Verification of colorable hypergraph states with stabilizer test

Hong Tao 1, Xiaoqian Zhang 2, Lei Shao 3 and Xiaoqing Tan 4, ∗

1 MOE Key Laboratory of Fundamental Physical Quantities Measurement, PGMF and School of Physics, Huazhong University of Science and Technology, Wuhan 430074, People’s Republic of China
2 State Key Laboratory of Optoelectronic Materials and Technologies and School of Physics, Sun Yat-sen University, Guangzhou 510006, People’s Republic of China
3 Zhejiang Institute of Modern Physics, Department of Physics, Zhejiang University, Hangzhou 310027, People’s Republic of China
4 College of Information Science and Technology, Jinan University, Guangzhou 510632, People’s Republic of China
∗ Author to whom any correspondence should be addressed.

E-mail: ttanxq@jnu.edu.cn

Keywords: many-body quantum states, hypergraph states, fault-tolerant, blind quantum computing, computational complexity

Abstract
Many-body quantum states, as a matter of fact, are extremely essential to solve certain mathematical problems or simulate quantum systems in measurement-based quantum computation. However, how to verify large-scale quantum states, such as hypergraph states, is an exceedingly hard task for many-body quantum systems. Here, we propose a novel fault-tolerant solution for the verification of colorable hypergraph states by using the stabilizer test. Furthermore, our protocol is dramatically facilitated by making only Pauli-X and Pauli-Z measurements. For geometric structure hypergraph states, the computational complexity of our protocol is polynomial. As to appliance, it will be also applied to blind quantum computing based on the no-signaling principle.

1. Introduction

So far, quantum computing offers a new approach that can be applied to solve some NP and NP-hard problems. Compared with classical computing, quantum computing can achieve exponential acceleration and provide a reliable guarantee for the security of quantum information processing [1–5]. However, how to determine the security, correctness, and fault tolerance of computational tasks is a problem to be solved when using quantum computing to process quantum information. Therefore, a fault-tolerant and verifiable quantum computing is indispensable and will be the focus of scientific research. In recent years, due to the rapid development of quantum error correction techniques, there are an increasing number of schemes to effectively verify the correctness, security, and feasibility of quantum computation [6–22]. These schemes are implemented based on graph states, such as verifying Hamiltonian basis states [8], stabilizer tests [9], adaptive stabilizer tests [14].

Graph states are an important quantum resource for quantum metrology [23–28] with the optimal state to enhance the measurement precision by the theoretical tools-quantum Fisher information [29–37], and quantum computing with topologically sequences [38, 39] (Not all directed graphs have topological order, so directed acyclic graphs are also called topological graphs. For example, a cluster state is a class of topological graph states, and these can be applied to quantum computation [3, 4]). The polynomial hierarchy collapses to level 3 or 2 if the probability distribution of non-adaptive sequential single-qubits over graph states is classically and efficiently sampled [40–42]. Hypergraph state [43–46], as the generalization of the graph state, is equally efficient in the measurement-based quantum computation (MBQC) [47–57], such as Union Jack state [58] (It is constructed by preparing $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ state at every vertex, and then applying a three-body doubly controlled-Z unitary operation, $CCZ = CZ_2$, to every triangular cell in the lattice.), which is one of the universal resource states for MBQC. As a kind of important quantum resource, the correctness of the quantum states generated by quantum devices becomes particularly important. Therefore, the verification of
quantum states is necessary, and how to verify the hypergraph states of complex structures has become a difficult problem for many researchers.

However, in real experiments, more types of noise will be encountered, including various relations between qubits [59–61], experimental equipment error, human estimation error, external environment (temperature), etc. Since the traditional quantum state tomography scheme will not be able to achieve fault tolerance, we need to find a new scheme to verify quantum states and realize quantum computing without assuming the underlying quantum state noise. In other words, given a desired quantum state, whose quantum device generates a quantum state [16–18] that produces states $\rho_1, \rho_2, \ldots, \rho_{N-1}, \rho_N$ in the $N$ rounds, which can be written as $\rho_i$, and $\rho_i = |\Psi\rangle\langle\Psi|$ for pure states where all $i \in \{1, 2, \ldots, N\}$. At the same time, in the case of extra noise, the density matrix of its quantum states satisfies $\langle\Psi|\rho_i\Psi\rangle \leq 1 - \epsilon$, where $\epsilon$ is a very small number. However, there is a fault-tolerant technique that can reduce errors caused by additional noise (including, experimental equipment errors, estimation errors, etc.). In this paper, we propose a feasible verification hypergraph scheme, which increases the feasibility of our verification scheme by increasing the fault tolerance and reducing the error generated in the experimental process.

The need for a verification protocol satisfies two properties, completeness (if the prover is honest, equivalently, the probability that the state in the quantum register is the ground state of the Hamiltonian and the verifier accepts the prover is greater than $1 - \exp(-N)$) and soundness (if the probability distribution of the target state is close to 1 when the verifier accepts the prover). These two properties are mathematically equivalent to error-tolerant detectability [9]. For wrong output, we can detect it with high probability. But this is without satisfying the fault tolerance, and must also be coupled with acceptability, which means we need accepting the computational results of the test with high probability in a realistic noisy environment.

Here we propose a verifiable colorable hypergraph state protocol satisfying completeness and soundness (no underlying quantum graph noise are assumed). We define the set of correctable errors on a given resource state, any small amount of noise on the hypergraph causes rejection, the set of correctable errors defines the bound, and we can accept the test results within the specified range. We use stabilizer test scheme to verify a given hypergraph state $|G\rangle$ by decomposing hypergraph states into graph states. If the scheme is extended to the noisy case, we can determine whether a given hypergraph state is a fault-tolerant resource state within the correctable set. In this case, the test passes, it is necessary to ensure that the accuracy is sufficiently high (the output of the hypergraph copy of the device gets 99% fidelity with 90% probability). Our verification scheme is validity and the resource consumption is a polynomial of constant order $O(n^{5(G)})$. Finally, our scheme of the fault-tolerant verifiable hypergraph states can also be applied to blind quantum computing [9, 50].

