$ is a universal resource state. Our universal resource state $[0,0]^2$ is constructed in the following three steps. First, we define a hypergraph state $[0,0]^2$ that can simulate any three-qubit quantum circuit of depth one consisting of I and I and I and I and I is entangling the I mypergraph states I and I is entangling the I mypergraph states I and I is entangling the I mypergraph state I and I is entangling the I mypergraph states I and I is entangling the I mypergraph states I is entangling the I mypergraph states I in the proof of universality, we only use basic techniques of MBQC: an I-basis measurement teleports a qubit (up to an Hadamard gate), and a I-basis measurement decouples a qubit.

Note that in this paper we require that a resource state is a fixed state independent of the quantum circuit that we want to implement, because otherwise we cannot enjoy the advantage of MBQC. For example, universal quantum computing is possible with X and Z-basis measurements on Feynman-Kitaev history states^{21–23}. However, they cannot be generated before the quantum circuit is fixed. (More trivially, no measurement is required to simulate a quantum circuit U if our "resource state" is $U|0\rangle^{\otimes n}$).

Furthermore, in order to demonstrate an advantage of our hypergraph state, we propose a verifiable blind quantum computing (VBQC) protocol in which the client only needs X and Z-basis measurements. In VBQC, a client with computationally weak quantum devices delegates universal quantum computing to a remote quantum server in such a way that the client's privacy (input, algorithm, and output) is information-theoretically protected and at the same time the honesty of the server is verifiable. In the original proposal of VBQC²⁴, the client has to prepare ten kinds of single-qubit states at the server's side. Although this requirement for the client has already been reduced to the X and Z-basis measurements in ref.²⁵, our VBQC protocol is much simpler than it (for details, see the "Application" subsection in the Results section). The reduction of the number of measurement bases required for MBQC and its verification would be a plausible way to ease the client's burden in the sense that it seems to be impossible to make the client of VBQC completely classical as long as we require the information-theoretical security^{26–28}.

Results

This section is organized as follows: first, as preliminaries, we review the definition of hypergraph states. Second, as the main result, we construct the universal hypergraph state that enables universal quantum computing with X and Z-basis measurements. Third, we discuss the verifiability of our hypergraph state without assuming any i.i.d. property. Finally, we propose the VBQC protocol using our hypergraph state.

Hypergraph states. In this subsection, we review the definition of hypergraph states²⁹.

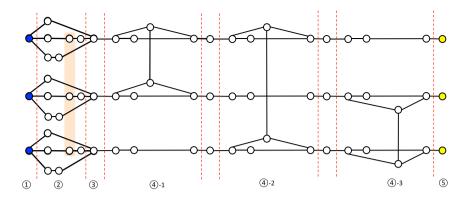


Figure 1. The hypergraph G_3^1 to define the hypergraph state $|G_3^1\rangle$ simulating any quantum circuit of depth one consisting of H and CCZ on three input qubits. The orange rectangle represents a hyperedge connecting three vertices, which corresponds to the CCZ gate. The black lines represent edges connecting two vertices, which correspond to the CZ gates. The hypergraph G_3^1 has 66 vertices and is separated into five regions. In addition, the fourth region is also separated into three parts. Each circled number represents the number of each region. Since input (blue) and output (yellow) qubits are prepared in the first and the fifth regions, we call them the input and output regions, respectively. For example, if we simulate the CCZ gate using $|G_3^1\rangle$, the three input qubits corresponding to three blue vertices are finally teleported to three output qubits corresponding to three yellow vertices while CCZ is applied.

Definition 1 (**Hypergraph states**) Let $G \equiv (V, E)$ be a hypergraph, i.e. a pair of a set V of vertices and a set E of hyperedges, where the number |V| of vertices is n. A hyperedge is a set of vertices. A hypergraph state $|G\rangle$ corresponding to G is defined as

$$|G\rangle \equiv \left(\prod_{e \in E} \tilde{CZ}_e\right)| + \rangle^{\otimes n},$$

where each $|+\rangle$ state is placed on each vertex,

$$\widetilde{CZ}_e \equiv \underset{i \in e}{\otimes} I_i - 2 \underset{i \in e}{\otimes} |1\rangle\langle 1|_i$$

is the generalized controlled-Z (CZ) gate acting on vertices in the hyperedge e, and I_i is the two-dimensional identity gate on the ith qubit.

Note that in this paper, we only consider hypergraph states satisfying $2 \le |e| \le 3$ for all $e \in E$, where |e| is the number of vertices in the hyperedge e, because such a restriction is enough for the construction of our hypergraph state. When |e| = 2 and 3, the generalized CZ gate becomes the conventional CZ gate $CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$ and the CCZ gate, respectively. Since the CCZ gate is a non-Clifford operation, hypergraph states are out of the application range of the Gottesman-Knill theorem.

Pauli-X and Z universal hypergraph state. In this subsection, we give an intuitive idea of how to construct the hypergraph state $|G_n^d\rangle$ that enables n-qubit d-depth universal quantum computing with only adaptive X and Z-basis measurements. First, we construct a small hypergraph state $|G_3^1\rangle$ that can simulate one-depth quantum computing on three input qubits. Second, by entangling the $m=\binom{n}{3}$ small hypergraph states $|G_3^1\rangle^{\otimes m}$ and several single- and two-qubit states, we construct another hypergraph state $|G_n^1\rangle$ that can simulate one-depth quantum computing on n input qubits. Finally, by entangling the d hypergraph states $|G_n^1\rangle^{\otimes d}$ and several single-qubit states, we define the target hypergraph state $|G_n^d\rangle$ on poly (n,d) qubits that can simulate d-depth quantum computing on n input qubits. That is, our hypergraph state $|G_n^d\rangle$ realizes universal quantum computing only with N and N-basis measurements.

A hypergraph state for one-depth quantum computing on three input qubits. To simulate one-depth quantum computing on three input qubits, we define the hypergraph state $|G_3^1\rangle$ on 66 qubits, based on the hypergraph G_3^1 defined in Fig. 1. It satisfies the following theorem:

Theorem 1 The hypergraph state $|G_3^1\rangle$ defined by Fig. 1 can simulate any quantum circuit of depth one consisting of H and CCZ on three input qubits with adaptive X and Z-basis measurements.

