Efficient verification of hypergraph states

Huangjun Zhu\textsuperscript{1,2,3,4,5,∗} and Masahito Hayashi\textsuperscript{6,7,8}

\textsuperscript{1}Department of Physics and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China  
\textsuperscript{2}State Key Laboratory of Surface Physics, Fudan University, Shanghai 200433, China  
\textsuperscript{3}Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China  
\textsuperscript{4}Collaborative Innovation Center of Advanced Microstructures, Nanjing 210093, China  
\textsuperscript{5}Institute for Theoretical Physics, University of Cologne, Cologne 50937, Germany  
\textsuperscript{6}Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan  
\textsuperscript{7}Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055, China  
\textsuperscript{8}Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore

(Dated: June 15, 2018)

Quantum states with genuine multipartite entanglement, such as hypergraph states, are of central interest in quantum information processing and foundational studies. Efficient verification of these states is a key to various applications. Here we propose a simple method for verifying hypergraph states which requires only two distinct Pauli measurements for each party, but its efficiency is comparable to the best nonlocal collective strategy. For a given state, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. Our protocol is exponentially more efficient than all known candidates based on local measurements, including tomography and direct fidelity estimation. Moreover, our protocol enables the verification of hypergraph states and genuine multipartite entanglement of thousands of qubits. Furthermore, our approach can be applied even in the adversarial scenario and is thus particularly appealing to applications like blind measurement-based quantum computation.

I. INTRODUCTION

Entanglement is the characteristic feature of quantum theory and a key resource in quantum information processing. As an archetypal example of quantum states with genuine multipartite entanglement (GME), graph states are of central interest to (blind) quantum computation\textsuperscript{[1–5]}, quantum error correction\textsuperscript{[6, 7]}, quantum networks\textsuperscript{[8]}, and foundational studies on nonlocality\textsuperscript{[9–11]}. Hypergraph states\textsuperscript{[12–16]}, as a generalization of graph states, are equally useful in these research areas\textsuperscript{[17–21]}. Moreover, certain hypergraph states, like Union Jack states, possess a number of merits not shared by ordinary graph states. For example, they are universal for measurement-based quantum computation (MBQC) under only Pauli measurements\textsuperscript{[17, 18, 21]}, which is impossible for graph states; in addition, they possess symmetry-protected topological orders, which are a focus of ongoing research\textsuperscript{[17, 18, 22]}. Furthermore, hypergraph states are attractive for demonstrating quantum supremacy\textsuperscript{[23].}

The applications of hypergraph states rely crucially on our ability to verify them with local measurements that are accessible. However, no efficient method is known so far for verifying general hypergraph states, although graph states can be verified with reasonable efficiency\textsuperscript{[5, 24, 25]}. In general, the resource required in traditional tomography increases exponentially with the number of qubits. The same is true for more specialized and more efficient methods, such as compressed sensing\textsuperscript{[27]}. direct fidelity estimation (DFE)\textsuperscript{[28]}, and the method tailored for hypergraph states proposed in Ref.\textsuperscript{[19]}. Actually, it is already too prohibitive to verify hypergraph states of 15 qubits.

In this paper, we propose a simple method for verifying general (qubit and qudit) hypergraph states which requires only two distinct Pauli measurements for each party. To verify an $n$-qubit hypergraph state, our protocol requires at most $n$ (potential) measurement settings and $cn/\epsilon$ measurements in total, where $c$ is the infidelity required and $c$ is a constant depending on the significance level. For a given hypergraph state, $n$ can be replaced by the chromatic number or degree (plus one) of the underlying hypergraph. The efficiency of our protocol has a simple graph theoretic interpretation. For many interesting families of graph and hypergraph states, including cluster states and Union Jack states, the number of measurement settings and that of measurements do not increase with the number of qubits. For example, the Union Jack states can be verified with only three measurement settings and $3c/\epsilon$ measurements in total.

Our protocol is exponentially more efficient than known candidates, including tomography and DFE. They enable the verification of hypergraph states and GME of thousands of qubits, which are more than enough for demonstrating quantum supremacy. Furthermore, our protocol can be applied even in the adversarial scenario in which the states are prepared by a potentially malicious adversary. This feature is particularly appealing to blind MBQC\textsuperscript{[1]–[4]} and many other applications in which security requirement is high.