This paper is organized as follows. In section 2, we introduce what is a hypergraph state. In section 3, we give the error set of colorable hypergraph states. In section 3.1, we consider a generic scenario on a three-colorable hypergraph state (the Union Jack state) and give a test scheme with stabilizer tests in section 3.2. In section 4, we propose a verification protocol for hypergraph states based on the stabilizer test. In section 5, we introduce the application to blind quantum computing. Finally, we give the conclusion in the paper.

2. Hypergraph state

We first define hypergraph states and describe their properties [12, 14, 19]. The hypergraph $G = (V, E)$ is a pair of the set of vertices $V$ and the set of hyperedges $E$, where the numbers of qubits are $n = |V|$ and the edge satisfies $|e| \geq 2$ with $e \in E$, and $|e|$ is the number of edges linked to the hyperedge $e$. Therefore, we can find the degree of the vertex is $\geq 2$. For example, the minimum degree of the graph state (cluster state [57]) is 2, and the minimum degree of the hypergraph state (Union Jack state) is 3. The Union Jack state [58] could be shown as figure 1. The hypergraph state $|G\rangle$ corresponding to the hypergraph $G$ is defined by

$$|G\rangle \equiv \prod_{e \in E} \mathcal{CZ}_e |+\rangle^\otimes n, \quad (1)$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|0\rangle$ and $|1\rangle$ are the eigenstates corresponding to the Pauli-Z eigenvalues $\pm 1$, respectively. And the control-Z operator $\mathcal{CZ}_e$ can be written as

$$\mathcal{CZ}_e \equiv \bigotimes_{i \in e} \mathbb{I}_i - 2 \bigotimes_{i \in e} |1\rangle\langle 1| \quad (2)$$

is the generalized CZ gate acting on vertices in the hyperedge $e$. Here, $\mathbb{I}_i$ is the two-dimension identity operator. For example, if $|e| = 2$, it is nothing but the standard CZ gate. If $|e| = 3$, it is the CZ$_2$ gate,

$$\mathcal{CZ}_e \equiv (F^\otimes 2 - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes Z. \quad (3)$$
Figure 1. Examples of the hypergraph state: the Union Jack states on a two-dimension lattice. Every vertex represents a qubit initialized in $|+\rangle$ state, and every triangular cell represents an applied three-body unitary CCZ. The three vertices of each elementary are connected by an order-three hyperedge. The quantum states are three-colorable as illustrated.

The density matrix form of the hypergraph state $|G\rangle$ is

$$\rho = |G\rangle\langle G| = \prod_{i=1}^{n} \frac{g_i^n + g_i^0}{2},$$

where the $i$th stabilizer $g_i$ of the hypergraph state $|G\rangle$ ($i = 1, 2, \ldots, n$) is defined by

$$g_i = \left( \prod_{e \in E} CZ_e \right) X_i \left( \prod_{e \in E} CZ_e \right).$$

And the stabilizer $g_i$ satisfies the following property,

$$g_i |G\rangle = |G\rangle.$$  

Hypergraph states have some advantages. For example, certain hypergraph states, such as the Union Jack state are universal resource states for MBQC with only Pauli measurements. With the development of quantum computers, it is of great significance to study the verification of hypergraph states. Some verification schemes for hypergraph state have been proposed so far, and we present a relatively simple scheme to verify hypergraph states.

### 3. Cover strategy

Let $A_i$ be the independent set of the hypergraph state $G$, which is the set of the vertices of the color $c_i$ of the hypergraph. A set $A = \{A_1, A_2, \ldots, A_m\}$ of the independent sets of $G$ is an independent cover if $\bigcup_{i=1}^{m} A_i = V$.

The cover $A$ is also defined as the colorable set of the graph $G$ with $m$ colors when $A$ is formed by the vertex $V$ (assuming $A_i$ is a nonempty set of $V$). A hypergraph $G$ is $m$-colorable if its vertices can be colored using $m$ different colors. For example, a two-colorable graph is also called the bipartite graph. The chromatic number $\gamma(G)$ is the minimum number of colors in any coloring of the hypergraph $G$, equivalently, the minimum number of elements in any independent cover of the hypergraph $G$, there is $\gamma(G) \leq m$, (when the hypergraph $G$ is geometric (Geometric graphs in the broadest sense are graphs drawn on a Euclidean plane, possibly with intersecting straight edges, and topological graphs, where an edge can be any continuous curve connecting vertices.)).

For example, the Union Jack state, the chromatic number is equal to number of the colors $m$, $\gamma(G) = m$. We can use three colors (3 is also the minimum coloring number) instead of using more colors in figure 1. Using more colors will increase the computational complexity (the number of qubits and the number of tests), thus we give the minimum number of colorings. The other reason for being three colors is that for the Union Jack state, the entanglement between qubits is a CCZ gate, and the entanglement between three qubits. Because we can distinguish the subgraph with only three colors.