Proof. Our idea is that we embed all nine patterns, $H^a \otimes H^b \otimes H^c$ and CCZ, where $a, b, c \in \{0, 1\}$, of applying quantum gates into the hypergraph state $|G_3^1\rangle$ and then select one pattern by adaptive X and Z-basis measurements. Below, we show Theorem 1 according to two steps.

Step 1: Simulation of *H* and *CCZ* up to byproducts.

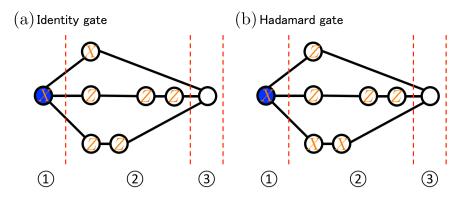


Figure 2. Measurement patterns to realize single-qubit operations. This figure shows a graph state and the measurement patterns on the graph state. *X* and *Z* represent the *X* and *Z*-basis measurements, respectively. (a) The measurement pattern for the identity operator. (b) The measurement pattern for the Hadamard gate.

The first region in Fig. 1 corresponds to three input qubits. The second region corresponds to the one-depth quantum computation. In MBQC, by measuring a qubit whose state is $|\psi\rangle$ in the X basis, $|\psi\rangle$ is teleported to a neighboring qubit connected to the measured qubit while H is applied on $|\psi\rangle$. In other words, the state of the neighboring qubit becomes $H|\psi\rangle$ up to a Pauli byproduct. On the other hand, by measuring a qubit in the Z basis, we can decouple the qubit from other qubits. In this proof, we use these two properties of MBQC.

First, we explain how to perform a tensor product of single qubit operations, i.e. H_i ($i \in \{1, 2, 3\}$), $H_j \otimes H_k$ ((j, k) $\in \{(1, 2), (1, 3), (2, 3)\}$), or $H_1 \otimes H_2 \otimes H_3$ (Remember that we now focus on the universal gate set $\{H, CCZ\}$). These operations can be realized by the combination of the Hadamard gates and the identity operators. In Fig. 2, we give the explicit measurement patterns to realize these two operations. We choose a single path by the X-basis measurements, and delete other two paths by the Z-basis measurements. Consider for instance applying $H \otimes H \otimes I$ on input qubits $|+\rangle^{\otimes 3}$. In this case, for the first and the second input qubits, we select the lower paths. For the third input qubit, we select the upper path. As a result, from the two properties of MBQC, $(H \otimes H \otimes I)|+\rangle^{\otimes 3}$ is prepared in the third region up to byproducts. Since the byproducts are tensor products of X and X, we can remove its effect by adapting following single-qubit measurement directions.

However, when we simulate CCZ, byproducts include the CZ gates, because $X_i(CCZ_{ijk})X_i = CCZ_{ijk}CZ_{jk}$. In order to simulate CCZ, we measure qubits in the first and the second regions following the measurement pattern in Fig. 3. This measurement pattern corresponds to select the middle paths for all input qubits. As a result, the state of qubits in the third region becomes $CCZ|+\rangle^{\otimes 3}$ up to byproducts including CZ gates. Since CZ is not a single-qubit Pauli operation, we have to correct it.

Step 2: Correction of nonlocal byproducts caused by applying a *CCZ*.

In order to correct CZ gates, we use qubits in the fourth region in Fig. 1. Note that Pauli byproducts do not have to be corrected at this time because they can be accounted by adapting following single-qubit measurement directions. In the fourth region, we again use X and Z-basis measurements to realize gate teleportations and decoupling. Now, as a byproduct, there are three kinds of CZ gates, i.e. CZ_{12} , CZ_{13} , and CZ_{23} . The three parts of the fourth region are prepared to correct each of them. In the first part of the fourth region, there are two paths for the first and the second input qubits. If qubits in the upper paths are measured in the X basis and other two qubits in the lower paths are measured in the Z basis, CZ is applied on the first and the second input qubits. In other words, we can correct the byproduct CZ_{12} . On the other hand, if we do not want to apply the CZ_{12} , we select the lower paths, i.e. measure qubits in lower and upper paths in the X basis and the Z basis, respectively. With respect to the third input qubit, by measuring qubits in the X basis, the state in the third region is teleported to the region between the first and the second parts of the fourth region. The same argument holds for the second and the third parts of the fourth region to correct CZ_{13} and CZ_{23} . Finally, the output quantum state is teleported in the fifth region up to Pauli byproducts. Therefore, we can simulate any quantum circuit of depth one consisting of H and CCZ on three input qubits using the hypergraph state $|G_3^1\rangle$ defined by Fig. 1.

A hypergraph state for one-depth quantum computing on n input qubits. In this subsection, based on the hypergraph state $|G_3^1\rangle$ given in the previous subsection, we construct another hypergraph state $|G_n^1\rangle$ that can simulate one-depth quantum computing on n input qubits. Before explaining the general construction of $|G_n^1\rangle$ for any n, here we explain our basic idea with a simple example of n=4. When n=4, one-depth quantum computing means that we can apply H_i $(1 \le i \le 4)$, $H_i \otimes H_j$ $(1 \le i < j \le 4)$, $H_i \otimes H_j \otimes H_k$ $(1 \le i < j < k \le 4)$, $H_1 \otimes H_2 \otimes H_3 \otimes H_4$, CCZ_{ijk} $(1 \le i < j < k \le 4)$, or $CCZ_{ijk} \otimes H_l$ $(1 \le i < j < k \le 4)$, $I_i \otimes I_j \otimes I_$

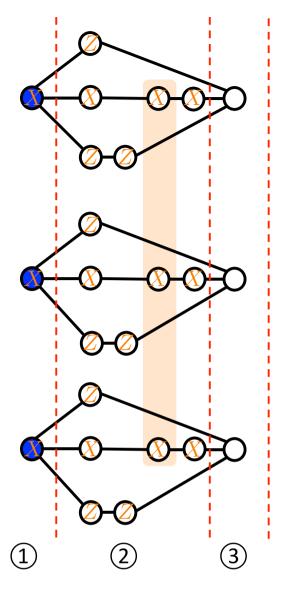


Figure 3. The measurement pattern to realize the *CCZ* gate up to nonlocal byproducts (*CZ* gates).