\href{mailto:zhuhuangjun@fudan.edu.cn}{zhuhuangjun@fudan.edu.cn}
II. VERIFICATION OF PURE STATES

Consider a device that is supposed to produce the target state $|\Psi\rangle$ in the (generally multipartite) Hilbert space $\mathcal{H}$. In practice, the device may actually produce $\sigma_1, \sigma_2, \ldots, \sigma_N$ in $N$ runs. We assume that the fidelity $\langle\Psi|\sigma_j|\Psi\rangle$ is either 1 or satisfies $\langle\Psi|\sigma_j|\Psi\rangle \leq \epsilon$ for all $j$ [20]. Now the task is to determine which is the case. This conclusion is useful if we assume the next state $\sigma_{N+1}$ produced has the same behavior as the previous ones.

To achieve this task we can perform two-outcome measurements from a set of accessible measurements. Here we are interested in local projective measurements that are most relevant in practice. Each two-outcome projective measurement $\{P_i, 1 - P_i\}$ is specified by a projector $P_i$, which corresponds to passing the test, and is performed with probability $\mu_i$. Here we assume that the target state $|\Psi\rangle$ always passes the test, that is, $P_i|\Psi\rangle = |\Psi\rangle$ for all $P_i$. When $\langle\Psi|\sigma_j|\Psi\rangle \leq 1 - \epsilon$, by contrast, the maximal probability that $\sigma_j$ can pass the test is given by [20] (see also the supplementary material)

$$\max_{\langle\Psi|\sigma_j|\Psi\rangle \leq 1 - \epsilon} \text{tr}(\Omega \sigma) = 1 - [1 - \lambda_2(\Omega)]\epsilon = 1 - \nu(\Omega)\epsilon, \quad (1)$$

where $\Omega := \sum_i \mu_i P_i$ is referred to as a verification operator and a strategy, $\lambda_2(\Omega)$ is the second largest eigenvalue of $\Omega$, and $\nu(\Omega) := 1 - \lambda_2(\Omega)$ is the spectral gap from the maximal eigenvalue.

After $N$ runs, $\sigma_j$ in the bad case can pass all tests with probability at most $[1 - \nu(\Omega)]^N$. Solving the equation $\delta = [1 - \nu(\Omega)]^N$ yields $\epsilon = (1 - \delta^{1/N})/\nu(\Omega) \leq -\ln \delta/\nu(\Omega)$, assuming $\delta > 0$. If all $N$ tests are passed, with significance level $\delta$, we can guarantee the state $\sigma_{N+1}$ satisfies

$$\langle\Psi|\sigma_{N+1}|\Psi\rangle \geq 1 - \frac{\delta^{1/N}}{\nu(\Omega)} \geq 1 - \frac{\ln \delta^{-1}}{N\nu(\Omega)}. \quad (2)$$

Note that the significance level is the maximum passing probability when the state $\sigma_{N+1}$ does not satisfy Eq. (2). Hence, to guarantee the condition $\langle\Psi|\sigma_{N+1}|\Psi\rangle \geq 1 - \epsilon$ with significance level $\delta$, it suffices to satisfy [20]

$$N \geq \frac{1}{\nu(\Omega)\epsilon} \ln \delta^{-1}. \quad (3)$$

The optimal protocol is obtained by maximizing the spectral gap $\nu(\Omega)$. If there is no restriction on the measurements, then the optimal protocol is composed of the projective measurement $\{|\Psi\rangle\langle\Psi|, 1 - |\Psi\rangle\langle\Psi|\}$, which case $\Omega = |\Psi\rangle\langle\Psi|$, $\nu(\Omega) = 1$, and $N \approx \frac{1}{2} \ln \delta^{-1}$. In practice, however, $|\Psi\rangle$ is usually entangled, and it is very difficult to perform such entangling measurements. It is therefore crucial to devise efficient protocols based on local projective measurements, which is a focus of this paper.