The $m$-colorable hypergraph state $|G\rangle$ is composed of the color-system $H_{c_1}, H_{c_2}, \ldots, H_{c_{\gamma(G)}}$, consisting of $n_{c_1}, n_{c_2}, \ldots, n_{c_{\gamma(G)}}$ qubits, where $n = n_{c_1} + n_{c_2} + \cdots + n_{c_{\gamma(G)}}$, $n$ is the qubits number of hypergraph state $|G\rangle$, where $\gamma(G) \leq m \leq n$. For example, the Union Jack state can be shown in figure 2. For each $A_i$, each qubit on
H Tao

\[ H_{\text{ Tao}} := \text{denotes the qubits } \otimes. \text{ Here, } +, \text{ respectively. And the operator } \otimes \text{ refer to the qubits number of subgraph in the subspace } \text{ is odd, one can get the form } \otimes Z, \text{m} \otimes \cdots \otimes H \text{n} \text{is defined in the following two forms. When } + c, \text{...}, (n Z := X. According to the stabilizer test scheme } \text{is odd, } \otimes \text{m} \otimes H \text{n} \text{into }. \text{Therefore, } \otimes Z | \text{n} \otimes \cdots \otimes H = X :\text{show that perform the Pauli-X(Z) operator on the color-qubit } c. \text{Therefore, when } \text{is even,}

\[ X := \bigotimes_{i=1}^{n_a} X_i, \quad Z := \bigotimes_{i=1}^{n_a} Z_i, \]

\[ X := \bigotimes_{i=1}^{n_a} X_i, \quad Z := \bigotimes_{i=1}^{n_a} Z_i, \]

where \( n = n_{\text{even}} + n_{\text{odd}} \) is the vertices number of the hypergraph, and \( n_{\text{even}} = n_{c_1} + n_{c_2} + \cdots + n_{c_{\gamma(G)-1}} \).

However, there are two tests for \( A_\gamma \) on system \( H_{c_1} \otimes H_{c_2} \otimes \cdots \otimes H_{c_{\gamma(G)-1}} \). We can divide hypergraph \( G \) into \( \gamma(G) \) graphs. The Pauli operators \( X, Z \) act on different chromatic numbers on \( c_i \), \( n_{c_i} \) denotes the qubits number of the \( i \)th color \( c_i \) with \( X \). Here if our hypergraph is geometric, the chromatic number is equal to the colorable number \( \gamma(G) = m \). Thus each graph corresponds to each independent set.

There are two kinds of operators \( X, Z \) on the system \( A_\gamma \). According to the stabilizer test scheme [9], the test number of stabilizer test is \( \frac{\gamma(G) \times (\gamma(G) - 1)}{2} \). Now we consider the first open set \( A_1 \). The hypergraph state \( |G \rangle \) is defined in the following two forms. When \( \gamma(G) \) is odd, one can get the form

\[ (X_{n_1} \otimes Z_{n_2} \otimes X_{n_3} \otimes \cdots \otimes X_{n_{\gamma(G)}}) |G \rangle = |G \rangle, \]

\[ (Z_{n_1} \otimes X_{n_2} \otimes Z_{n_3} \otimes \cdots \otimes Z_{n_{\gamma(G)}}) |G \rangle = |G \rangle, \]

where \( X_{n_i} := \bigotimes_{i=1}^{n_i} X_i, Z_{n_i} := \bigotimes_{i=1}^{n_i} Z_i \) show that perform the Pauli-X(Z) operator on the color-qubit \( c_i \). Therefore, when \( \gamma(G) \) is even,
(Z_{n_1} \otimes X_{n_2} \otimes Z_{n_3} \otimes \cdots \otimes X_{n_{c_i}(G)}) |G\rangle = |G\rangle.

We perform the fault-tolerant MBQC on the \( m \)-colorable hypergraph states. The total space \( \mathcal{H}_{c_i} \otimes \mathcal{H}_{c_2} \otimes \cdots \otimes \mathcal{H}_{c_{c_i}(G)} \) is spanned by \( \{ Z^a |G\} \) \( a \in \mathcal{F}_2 \) in [10] with the \( \mathcal{F}_2 = \{0,1\} \). However, the sets of the correction errors on the \( m \)-colorable hypergraph state are defined as the correctable state \( |G\rangle \) and the erroneous \( Z^a |G\rangle \) cause the same result under the error correction. The set of correction error is specific on the \( \mathcal{F}_2^{n_1} \otimes \mathcal{F}_2^{n_2} \otimes \cdots \otimes \mathcal{F}_2^{n_{c_i}(G)} \), the subset of the set \( S \) can be written as \( S_{c_1} \otimes S_{c_2} \otimes \cdots \otimes S_{c_{c_i}(G)} \).

3.1. Case study

Let us consider a generic scenario on a three-color hypergraph state \(|\Psi_{BRG}\rangle\) composed of the blue system \( \mathcal{H}_B \), the red system \( \mathcal{H}_R \), and the green system \( \mathcal{H}_G \), consisting of \( n_B \), \( n_R \), \( n_G \) qubits, where \( n = n_B + n_R + n_G \). For example, the decomposition structure of the Union Jack state is shown as figure 2. Figures 2(a) and (c) represent the first color (blue) acting on operators \( X \) and \( Z \) and the second color (red) acting on operators \( Z \) and \( X \). Figures 2(b) and (d) represent the second color (red) acting on operators \( Z \) and \( X \) and the third color (green) acting on operators \( X \) and \( Z \). Thus the hypergraph of three colors we can measure in four steps. We can obtain the following equations

\[
(X_{n_B} \otimes Z_{n_B} \otimes X_{n_R}) |\Psi_{BRG}\rangle = |\Psi_{BRG}\rangle,
\]

\[
(Z_{n_B} \otimes X_{n_B} \otimes Z_{n_R}) |\Psi_{BRG}\rangle = |\Psi_{BRG}\rangle,
\]

where

\[
X_{n_B} = \bigotimes_{i=1}^{n_B} X_{i_B}, \quad Z_{n_B} = \bigotimes_{i=1}^{n_B} Z_{i_B},
\]

\[
X_{n_R} = \bigotimes_{i=1}^{n_R} X_{i_R}, \quad Z_{n_R} = \bigotimes_{i=1}^{n_R} Z_{i_R},
\]

\[
X_{n_G} = \bigotimes_{i=1}^{n_G} X_{i_G}, \quad Z_{n_G} = \bigotimes_{i=1}^{n_G} Z_{i_G},
\]

are the Pauli operators on the blue (red, green) system.