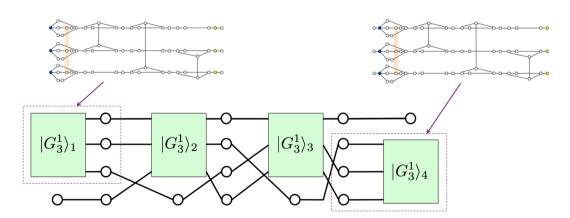


Figure 4. The hypergraph G_4^1 to define the hypergraph state $|G_4^1\rangle$ that enables one-depth quantum computing on four input qubits using X and Z-basis measurements. Each rectangle represents the hypergraph G_3^1 defined in Fig. 1.

measurements. Therefore, the hypergraph state $|G_4^1\rangle$ defined by Fig. 4 enables one-depth quantum computing on four input qubits with X and Z-basis measurements.

For general n, we apply the same idea as the case of n=4. Using the $m=\binom{n}{3}$ hypergraph states $|G_3^1\rangle^{\otimes m}$, we define the hypergraph state $|G_n^1\rangle$ on $(2n+63)\binom{n}{3}-n$ qubits as follows:

Definition 2 The hypergraph state $|G_n^1\rangle$ is the state constructed in the following three steps (see Fig. 5):

Step 1. Prepare m states, 3(m-2)+n states, and (n-3) (m-1) states in $|G_3^1\rangle$, $|+\rangle$, and $|\Phi^+\rangle \equiv CZ|+\rangle^{\otimes 2}$, respectively. Here, $m=\binom{n}{3}$.

Step 2. Let $|G_3^1\rangle_i$ be the i-th $|G_3^1\rangle$ ($1 \le i \le m$). Apply the CZ gate on each qubit in the fifth region of $|G_3^1\rangle_i$ and $|+\rangle$, where $1 \le j \le m-1$. For the definition of the region of $|G_3^1\rangle$, see Fig. 1.

Step 3. For all (i, j, k) $(1 \le i < j < k \le n)$ except for (i, j, k) = (1, 2, 3) and (n - 2, n - 1, n), apply the CZ gates on the i-th, j-th, and k-th qubits in the final layer of the k-th $(t \ge 1)$ group and the first, second, and third qubits in the first region of $|G_3^1\rangle_{t+1}$, respectively, where

$$t = \left(\sum_{s=0}^{i-1}\sum_{l=2}^{n-1}n-l-s+1\right) + \left(\sum_{l=1}^{j-i}n-l-i+1\right) + k-j - \frac{(n+1)(n-2)}{2} - n+i-1.$$
(1)

Note that the above operations are done such that the w-th $(1 \le w \le n)$ qubit from the top in the final layer of the t-th group is connected to that in the final layer of the (t+1)-th group via $|G_3^1\rangle_{t+1}$. In addition, if $t \ne m-1$, apply the CZ gate on each other qubit (qubits except for the i-th, j-th, and k-th ones) in the final layer of the t-th group and a left qubit of $|\Phi^+\rangle$ in the (t+1)-th group. Here, the left qubit denotes a qubit that is not in the final layer. On the other hand, if t = m-1, apply the CZ gate on each other qubit in the final layer of the (m-1)-th group and $|+\rangle$ in the m-th group.

The derivation of Eq. (1) is given in the Methods section. In Definition 2, when n=4, (i,j,k) can be equal to (1,2,4), (1,3,4), and (2,3,4). For each value, t=1,2, and 3, respectively. Therefore, in this case, $|G_n^1\rangle$ indeed becomes the hypergraph state corresponding to G_4^1 shown in Fig. 4. In addition, since $|G_3^1\rangle$ is composed of 66 qubits, from Definition 2, we can calculate the number of qubits in $|G_n^1\rangle$ as follows:

$$66\binom{n}{3} + 2(n-3)\binom{n}{3} - 1 + 3\binom{n}{3} - 2 + n = (2n+63)\binom{n}{3} - n.$$
 (2)

The hypergraph state $|G_n^1\rangle$ satisfies the following corollary:

Corollary 1 The hypergraph state $|G_n^1\rangle$ in Definition 2 can simulate any quantum circuit of depth one consisting of H and CCZ on n input qubits with adaptive X and Z-basis measurements.

Proof. In our construction, any triple of input qubits are connected via $|G_3^1\rangle$. More precisely, for any (i, j, k) except for (1, 2, 3), there exists a single t ($1 \le t \le m-1$) such that the ith, jth, and kth qubits from the top in the final layer of the tth group are simultaneously connected to $|G_3^1\rangle_{t+1}$. Note that the triple (1, 2, 3) is already simultaneously connected in $|G_3^1\rangle_1$ using the CCZ gate. Such the t is uniquely identified by Eq. (1). As an example, let us consider again the case of n=4. The triple (i,j,k) can be chosen from (1,2,4), (1,3,4), and (2,3,4). As shown in Fig. 4, these three triples are connected to $|G_3^1\rangle_2$, $|G_3^1\rangle_3$, and $|G_3^1\rangle_4$, respectively. Two purple dotted enclosures in Fig. 4 show how to connect three triples to $|G_3^1\rangle$. From Definition 2, this is true for any $n\ge 3$. This means that CCZ and H can be applied any input qubit using the measurement pattern similar to that of Theorem 1. Output qubits in $|G_3^1\rangle_4$ with $1\le t\le m-1$ and qubits that do not compose $|G_3^1\rangle_4$ (i.e. white vertices in Fig. 5) except for ones in the mth group are measured in the mth m

A hypergraph state for universal quantum computing. Using the hypergraph state $|G_n^1\rangle$ defined in Definition 2, we define the target hypergraph state $|G_n^d\rangle$ on $d(2n+63)\binom{n}{3}-n$ qubits, which enables d-depth universal quantum computing on n input qubits with only adaptive X and Z-basis measurements, as follows:

Definition 3 *The hypergraph state* $|G_n^d\rangle$ *is the state constructed in the following three steps (see Fig. 6):*

Step 1. Prepare d states and n(d-1) states in $|G_n^1\rangle$ and $|+\rangle$, respectively. Step 2. Let $|G_{n/i}^1\rangle$ be the i-th $|G_n^1\rangle$. For all t ($1 \le t \le d-1$), apply the CZ gate on each of $|+\rangle$ in the t-th column and each of the right-most qubit (output qubit) in the m-th group of $|G_{n/t}^1\rangle$ such that the j-th ($1 \le j \le n$) qubit from the top in the t-th column is connected to the j-th output qubit from the top in the m-th group of $|G_n^1\rangle$. For the definition of the group of $|G_n^1\rangle$, see Fig. 5. Here, $m = \binom{n}{3}$.