We define the set of correction error \( S \), the subset of \( S \) is written as

\[
S_B \otimes S_{BG}, \quad S_R \otimes S_{BG}, \quad S_G \otimes S_{BR}.
\]

By using the binary-valued adjacency matrix \( A \), i.e. \((i,j)\) element of \( A \) is 1, if and only if the vertices \( i \) and \( j \) are connected on the graph. For the equation (9), there are a number of relationships.

For example, owning to \( S_B \otimes S_{BG} \), we can get the following related equation

\[
X_{n_B} + A_1^T Z_{n_B} + A_2 X_{n_G} \in S_{BG},
\]

\[
X_{n_R} + A_1 Z_{n_R} + A_2^T Z_{n_G} \in S_R,
\]

where \( A_1, A_2 \) are the adjacency matrices as shown in the figures 2(a) and (b). Then a set of correctable errors on the three-colorable hypergraph state \(|\Psi_{BRG}\rangle\) is defined such that the correct state \(|\Psi_{BRG}\rangle\) and an erroneous one \( Z^a |\Psi_{BRG}\rangle \) result in the same computational outcome under the error correction. Such a set of errors is specified as a subset \( S \) of \( \mathcal{F}_2^{n_B} \otimes \mathcal{F}_2^{n_R} \otimes \mathcal{F}_2^{n_G} \). The projection to the subspace by \( S \). We assume the subset \( S \) is written as \( S_{BG} \) and \( S_R \) by using two subset \( S_{BG} \in \mathcal{F}_2^{n_B} \otimes \mathcal{F}_2^{n_R} \) and \( S_R \in \mathcal{F}_2^{n_R} \).

3.2. Test for verification quantum computation

The text is similar to the stabilizer test procedure [9]. Using statistical sampling protocol to verify whether the error is correctable, and satisfies independent and identically distributed. The protocol process runs as follows

(a) The honest prover generated \(|\Psi_{BRG}\rangle^{\otimes 6k+1}\), and the prover sends each qubit to the verifier one by one.
(b) The verifier divides \( 6k + 1 \) blocks of \( n \) qubits into four groups, \( 3 \times 2k \) blocks, and a single block (the fourth group) by random choice.
(c) The verifier uses the fourth group for her computation, other blocks are used for the test, which will be explained later.

(d) If the verifier passes the test, she accepts the result of the computation performed on the fourth group.

For each block of the first, the second, and the third groups, the verifier performs the following test.

Test for the blue system $T_B$: For every two blocks of the first group, the verifier measures the qubits of the blue systems into the $X(Z)$ basis, respectively. Then she obtains the operators $X_{n_B}, Z_{n_B}, X_{n_B}$ and $Z_{n_B}, X_{n_B}, Z_{n_B}$. If the following relationship is satisfied

$$X_{n_B} + A_1^T Z_{n_B} + A_2 X_{n_B} \in S_{BR},$$

then the test is passed.

Test for the red system $T_R$: For every two blocks of the second group, the verifier measures the qubits of the red systems into the $X(Z)$ basis, respectively. Then she obtains the operators $X_{n_R}, Z_{n_R}, X_{n_R}$ and $Z_{n_R}, X_{n_R}, Z_{n_R}$. If the following relationship is satisfied

$$X_{n_R} + A_1^T Z_{n_R} + A_2 X_{n_R} \in S_{RB},$$

then the test is passed.

Test for the green system $T_G$: For every two blocks of the third group, the verifier measures the qubits of the green systems into the $X(Z)$ basis, respectively. Then she obtains the operators $X_{n_G}, Z_{n_G}, X_{n_G}$ and $Z_{n_G}, X_{n_G}, Z_{n_G}$. If the following relationship is satisfied

$$X_{n_G} + A_1^T Z_{n_G} + A_2 X_{n_G} \in S_{GR},$$

then the test is passed.

The probability of passing the test in the case of noiseless is discussed below. The probability $p_{test, i}$, is that the verifier passes the stabilizer test for $g_i$ on the quantum state $\rho_{BR}$ is

$$p_{test, i} = \frac{1}{2} + \frac{\text{Tr}(\rho_{BR})}{2^{r+1}},$$

where the constant number $r$ satisfies

$$r \leq \frac{(n_B + n_R) \times (n_B + n_R - 1)}{2} + \frac{(n_R + n_G) \times (n_R + n_G - 1)}{2},$$

as shown in figures 2(a) and (b). Here, we can see that if $r = \text{poly}(n)$, then $p_{test, i} = 1/2 + O\left(2^{-\text{poly}(n)}\right)\text{[12]}$.

The probability $P_{pass}$ is the expected probability that the verifier passes the test on the quantum state $\rho = \langle \Psi_{BRG} | \Psi_{BRG} \rangle$, where the expectation passes the $N$-random sampling test. For the probability of the first resultant state $\rho_{BR}$ is

$$P_{pass} = \langle \Psi_{BR} | \rho_{BR} | \Psi_{BR} \rangle = \text{Tr}\left(\rho_{BR} \prod_{i=1}^{n_B} \left(\frac{\rho_{BR}^{n_B+n_R} + g_{BR}}{2}\right)\right) \geq 1 - \frac{1 - \delta}{\delta N}$$

with significance level $\delta$, $\delta \geq \frac{1}{N^2+1}$, and quantum state $|\Psi_{BR}| \langle \Psi_{BR} | = T_G(\rho)$. Here $g_{BR}$ is the stabilizer on the graph state as shown in figure 2(a). The probability of the second resultant state $\rho_{RG}$ is
where $g_{BG}$ is the stabilizer on the graph state as shown in figure 2(b), and quantum state $|\Psi_{BG}\rangle |\Psi_{BG}\rangle = \text{Tr}_B(\rho)$. Due to the independence of the tests with $i = B, G$, the joint probability of passing the test by the equation (19) and the equation (20) can be written as

$$P_{\text{pass}} = \frac{1}{\alpha(6k+1)},$$

From this, we can conclude the property in (23). If the test passes, with the significance level $\alpha$, assuming that $\alpha \geq \frac{1}{6k+1}$, we can ensure the computable state $\rho_{\text{com}}$ of the fourth group satisfies

$$\text{Tr}(\rho_{\text{com}}M_k) \geq 1 - \frac{1}{\alpha(6k+1)},$$

where $M_k$ is the projector of the subspace. According to the relation between detectability and the fidelity $\langle \Psi_{BG} | \rho_{\text{com}} | \Psi_{BG} \rangle$, and if the test passes, it is necessary to ensure that the accuracy is high enough, and the outputs copies of the hypergraph of the device have 99% probability to get the target with 99% fidelity.

$$\langle \Psi_{BG} | \rho_{\text{com}} | \Psi_{BG} \rangle \geq \frac{1}{\sqrt{\alpha(6k+1)}}.$$
By increasing fault tolerance with the error-correctable error sets, reducing the extra errors caused by underlying quantum graph state noise, the external environment, and experimental equipment, increasing the verifier’s trust in the prover, and improving the correctness of the quantum state. We can define a set of error-correctable error sets on the hypergraph states to improve the correctness of quantum states. For example, the schemes in [4, 5, 60, 62] could be viewed using the surface code with the concatenated Reed–Muller 15-qubit code [63, 64] and the concatenated Steane 7-qubit code [65, 66].

4. Verification protocol

A weighted independence cover set \((A, \mu)\) of the hypergraph state \(\rho = |G\rangle \langle G|\) is a open cover with weights \(\mu_i\) for \(A_i \in A\) that is composed of \(m\) nonempty independence sets, where \(\mu_i\) is a probability distribution. We can structure a verification protocol for the \(m\)-colorable hypergraph state \(\rho\). We propose a verification protocol for the hypergraph states based on the stabilizer test [9]. In figure 3, we show the verification scheme. Our verifiable protocol runs as follows.

Step 1. The prover sends the verifier an \(n(\sum_{i=0}^{\nu} n_i k + d + 1)\)-qubit quantum state, the quantum state consists of the \(\sum_{i=0}^{\nu} n_i k + d + 1\) registers, and each register stores \(n\) qubits, where the \(\nu\) is written as \(\gamma(G) \times (\gamma(G) - 1)\), and \(n_i = n_{i-}\). If the prover is honest, the prover sends \(\rho^{\otimes \sum_{i=0}^{\nu} n_i k + d + 1}\) to the verifier. On the other hand, if the prover is malicious, the prover sends an any \(n(\sum_{i=0}^{\nu} n_i k + d + 1)\) qubits instead of the correct quantum state \(\rho^{\otimes \sum_{i=0}^{\nu} n_i k + d + 1}\).

Step 2. The verifier chooses \(d\) registers uniformly random and discards them to guarantee that the remaining \(n(\sum_{i=0}^{\nu} n_i k + 1)\)-qubit state \(\rho_i\) is close to an independent and identically distributed sample by using the quantum de Finetti theorem [49]. Next, the verifier chooses one register called the target register with the target (correct) quantum state \(\rho_{tar}\). The quantum state of the target register is uniformly random and used for the quantum computation. The remaining \(\sum_{i=0}^{\nu} n_i k\) registers are divided into \(\sum_{i=0}^{\nu} n_i\) groups such that which the \(k\) registers are assigned to the every group is uniformly random. The verifier performs the parceled stabilizer test for \(g_{ij}\) on the every register in the \(i\)th group, where \(i \in \{1, 2, \ldots, \nu\}, j \in \{1, 2, \ldots, \nu\}\).

Let \(K_{ij}\) be the number of times that the verifier passes the parceled stabilizer test for \(g_{ij}\) on \(j\). If every group of tests passes, then the following formula is satisfied

\[
\frac{K_{ij}}{K_{j}} \geq 1 + \frac{1 - \epsilon}{2^{r+1}},
\]

where \(r = \text{ploy}(n)\), and \(n = n_{e_1} + n_{e_2} + \cdots + n_{e_m}, \epsilon = \frac{1}{r}, K_{j} = \frac{n^2}{2}\). We see that the verifier passes the stabilizer test for the \(i\)th group. If the verifier passes the stabilizer test for all \(i\) and \(j\), which means that the verifier accepts the prover.

The validity of the protocol is proved by showing the completeness and correctness of the protocol. Simply say, we show that the verification protocol is complete if the verifier accepts the correct quantum state with high probability. On the other hand, if the protocol can guarantee that the quantum state that passes the verification protocol has a high probability of being close to the rationally correct state, then the protocol is soundness.

Theorem 1 (Completeness). If the prover is honest, i.e. the quantum state of each register is the correct quantum state \(\rho\), the probability that the verifier accepts the prover is \(\geq 1 - \nu ne^{-\text{ploy}(n)}\).

Proof. The quantum state of each register is the correct quantum state \(\rho\), the passing probability of the quantum state is \(P_{\text{pass}} = 1/2\), and the passing probability \(P_{\text{test},i} = 1/2 + O(2^{-(r+1)})\) with stabilizer test. Because of the Union bound and the Hoeffding inequality [67], we can obtain the probability which the verifier accepts the prover,

\[
P_r = P \left\{ \bigwedge_{j=1}^{\nu} \bigg[ \frac{K_{ij}}{K_{j}} \geq 1 + \frac{1 - \epsilon}{2^{r+1}} \bigg] \right\}
\geq 1 - \sum_{j=1}^{\nu} \sum_{i=1}^{n} P \left[ \frac{K_{ij}}{K_{j}} < \frac{1 - \epsilon}{2^{r+1}} \right]
\geq 1 - \nu ne^{-\text{ploy}(n)}.
\]

The verifier accepts the prover is \(\geq 1 - \nu ne^{-\text{ploy}(n)}\). \(\square\)
Figure 3. The verification scheme of the prover–verifier interaction considered in this paper. The quantum server is designated as the prover, and the client is designated as the verifier. The red dots represent qubits, and $n(\sum_{l=0}^{\infty} n_{c_l} k + d + 1)$ is the number of qubits that the quantum server needs to transmit to the client.