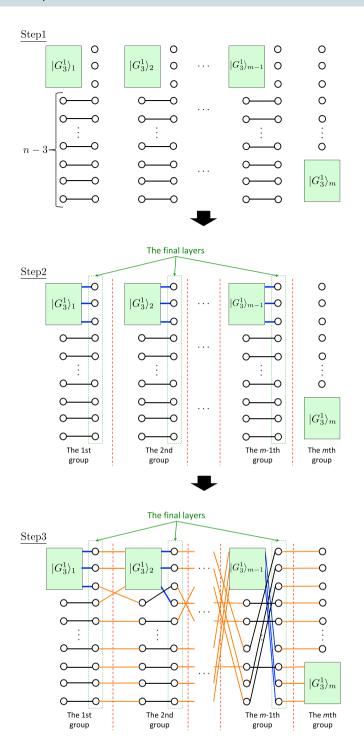


Figure 5. The construction of the hypergraph G_n^1 to define $|G_n^1\rangle$. Each rectangle represents the hypergraph G_3^1 defined in Fig. 1. The black, blue, and orange lines represent edges corresponding to the CZ gates applied in steps 1, 2, and 3, respectively. Here, $m = \binom{n}{3}$.

Step 3. For all t $(1 \le t \le d-1)$, apply the CZ gate on each of $|+\rangle$ in the t-th column and each of the left-most qubit (input qubit) in the first group of $|G_n^1\rangle_{t+1}$ such that the j-th $(1 \le j \le n)$ qubit from the top in the t-th column is connected to the j-th input qubit from the top in the first group of $|G_n^1\rangle_{t+1}$.

Combining Eq. (2) and Definition 3, we can calculate the number of qubits in $|G_n^d\rangle$ as follows:

$$d\left[(2n+63)\binom{n}{3}-n\right]+n(d-1)=d(2n+63)\binom{n}{3}-n. \tag{3}$$

Hence, when d = poly(n), the number of vertices of G_n^d is poly(n). Furthermore, the maximal number of vertices connected to a hyperedge is upper bounded by a constant number, which is three in our case. Therefore, the

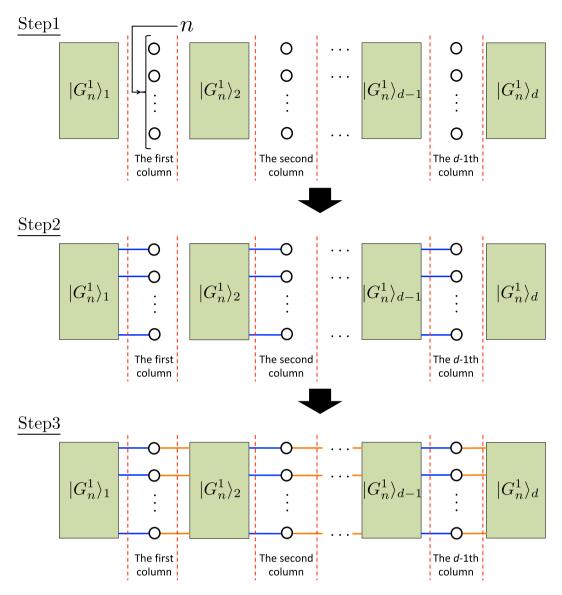


Figure 6. The construction of the hypergraph G_n^d to define our universal hypergraph state $|G_n^d\rangle$. Each rectangle represents the hypergraph G_n^1 defined in Fig. 5. The blue and orange lines represent edges corresponding to the CZ gates applied in steps 2 and 3, respectively.

number of hyperedges is also poly(n). In short, our hypergraph state $|G_n^d\rangle$ is generated in poly(n) time from poly(n) qubits when d = poly(n).

Our universal hypergraph state $|G_n^d\rangle$ satisfies the following theorem:

Theorem 2 The hypergraph state $|G_n^d\rangle$ in Definition 3 can simulate any quantum circuit of depth d consisting of H and CCZ on n input qubits with adaptive X and Z-basis measurements.

Proof. Using the teleportation by the *X*-basis measurement, we can teleport the state of output qubits of $|G_n^1\rangle_t$ to input qubits of $|G_n^1\rangle_{t+1}$ via qubits in the *t*th column. Therefore, from Corollary $1, |G_n^d\rangle$ enables *d*-depth universal quantum computing on *n* input qubits.

Theorem 2 shows that our hypergraph state $|G_n^d\rangle$ only requires X and Z-basis measurements to realize universal quantum computing. In other words, when d = poly(n), we can efficiently simulate any quantum circuit of depth d consisting of poly(n) number of H and CCZ by measuring our hypergraph state $|G_n^d\rangle$ in the X and Z bases.

Verification of our universal hypergraph state. In this subsection, we discuss the verifiability of our hypergraph state $|G_n^d\rangle$ without assuming any independent and identically distributed (i.i.d.) property. Let us consider the following general situation: there exist two parties, Alice and Bob. Alice can only perform single-qubit measurements and has no quantum memory. On the other hand, Bob possesses a universal quantum computer, i.e. he can prepare universal resource states. Therefore, she delegates the preparation of universal resource states

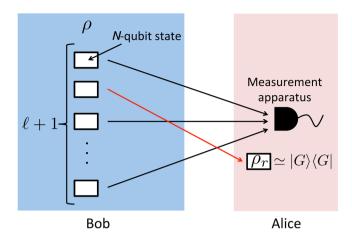


Figure 7. The verification protocol for an N-qubit hypergraph state $|G\rangle$. First, Bob generates an $N(\ell+1)$ -qubit state ρ , and sends each qubit of them to Alice one by one. The quantum state ρ consists of $\ell+1$ registers, and each register stores N qubits. Second, Alice uniformly randomly chooses ℓ registers and tests them. If all the measurement outcomes satisfy Eq. (4), the remaining single register ρ is guaranteed to be close to the ideal hypergraph state $|G\rangle$ (for details, see Theorem 3). Therefore, Alice can safely use ρ for her MBQC.

to Bob, and he sends each qubit of his generated state one by one to Alice. However, since she does not trust him, she has to verify the correctness of his state.