**Theorem 2 (Soundness).** If the verifier accepts the prover, the state of the target register satisfies

$$\langle G | \rho_{\text{tar}} | G \rangle \geq 1 - \frac{1}{n^2},$$

with a probability larger than $1 - \frac{1}{n^2}$.

**Proof.** Let $M$ be the $n_{c_l}$-qubit projector $M = I \otimes \cdots \otimes | A_l \rangle \langle A_l |$. Here $| A_l \rangle$ represents subset of hypergraph states $| G \rangle$ with the weighted independence cover $(A_l, \mu_l)$ for all $l$. The set $A$ of the hypergraph state $| G \rangle$ is an independence cover if $\bigcup_{l=1}^{m} A_l = V$. $T$ is the positive-operator-value measurement element corresponding to the event where the verifier accepts the prover. We can show that any $n_{c_l}$-qubit state $\rho_{c_l}$ is in the independence cover $A_l$. According to the results in [12, 14],

$$\text{Tr} \left( (T \otimes M) \rho_{c_l} \right) \leq \frac{1}{2n_{c_l}^2}. \quad (27)$$

Because of the quantum de Finetti theorem (for the fully one-way local operations and classical communication (LOCC) norm) [49] and equation (27), we could obtain

$$\text{Tr} \left( (T \otimes M) \rho_{c_l} \right) \leq \text{Tr} \left[ (T \otimes M) \int d\mu \otimes \sum_{l=0}^{\infty} n_{c_l} k \right] + \frac{1}{d} \sqrt{2 \sum_{l=0}^{\infty} n_{c_l}^2 k^3 \log 2} \leq \frac{1}{(\sum_{l=0}^{\infty} n_{c_l}^2) k^2}, \quad (28)$$

where $d = 2n_{c_l}^2 \mu k^3 \log 2$. Here, $\mu$ is a probability measurement on the quantum state $\rho$. There are the following facts

$$\sum_{l=1}^{m} n_{c_l}^2 \geq \frac{n^2}{m} = n^{2-\log m}, \quad (29)$$

with $\gamma(G) \leq m, m \leq n$. Using the equation (27) and the equation (28) to compute that

$$\text{Tr} \left( (T \otimes M) \rho_{c_l} \right) \leq \frac{1}{n^2 \mu^2}. \quad (30)$$

Since we can have

$$\text{Tr} \left[ (T \otimes M) \rho_{c_l} \right] = \text{Tr} \left[ (T \otimes I) \rho_{c_l} \right] \text{Tr} [M \rho_{\text{tar}}]. \quad (31)$$

Therefore, if

$$\text{Tr} [M \rho_{\text{tar}}] > \frac{1}{n \mu}, \quad (32)$$

then one can get

$$\text{Tr} \left[ (T \otimes I) \rho_{c_l} \right] < \frac{1}{n \mu}. \quad (33)$$
which means that if the verifier accepts the prover,

$$\langle G | \rho_{\text{tar}} | G \rangle \geq 1 - \frac{1}{n\upsilon},$$

(34)

with a probability larger than $1 - \frac{1}{n\upsilon}$.

5. Application to blind quantum computation

In terms of application, we propose the verification scheme to apply the blind quantum computation (BQC) [30–55]. BQC allows a client with limited quantum technology to delegate her quantum computational tasks to a server who can perform universal quantum computation while retaining the client’s secret information. The verifier (Alice) does not have enough quantum technology, and can delegate her quantum computing work to the prover (Bob), who has a full-fledged quantum computer (or perform the universal quantum computation), without leaking any her privacy.

Here, the quantum server generates $m$-colorable hypergraph states $\rho$ and sends them to the client with MBQC [56] of verification scheme [9]. According to the detectable, the exactness of the quantum output is guaranteed under the acceptance, and the blindness is guaranteed by the no-signaling principle. With the acceptance, our proposed verification scheme can apply blind quantum computation even under the quantum noise or quantum server deviation as long as the quantum server is honest. For the correct calculation state $\rho_{\text{tar}}$, Alice sends each qubit of the correct calculation state $\rho_{\text{tar}}$ to Bob one by one, and Bob executes the correct quantum computation according to Alice’s request. Likewise, if Bob is malicious, Alice does not accept the quantum state sent by Bob. The protocol is canceled. Assuming that Alice has a few quantum capabilities to perform single-qubit Pauli-X($Z$) measurements, then Alice can perform quantum computations on the correct calculation state $\rho_{\text{tar}}$.

6. Conclusion

A graph state is a general quantum resource with quantum computation, and a hypergraph is a kind of graph state. Various schemes have been proposed for the verification of the graph state. However, due to the hypergraph state’s more complex structure, the hypergraph state is more difficult to verify. However, some verification schemes for hypergraph have been proposed [12, 19, 20] which are more complicated in form. Based on the stabilizer verification scheme of graph states in [9], a feasible scheme for verifying hypergraph states is proposed, our verification protocol requires weaker quantum computing technology for the verifier, and the verifier only need the power to perform the single-qubit measurement. Compared with other verification hypergraph schemes [19, 20], the schemes established a general framework for verifying pure quantum states (including bipartite pure states, hypergraph states, Dicke states, Greenberger-Horne-Zeilinger (GHZ) states, stabilizer states, weighted graph states etc). Our scheme adopts the stabilizer test scheme and only needs a single-qubit measurement.

Due to the more complex graph structure, the complexity of quantum computing is higher. Compared with graph states, the computational complexity of hypergraph state verification is higher. To reduce the complexity of the hypergraph state, we propose a fault-tolerant verification hypergraph protocol. Here, we compare the approach presented above with previous works. Our scheme does not increase the computational complexity, and the implementation scheme is relatively simple. We give a test scheme, decompose the hypergraph state into graph states, and test the correctness of the resulting quantum state using the stabilizer test scheme [9]. We give detectability, which proves that our test scheme is feasible. The test and verification scenarios only need to perform single-qubit Pauli-X($Z$) measurements. The disadvantage is that more quantum resources are required.

In this paper, our verifiable protocol can be applied to arbitrary fault-tolerant hypergraph states (graph state) $|G\rangle$ in the BQC. The fault-tolerant scheme reduces errors caused by underlying quantum graph state noise, the external environment and experimental equipment, increases the verifier’s trust in the prover, and improves the feasibility of the verification scheme. If the prover is honest, then the verifier can accept the correct computed state with a high probability greater than or equal to $1 - \frac{1}{n\upsilon}$. For a concrete example, we define a set of correctable errors based on topologically protected MBQC on the Union Jack state. We can calculate the acceptability of distributed probability under the actual noise model. The probability of the test scheme passing with the test state $\rho$ is $P_{\text{pass}} > 1 - \frac{2(1-\delta)}{\delta N}$, so we can accept test results with high probability.

Data availability statement

No new data were created or analysed in this study.
Acknowledgments

This work was supported by the Natural Science Foundation of Guangdong Province of China under Grant No. 2021A1515011440, the Major Program of Guangdong Basic and Applied Research under Grant No. 2019B030302008 and the National Natural Science Foundation of China under Grant No. 62032009.

ORCID iDs

Hong Tao ★ https://orcid.org/0000-0002-3561-1384
Xiaoqing Tan ★ https://orcid.org/0000-0002-3303-2493