Let us assume that we want to verify an N-qubit hypergraph state $|G\rangle$ corresponding to the hypergraph G. So far, several verification protocols for hypergraph states have been proposed $^{30-32}$. All of them require only Pauli-X and Z basis measurements. This is a reason why we tried to construct a universal hypergraph state that only requires Pauli-X and Z basis measurements for universal MBQC. The most resource-efficient one 32 is the following protocol (see Fig. 7):

- 1. Bob generates an $N(\ell+1)$ -qubit state ρ and sends each qubit to Alice one by one, where $N=d(2n+63)\binom{n}{3}-n$ in our case (see Eq. (3)). If Bob is honest, $\rho=(|G\rangle\langle G|)^{\otimes \ell+1}$. If Bob is malicious, ρ is an arbitrary quantum state, which may be entangled. Without loss of generality, we can assume that ρ consists of $\ell+1$ registers, and each register stores N qubits.
- 2. Alice uniformly randomly chooses ℓ registers from $\ell+1$ registers. For each of them, Alice applies the following protocol, the so-called cover protocol³²: Alice uniformly randomly chooses the value of i from $\{1, 2, ..., \chi(G)\}$ and then applies the ith color test. (Definitions of $\chi(G)$ and the ith color test are given later.) If all ℓ registers pass the tests, Alice proceeds the next step. Otherwise, Alice aborts the protocol.
- 3. Alice uses the remaining single register ρ_r to perform MBQC.

Let us define $\chi(G)$. It is the chromatic number of G, i.e. the minimal number of colors in any hypergraph coloring of G. Here, a hypergraph coloring is a way of coloring each vertex such that no hyperedge contains two vertices having the same color. We say that G is $\chi(G)$ -colorable. Let C_i ($1 \le i \le \chi(G)$) be the set of vertices colored by the ith color. By definition, any two elements of C_i are disconnected to each other, and $\bigcup_{i=1}^{\chi(G)} C_i = V$, where V is the set of vertices of G.

We also define the *i*th color test.

*i*th color test We measure qubits in C_i in the X basis and other qubits in the Z basis. These measurements correspond to measure stabilizers of $|G\rangle$. Let o_i be the measurement outcome on the jth $(1 \le j \le N)$ qubit. If

$$o_j + \sum_{e \in E \mid e \ni j} \prod_{k \in e, k \neq j} o_k \equiv 0 \pmod{2}$$
(4)

for all $j \in C_i$, we consider that the *i*th test is passed. Here, $e \in E|e\ni j$ means the summation over hyperedges that include the *j*th vertex. Equation (4) means that the tested register is properly stabilized.

This verification protocol satisfies the following theorem:

Theorem 3 (ref.32) Let

$$\ell = \left\lceil \frac{\chi(G)(1-\delta)}{\delta \varepsilon} \right\rceil,$$

where $\lceil \cdot \rceil$ is the ceiling function. Then, if Alice proceeds step 3, with significance level δ ,

$$\langle G|\rho_r|G\rangle \ge 1 - \varepsilon.$$
 (5)

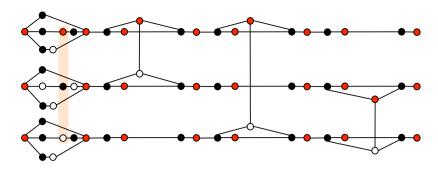


Figure 8. A three-coloring of G_3^1 . Most importantly, six vertices corresponding to the input and output qubits are colored in the same color (red). This property is useful to show $\chi(G_n^d) = 3$.

Note that the significance level is the maximum probability of Alice proceeding step 3 when the state ρ_r does not satisfy Eq. (5). This theorem means that we can estimate the lower bound of the fidelity $\langle G|\rho_r|G\rangle$ between the given state ρ_r and the target hypergraph state $|G\rangle$.

Now let us apply the verification protocol to our hypergraph state $|G_n^d\rangle$. To derive the number of registers required to verify our hypergraph state $|G_n^d\rangle$, we show the following theorem:

Theorem 4 Let G_n^d be a hypergraph defined in Definition 3. Then,

$$\chi(G_n^d)=3.$$

Proof. Since the maximum order of hyperedges of G_n^d is three, $\chi(G_n^d) \geq 3$. The task left is to show that three colors are sufficient for coloring of G_n^d . To this end, first, we give an explicit coloring of G_3^1 in Fig. 8. From Fig. 8, it is evident that three colors (red, black, and white) are sufficient for coloring of G_3^1 . Next, based on this coloring, we consider the coloring of G_n^1 . In the construction of $|G_n^1\rangle$ (see Fig. 5), we use quantum states $|G_3^1\rangle$, $|\Phi^+\rangle$, and $|+\rangle$. Each $|G_3^1\rangle$ is colored in the same manner as in Fig. 8. Since input and output qubits of $|G_3^1\rangle$ are colored in the same color (red), each single qubit $|+\rangle$ except for them in the mth group and each right qubit of $|\Phi^+\rangle$ can be colored in black (or white). In this case, the other qubits can be colored in red. Therefore, G_n^1 is also three-colorable. Furthermore, from this coloring, we notice that input and output qubits of $|G_n^1\rangle$ are also colored in the same color (red). As a result, in the construction of $|G_n^d\rangle$ (see Fig. 6), all single qubits in columns can be colored in black (or white). This means that $\chi(G_n^d)=3$.

From Theorem 3 and Theorem 4, we obtain

Corollary 2 Our hypergraph state $|G_n^d\rangle$ can be verified using $[3(1-\delta)/(d\varepsilon)] + 1$ samples (registers).

It is important to point out that the chromatic number of the Union Jack state is also three³², which means that the efficiency of verifying our hypergraph state is the same as that of verifying the Union Jack state.

In short, from Theorem 2, Corollary 2, and the fact that the existing polynomial-time verification protocols $^{30-32}$ only require *X* and *Z*-basis measurements, the following corollary holds:

Corollary 3 Our hypergraph state $|G_n^d\rangle$ is a polynomial-time generated quantum state such that X and Z-basis measurements are sufficient

- 1. To simulate universal quantum computing in polynomial time of n, and
- 2. To estimate the fidelity in polynomial time of the size of the hypergraph state.

Importantly, all existing other universal resource states require at least one additional measurement basis other than *X* and *Z* bases, while Corollary 3 says that our hypergraph state only needs *X* and *Z*-basis measurements for both MBQC and verification. It is an important advantage of our hypergraph state.

Application. In this subsection, utilizing our hypergraph state $|G_n^d\rangle$, we propose a VBQC protocol where requirements for a client is only X and Z-basis measurements. In VBQC, a client with computationally weak quantum devices delegates universal quantum computing to a remote quantum server in such a way that the client's privacy (input, algorithm, and output) is information-theoretically protected and at the same time the honesty of the server is verifiable.

Our VBQC protocol runs as follows (the protocol is described for an honest server. If the server is malicious, the server can do any deviation that does not violate the no-signaling principle.):

- 1. The client chooses the value of ℓ' from $\{1, 2, ..., \ell+1\}$ uniformly at random.
- 2. The quantum server generates $\ell+1$ hypergraph states $|G_n^d\rangle^{\otimes \ell+1}$, and sends each qubit of them to the client one by one.
- 3. For the ℓ' th hypergraph state, the client performs MBQC. For other ℓ hypergraph states, the client applies the cover protocol of the "Verification of our universal hypergraph state" subsection.
- If the *l* hypergraph states pass the cover protocol, the client accepts the outcome of the MBQC on the *l'* th hypergraph state. Otherwise, the client rejects the outcome.

From the universality of our hypergraph state $|G_n^d\rangle$ (Theorem 2), the client can obtain the correct result if the server is honest, i.e. the sever sends the ideal states. Since there exists only one-way communication from the server to the client in our VBQC protocol, the privacy of the client is information-theoretically preserved due to the no-signaling principal. The verifiability of our VBQC protocol is automatically satisfied by the verification protocol.

In the original proposal of VBQC²⁴, the client has to prepare ten kinds of single-qubit states at the server's side. Although this requirement for the client has already been reduced to the *X* and *Z*-basis measurements in ref.²⁵, our VBQC protocol is simpler than it, and our constructive method is completely different from theirs. In particular, the security proof of our VBQC protocol is much simpler because our VBQC protocol needs only one-way communication and therefore the security is trivially satisfied due to the no-signaling principle, while the protocol of ref.²⁵ needs two-way communications. Furthermore, the verifiability of the protocol in ref.²⁵ has been shown by appropriately tailoring the verifiability proof of the original proposal²⁴ to this protocol. On the other hand, the verifiability of our VBQC protocol is automatically shown from the verifiability of hypergraph states. This difference also makes our VBQC protocol simpler than that in ref.²⁵.

Note that there are mainly two types of VBQC protocols. In the first type, the client prepares single-qubit states and then sends them to the server. All of measurements are delegated to the server. This type includes the original VBQC protocol²⁴. On the other hand, in the second type¹⁴, the preparation of universal resource states is delegated to the server. The only requirements for the client are single-qubit measurements on the received resource states. Our VBQC protocol is constructed by applying our hypergraph state to the second-type VBQC protocol.

Discussion

We have constructed a hypergraph state that enables universal quantum computing with only *X* and *Z*-basis measurements. We have also shown that these two measurements are sufficient to verify our hypergraph state, and have also constructed a VBQC protocol, which only requires *X* and *Z*-basis measurements for the client. Our result decreases the number of measurement bases required for reliable MBQC from existing universal resource states. Two seems to be the optimal solution, because no feed-forward operation is possible if only a single measurement basis is used.

In this paper, we have considered a hypergraph state. It is open whether two measurement bases are enough also for a (an unweighted) graph state. It might be possible to find a measurement pattern on a graph state where only two measurement bases are enough for universal MBQC. However, we point out that if we require that the MBQC is verifiable at the same time and use one of existing verification protocols^{17–19}, at least three measurement bases should be necessary. The reason is as follows. As far as we know, all of existing verification protocols require X and Z-basis measurements for the verification of graph states. However, due to the Gottesman-Knill theorem, only X and Z-basis measurements are not enough for the universality. Therefore, at least a single non-Clifford basis measurement should be added, and in total, three measurement bases are necessary. Our resource state realizes universal MBQC and its verification with the minimum number of local measurements when we restrict verification protocols to be one of existing protocols. (Also remember that in the case of weighted graph states, X and Z-basis measurements are enough for the universality X, but they do not seem to be enough for the verification.)

Our hypergraph state has two advantages over the Union Jack state, which is another universal hypergraph state³³. First, MBQC on our hypergraph state uses no imaginary number, while that on the Union Jack state does, because it needs Y-basis measurements. This feature should simplify the further theoretical analysis of MBQC on hypergraph states. As a concrete example, let us consider the self-testing. Simply speaking, the self-testing is a device-independent verification for a set of a state and operators. To devise a self-testing protocol, a certain equivalence between two sets of a state and operators is defined. A definition of equivalence used, for example, in ref.³⁴ is tailored for the case where the ideal set of a state and operators contains no imaginary number. Although the definition can be extended to the imaginary-number case³⁵, the MBQC on our universal hypergraph state does not need such the extension. This property may facilitate the proposal of a self-testing protocol for a set of our hypergraph state and Pauli-X and Z basis measurements. Second, our proof of universality is simpler than their proof, because they use the percolation argument, while we only use the basic techniques of MBQC (i.e. the teleportation by the X-basis measurement and the decoupling by the Z-basis measurement). Note that the deterministic universality (i.e., universality without the percolation argument) has already been achieved in ref.³⁶. As an advantage of their universal hypergraph state over ours, their state enables to parallelize the CCZ and SWAP gates while it requires more number of measurement bases than ours (i.e., three Pauli bases). It would be an interesting future work to consider whether we can construct a resource state that has both of our and their advantages without losing the deterministic universality.