References

[1] Nielsen M A and Chuang I L 2010 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[2] Hayashi M, Ishizaka S, Kawachi A, Kimura G and Ogawa T 2014 Introduction to Quantum Information Science (Graduate Texts in Physics) (Berlin: Springer)
[3] Rausendorf R and Briegel H J 2001 A one-way quantum computer Phys. Rev. Lett. 86 5188–91
[4] Rausendorf R, Harrington J and Goyal K 2006 A fault-tolerant one-way quantum computer Ann. Phys., NY 321 2242–70
[5] Rausendorf R and Harrington J 2007 Fault-tolerant quantum computation with high threshold in two dimensions Phys. Rev. Lett. 98 190504
[6] Morimae T 2014 Verification for measurement-only blind quantum computing Phys. Rev. A 89 060302(R)
[7] Morimae T 2016 Measurement-only verifiable blind quantum computing with quantum input verification Phys. Rev. A 94 042301
[8] Morimae T, Nagaj D and Schuch N 2016 Quantum proofs can be verified using only single qubit measurements Phys. Rev. A 93 022326
[9] Hayashi M and Morimae T 2015 Verifiable measurement-only blind quantum computing with stabilizer testing Phys. Rev. Lett. 115 220502
[10] Fujii K and Hayashi M 2017 Verifiable fault-tolerance in measurement-based quantum computation Phys. Rev. A 96 030301(R)
[11] Gheorghiu A, Kapourniotis T and Kashefi E 2017 Verification of quantum computation: an overview of existing approaches Theory Comput. Syst. 63 715–808
[12] Morimae T, Takeuchi Y and Hayashi M 2017 Verification of hypergraph states Phys. Rev. A 96 062321
[13] Fitzsimons J F, Hajdušek M and Morimae T 2018 Post hoc verification of quantum computation Phys. Rev. Lett. 120 040501
[14] Takeuchi Y and Morimae T 2018 Verification of many-qubit states Phys. Rev. X 8 021060
[15] Takeuchi Y, Mantri A, Morimae T, Mizutani A and Fitzsimons J F 2019 Resource-efficient verification of quantum computing using Serfings bound npj Quantum Inf. 5 27
[16] Hayashi M and Takeuchi Y 2019 Verifying commuting quantum computations via fidelity estimation of weighted graph states New J. Phys. 21 093060
[17] Li Z B, Han Y G and Zhu H J 2019 Efficient verification of bipartite pure states Phys. Rev. A 100 032316
[18] Yu X D, Shang J W and Ghone O 2019 Optimal verification of general bipartite pure states npj Quantum Inf. 5 112
[19] Zha H J and Hayashi M 2019 Efficient verification of pure quantum states in the adversarial scenario Phys. Rev. Lett. 123 260504
[20] Zha H J and Hayashi M 2019 General framework for verifying pure quantum states in the adversarial scenario Phys. Rev. A 100 062335
[21] Fujii K, Kobayashi H, Morimae T, Nishimura H, Tamate S and Tani S 2015 Power of quantum computation with few clean qubits (arXiv:1509.07276)
[22] Wang K and Hayashi M 2019 Optimal verification of two-qubit pure states Phys. Rev. A 100 023215
[23] Liu J, Jing X-X and Wang X G 2013 Phase-matching condition for enhancement of phase sensitivity in quantum metrology Phys. Rev. A 88 042316
[24] Giovannetti V, Lloyd S and Maccone L 2006 Quantum metrology Phys. Rev. Lett. 96 010401
[25] Shao Y, Liu B, Zhang M, Yang H and Liu J 2020 Operational definition of a quantum speed limit Phys. Rev. Res. 2 023299
[26] Zhang M, Yu H-M, Yuan H, Wang X G, Demkowicz-Dobrzański R and Liu J 2022 QuantumEstimation: an open-source toolkit for quantum parameter estimation Phys. Rev. Res. 4 043057
[27] Liu J, Zhang M, Chen H Z, Wang L N and Yuan H 2022 Optimal scheme for quantum metrology Adv. Quantum Technol. 5 2100080
[28] Shettell N and Markham D 2020 Graph states as a resource for quantum metrology Phys. Rev. Lett. 124 110502
[29] Liu J, Yuan H, Lu X-M and Wang X G 2020 Quantum Fisher information matrix and multiparameter estimation J. Phys. A: Math. Theor. 53 023001
[30] Liu J, Xiong H-N, Song F and Wang X G 2014 Fidelity susceptibility and quantum Fisher information for density operators with arbitrary ranks Physica A 410 167–73
[31] Szczysyłłska M, Baumgärtz T and Datta A 2016 Multi-parameter quantum metrology Adv. Phys. X 1 621
[32] Liu J, Jing X-X, Zhong W and Wang X G 2014 Quantum Fisher information for density matrices with arbitrary ranks Commun. Theor. Phys. 61 45–50
[33] Liu J and Yuan H 2017 Quantum parameter estimation with optimal control Phys. Rev. A 96 012117
[34] Liu J and Yuan H 2017 Control-enhanced multiparameter quantum estimation Phys. Rev. A 96 042114
[35] Yuan H D 2016 Sequential feedback scheme outperforms the parallel scheme for Hamiltonian parameter estimation Phys. Rev. Lett. 117 160801
[36] Liu J, Jing X-X and Wang X G 2015 Quantum metrology with unitary parametrization processes Sci. Rep. 5 8565
[37] Liu J, Lu X, Ma J and Wang X G 2012 Fidelity and fidelity susceptibility based on Hilbert-Schmidt inner product Sci. China Phys. Mech. Astron. 55 1529–34
[38] Eric D, Alexei K, Andrew L and John P 2002 Topological quantum memory J. Math. Phys. 43 4452
[39] Rausendorf R, Harrington J and Goyal K 2007 Topological fault-tolerance in cluster state quantum computation New J. Phys. 9 199
[40] Bremner M J, Montanaro A and Shepherd D J 2016 Average-case complexity versus approximate simulation of commuting quantum computations Phys. Rev. Lett. 117 080501
[41] Bremner M J, Jozsa R and Shepherd D J 2011 Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy Proc. R. Soc. A 467 459–72
[42] Fuji K and Morimae T 2017 Quantum commuting circuits and complexity of Ising partition functions New J. Phys. 19 033003
[43] Rossi M, Huber M, Bru D and Macchiavello C 2013 Quantum hypergraph states New J. Phys. 15 113022
[44] Zhu H J and Hayashi M 2019 Efficient verification of hypergraph states Phys. Rev. Appl. 12 054047
[45] Qu R, Wang J, Li Z S and Bao Y-R 2013 Encoding hypergraphs into quantum states Phys. Rev. A 87 022311
[46] Xiong F-L, Zhen Y-Z, Cao W-F, Chen K and Chen Z-B 2018 Qudit hypergraph states and their properties Phys. Rev. A 97 012323
[47] Briegel H J, Browne D E, Dur W, Raussendorf R and Van den Nest M 2009 Measurement-based quantum computation Nat. Phys. 5 19–26
[48] Raussendorf R, Browne D E and Briegel H J 2003 Measurement-based quantum computation on cluster states Phys. Rev. A 68 022312
[49] Li K and Smith G 2015 Quantum de Finetti theorem under fully-one-way adaptive measurements Phys. Rev. Lett. 114 160503
[50] Broadbent A, Fitzsimons J and Kashefi E 2010 Universal blind quantum computation IEEE Symp. on Foundations of Computer Science 2009 (FOCS’09) pp 517–26
[51] Broadbent A, Fitzsimons J and Kashefi E 2010 Measurement-based and universal blind quantum computation (Berlin: Springer)
[52] Morimae T and Fuji K 2013 Secure entanglement distillation for double-server blind quantum computation Phys. Rev. Lett. 111 020502
[53] Li Q, Chan W H, Wu C H and Wen Z H 2014 Triple-server blind quantum computation using entanglement swapping Phys. Rev. A 89 040302(R)
[54] Morimae T and Fuji K 2013 Keisuke, Blind quantum computation protocol in which Alice only makes measurements Phys. Rev. A 87 050301(R)
[55] Zhang X 2018 Measurement-based universal blind quantum computation with minor resources Quantum Inf. Process. 21 14
[56] Briegel H J, Browne D E, Dr W, Raussendorf R and Van den Nest M 2009 Measurement-based quantum computation Nat. Phys. 5 19–26
[57] Raussendorf R, Browne D E and Briegel H J 2003 Measurement-based quantum computation on cluster states Phys. Rev. A 68 022312
[58] Miller J and Miyake A 2016 Hierarchy of universal entanglement in 2D measurement-based quantum computation npj Quantum Inf. 2 16036
[59] Wallman J, Granade C, Harper R and Flammia S T 2015 Estimating the coherence of noise New J. Phys. 17 113020
[60] Ball H, Stace T M, Flammia S T and Biercuk M J 2016 Effect of noise on correlations of randomized benchmarking Phys. Rev. A 93 022303
[61] Dawson C M, Haselgrove H L and Nielsen M A 2006 Noise thresholds for optical quantum computers Phys. Rev. Lett. 96 020501
[62] Dawson C M, Haselgrove H L and Nielsen M A 2006 Noise thresholds for optical cluster-state quantum computation Phys. Rev. A 73 052306
[63] Raussendorf R, Harrington J and Goyal K 2007 Topological fault-tolerance in cluster state quantum computation New J. Phys. 9 199
[64] Fowler A G, Stephens A M and Groszkowski P 2009 High-threshold universal quantum computation on the surface code Phys. Rev. A 80 052312
[65] Fuji K 2015 Quantum Computation With Topological Codes: From Qubit to Topological Fault-Tolerance (Springer Briefs in Math-Ematical Physics vol 8) (Berlin: Springer)
[66] Steane A M 1999 Efficient fault-tolerant quantum computing Nature 399 124
[67] Tsun A 2020 Probability and Statistics With Applications to Computing (University of Washington) accepted (available at: www.alextsun.com/files/Prob_Stat_for_CS_Book.pdf)