At the last of this section, we mention the relation between the complexity of resource states and the required number of measurement bases for the universality. The cluster state 37 only has the CZ gates and requires two Pauli-basis measurements and one additional non-Clifford measurement for the deterministic universality 38 (see Table 1). The Union Jack state only has the CCZ gates and requires three Pauli-basis measurements for the probabilistic universality due to the percolation argument 33 . This probabilistic universality can be improved to the deterministic one using another hypergraph state in ref. 36 . that also only has the CCZ gates and requires only three Pauli-basis measurements for the universality. Our hypergraph states uses the CZ and CCZ gates, but the universality (and the verifiability) is achieved using only Pauli-X and Z basis measurements. The Mølmer-Sørensen graph state, which is a weighted graph state, only uses one type of two-qubit phase gates and requires only Pauli-X and X basis measurements for the deterministic universality. Furthermore, the cluster state, the Union Jack state, and the Mølmer-Sørensen graph state are embedded in two-dimensional space while ours and the hypergraph state in ref. 36 . are not. Roughly speaking, these known facts including our present result indicate that making a

resource state somewhat complex gives an advantage in the number of measurement bases. However, the relation between the complexity of resource states and the number of measurement bases seems to, in general, depend on the construction of universal resource states. Therefore, although the complete characterization of the relation would be an interesting direction of research, it seems to be hard, which is beyond the scope of our current research.

Methods

In this section, we derive Eq. (1) in Definition 2. We would like to define t such that it increases one by one from 0 as (i, j, k) becomes (1, 2, 3), (1, 2, 4), (1, 2, 5), ..., (1, 2, n), (1, 3, 4), ..., (1, 3, n), ..., (1, n - 1, n), (2, 3, 4), ..., (n - 2, n - 1, n). In other words, the number t specifies the distance between (i, j, k) and (1, 2, 3). For example, since (1, 2, 4) is the next triple of (1, 2, 3), the number t must be one when (i, j, k) = (1, 2, 4). In order to ease the derivation, here we define $\tilde{t} \equiv t + 1$.

First, we consider the case of (i, j, k) = (1, 2, k) $(3 \le k \le n)$. In this case, $\tilde{t} = k - 2$. In the case of (i, j, k) = (1, 3, k) $(4 \le k \le n)$, $\tilde{t} = (n - 2) + (k - 3)$. Here, (n - 2) is the value of \tilde{t} of the triple (1, 2, n). In the same way, when (i, j, k) = (1, 4, k) $(5 \le k \le n)$, $\tilde{t} = (n - 2) + (n - 3) + (k - 4)$.

Second, repeating the same calculation, when (i, j, k) = (1, j, k) and $3 \le j < k \le n$,

$$t = \tilde{t} - 1 = \left[\sum_{l=2}^{j-1} (n-l) \right] + (k-j) - 1.$$
 (6)

In order to take the case of j = 2 into consideration, we slightly modify Eq. (6) as follows:

$$t = \left[\sum_{l=2}^{j-1} (n-l)\right] + (k-j) - 1$$

$$= \left[\sum_{l=1}^{j-1} (n-l)\right] + (k-j) - 1 - (n-1)$$

$$= \left[\sum_{l=1}^{j-1} (n-l)\right] + k - j - n.$$
(7)

Indeed, if we substitute i = 1 for Eq. (1), Eq. (7) is derived.

Finally, we derive t for any (i, j, k) with $1 \le i < j < k \le n$. To this end, we use the similar argument as above. When (i, j, k) = (2, 3, k) $(4 \le k \le n)$,

$$t = \left\{ \left[\sum_{l=1}^{n-2} (n-l) \right] + n - (n-1) - n \right\} + (k-3),$$

where the first term is the value of *t* of the triple (1, n-1, n). Then, when (i, j, k) = (2, 4, k) $(5 \le k \le n)$,

$$t = \left\{ \left[\sum_{l=1}^{n-2} (n-l) \right] - (n-1) \right\} + (n-3) + (k-4).$$

Therefore, using the similar argument as the case of (i, j, k) = (1, j, k), when (i, j, k) = (2, j, k) with $3 \le j < k \le n$,

$$t = \left\{ \left[\sum_{l=1}^{n-2} (n-l) \right] - (n-1) \right\}$$

+
$$\left\{ \left[\sum_{l=1}^{j-2} (n-l-1) \right] + (k-j) - (n-2) \right\}.$$

Similarly, when (i, j, k) = (3, j, k) with $4 \le j < k \le n$,

$$t = \left\{ \left[\sum_{l=1}^{n-2} (n-l) \right] - (n-1) \right\}$$

$$+ \left\{ \left[\sum_{l=1}^{n-3} (n-l-1) \right] - (n-3) \right\}$$

$$+ \left\{ \left[\sum_{l=1}^{j-3} (n-l-2) \right] + (k-j) - (n-3) \right\}.$$

Repeating this calculation for i, we can obtain Eq. (1).

Data Availability

No data sets were generated or analyzed during the current study.

References

- Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26, 1484 (1997).
- 2. Aharonov, D., Arad I., Eban, E. & Landau, Z. Polynomial Quantum Algorithms for Additive approximations of the Potts model and other Points of the Tutte Plane. Preprint at arXiv:quant-ph/0702008 (2007).
- 3. Bernstein, E. & Vazirani, U. Quantum complexity theory. SIAM J. Comput. 26, 1411 (1997).
- Nielsen, M. A. & Chuang, I. L. Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2000).
- 5. Farhi, E., Goldstone, J., Gutmann, S. & Sipser, M. Quantum Computation by Adiabatic Evolution, Preprint at arXiv:quant-ph/0001106 (2000).
- 6. Raussendorf, R. & Briegel, H. J. A One-Way Quantum Computer. Phys. Rev. Lett. 86, 5188 (2001).
- 7. Raussendorf, R., Browne, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* 68, 022312 (2003).
- 8. Kitaev, A. Fault-tolerant quantum computation by anyons. Ann. Phys. 303, 2 (2003).
- 9. G.-Segovia, M., Shadbolt, P., Browne, D. E. & Rudolph, T. From Three-Photon Greenberger-Horne-Zeilinger States to Ballistic Universal Quantum Computation. *Phys. Rev. Lett.* **115**, 020502 (2015).
- 10. Walther, P. et al. Experimental one-way quantum computing. Nature (London) 434, 169 (2005).
- 11. Briegel, H. J., Browne, D. E., Dür, W., Raussendorf, R. & Van den Nest, M. Measurement-based quantum computation. *Nat. Phys.* 5, 19 (2009)
- 12. Lanyon, B. P. et al. Measurement-Based Quantum Computation with Trapped Ions. Phys. Rev. Lett. 111, 210501 (2013).
- 13. A.-Arriagada, F. et al. One-way quantum computing in superconducting circuits. Phys. Rev. A 97, 032320 (2018).
- Morimae, T. & Fujii, K. Blind quantum computation protocol in which Alice only makes measurements. Phys. Rev. A 87, 050301(R) (2013).
- 15. Kissinger, A. & van de Wetering, J. Universal MBQC with generalised parity-phase interactions and Pauli measurements. *Quantum* 3, 134 (2019).
- 16. Hayashi, M. & Takeuchi, Y. Verifying commuting quantum computations via fidelity estimation of weighted graph states, Preprint at arXiv:1902.03369 (2019).
- 17. Hayashi, M. & Morimae, T. Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing. *Phys. Rev. Lett.* 115, 220502 (2015).
- 18. Markham, D. & Krause, A. A simple protocol for certifying graph states and applications in quantum networks, Preprint at arXiv:1801.05057 (2018).
- Takeuchi, Y., Mantri, A., Morimae, T., Mizutani, A. & Fitzsimons, J. F. Resource-efficient verification of quantum computing using Serfling's bound. npj Quantum Information 5, 27 (2019).
- 20. Shi, Y. Both Toffoli and Controlled-NOT need little help to do universal quantum computation, Preprint at arXiv:quant-ph/0205115 (2002).
- 21. Feynman, R. P. Quantum mechanical computers. Found. Phys. 16, 507 (1986).
- 22. Kitaev, A. Y., Shen, A. H. & Vyalyi, M. N. Classical and Quantum Computation (AMS, Boston, 2002).
- 23. Biamonte, J. D. & Love, P. J. Realizable Hamiltonians for universal adiabatic quantum computers. Phys. Rev. A 78, 012352 (2008).
- 24. Fitzsimons, J. F. & Kashefi, E. Unconditionally verifiable blind quantum computation. Phys. Rev. A 96, 012303 (2017).
- 25. Takeuchi, Y., Fujii, K., Morimae, T. & Imoto, N. Fault-tolerant verifiable blind quantum computing with logical state remote preparation, Preprint at arXiv:1607.01568 (2016).
- Morimae, T. & Koshiba, T. Impossibility of perfectly-secure one-round delegated quantum computing for classical client. Quantum Inf. Comput. 19, 214 (2019).
- 27. Aaronson, S., Cojocaru, A., Gheorghiu, A. & Kashefi, E. On the implausibility of classical client blind quantum computing, Preprint at arXiv:1704.08482 (2017).
- 28. Morimae, T., Nishimura, H., Takeuchi, Y., & Tani, S. Impossibility of blind quantum sampling for classical client. *Quantum Inf. Comput.* 19, 793 (2019).
- 29. Rossi, M., Huber, M., Bruß, D. & Macchiavello, C. Quantum hypergraph states. New J. Phys. 15, 113022 (2013).
- 30. Morimae, T., Takeuchi, Y. & Hayashi, M. Verification of hypergraph states. Phys. Rev. A 96, 062321 (2017).
- 31. Takeuchi, Y. & Morimae, T. Verification of Many-Qubit States. Phys. Rev. X 8, 021060 (2018).
- 32. Zhu, H. & Hayashi, M. Efficient verification of hypergraph states, Preprint at arXiv:1806.05565 (2018).
- 33. Miller, J. & Miyake, A. Hierarchy of universal entanglement in 2D measurement-based quantum computation. npj Quantum Information 2, 16036 (2016).
- 34. McKague, M. Interactive proofs for BQP via self-tested graph states. Theory of Computing 12, 1 (2016).
- 35. McKague, M. & Mosca, M. Generalized Self-testing and the Security of the 6-State Protocol, In *Proc. of Theory of Quantum Computation, Communication, and Cryptography 2010* p. 113 (Springer, Leeds, 2011).
- 36. Gachechiladze, M., Gühne, O. & Miyake, A. Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states. *Phys. Rev. A* **99**, 052304 (2019).
- 37. Briegel, H. J. & Raussendorf, R. Persistent Entanglement in Arrays of Interacting Particles. Phys. Rev. Lett. 86, 910 (2001).
- 38. Mantri, A., Demarie, T. F. & Fitzsimons, J. F. Universality of quantum computation with cluster states and (X, Y)-plane measurements. Sci. Rep. 7, 42861 (2017).
- 39. Hartmann, L., Calsamiglia, J., Dür, W. & Briegel, H. J. Weighted graph states and applications to spin chains, lattices and gases. *J. Phys. B* 40, S1 (2007).
- 40. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal Blind Quantum Computation. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science*, p. 517 (IEEE, Los Alamitos, 2009).
- 41. Mhalla, M. & Perdrix, S. Graph States, Pivot Minor, and Universality of (X, Z)-measurements. Int. J. Unconvent. Comput. 9, 153
- 42. Raussendorf, R., Harrington, J. & Goyal, K. A fault-tolerant one-way quantum computer. Ann. Phys. 321, 2242 (2006).
- 43. Raussendorf, R., Harrington, J. & Goyal, K. Topological fault-tolerance in cluster state quantum computation. New J. Phys. 9, 199 (2007).
- 44. Raussendorf, R. & Harrington, J. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.* **98**, 190504 (2007).
- 45. Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. Nat. Commun. 3, 1036 (2012).
- 46. Affleck, I., Kennedy, T., Lieb, E. H. & Tasaki, H. Valence Bond Ground States in Isotropic Quantum Antiferromagnets. *Commun. Math. Phys.* 115, 477 (1988).
- 47. Brennen, G. K. & Miyake, A. Measurement-Based Quantum Computer in the Gapped Ground State of a Two-Body Hamiltonian. *Phys. Rev. Lett.* **101**, 010502 (2008).

Acknowledgements

We thank Jingfang Zhou and Atul Mantri for helpful discussions. We also thank Mariami Gachechiladze, Otfried Gühne, and Akimasa Miyake for pointing out ref.¹⁵ to us. T.M. is supported by the JSPS Grant-in-Aid for Young Scientists (B) No. JP17K12637, and JST PRESTO No. JPMJPR176A. M.H. is supported in part by Fund for the Promotion of Joint International Research (Fostering Joint International Research) Grant No. 15KK0007, 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.

Author Contributions

Y.T. conceived the key idea. Y.T. refined the key idea through discussions with T.M. and M.H. Y.T. performed the calculations, and all the authors contributed to checking the validity of the calculations and writing of the paper.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2019