When all $\sigma_j$ are identical to $\sigma$, let $F = \langle\Psi|\sigma|\Psi\rangle$; then $F \leq \text{tr}(\Omega \sigma) \leq \nu(\Omega) F + 1 - \nu(\Omega)$, which implies that

$$1 - \frac{\text{tr}(\Omega \sigma)}{\nu(\Omega)} \leq 1 - F \leq \nu(\Omega)^{-1}[1 - \text{tr}(\Omega \sigma)]. \quad (4)$$

So the passing probability $\text{tr}(\Omega \sigma)$ provides upper and lower bounds for the fidelity (or infidelity). In general, Eq. (4) still holds if $F$ and $\text{tr}(\Omega \sigma)$ are replaced by the average over all $\sigma_j$.

Next, consider the adversarial scenario in which the device is controlled by a potentially malicious adversary and may produce an arbitrary state $\rho$ on the whole system $\mathcal{H}^{\otimes (N+1)}$, as encountered in blind MBQC. Our task is to ensure that the reduced state on one system has infidelity less than $\epsilon$ by performing $N$ tests on other systems. To this end, we randomly choose $N$ systems and apply the strategy $\Omega$ to each system chosen. Since $N$ systems are chosen randomly, without loss of generality, we assume that $\rho$ is permutation invariant.

If $N$ tests are passed with significance level $\delta > 0$, then the reduced state on the remaining system is given by $\sigma_{N+1} = \rho_p^{-1} \text{tr}'[(\Omega \otimes 1) \rho]$, where $\rho_p := \text{tr}[(\Omega \otimes N) \otimes 1] \rho$ and $\text{tr}'$ means the partial trace over systems $1, 2, \ldots, N$. We have $\langle\Psi|\sigma_{N+1}|\Psi\rangle \geq F(N, \delta, \Omega)$ with

$$F(N, \delta, \Omega) := \min_\rho \{\rho_p^{-1} f_\rho | f_\rho \geq \delta\}, \quad (5)$$

where $f_\rho := \text{tr}[(\Omega \otimes N) \otimes 1] \rho$. The following theorem is proved in the supplementary material.

**Theorem 1.** We have

$$F(N, \delta, \Omega) \geq \frac{1 - \frac{1}{N} \delta}{\nu(\Omega)}; \quad (6)$$

the inequality is saturated when $\delta \geq \delta^* := \frac{1 + N(1 - \nu(\Omega))}{N + 1}$. If $\nu(\Omega) \geq 1/2$, then

$$F(N, \delta, \Omega) \geq 1 - \frac{1}{\delta (N + 1)}; \quad (7)$$

the inequality is saturated if $\Omega$ has an eigenvalue equal to zero and $1/(N + 1) \leq \delta \leq \delta^*$.

The lower bound in Eq. (6) is positive only when $\delta > 1/[N\nu(\Omega) + 1]$, and the one in Eq. (7) is positive only when $\delta > 1/(N + 1)$. The two bounds coincide when $\delta = \delta^*$. Equation (3) is optimal when $\delta \geq \delta^*$, while Eq. (7) is better when $\delta < \delta^*$. The lower bound in Eq. (7) under the condition $\nu(\Omega) \geq 1/2$ was also given in Ref. [21] with a slightly different situation.

By Theorem 1 the condition $\langle\Psi|\sigma_{N+1}|\Psi\rangle \geq 1 - \epsilon$ can be guaranteed with significance level $\delta$ as long as

$$N \geq \frac{1 - \delta}{\delta \nu(\Omega)}. \quad (8)$$

Therefore, the state $|\Psi\rangle$ can be verified efficiently even in the adversarial scenario if we can find a strategy $\Omega$ with sufficiently large $\nu(\Omega)$.

The above analysis can be extended to the scenario in which we want to verify whether the support of the resultant state belongs to a certain subspace $\mathcal{K}$. In this case, we need to replace the projector $|\Psi\rangle\langle\Psi|$ by the projector $P$ onto the subspace $\mathcal{K}$, impose the condition $P_i P = P$, and redefine $f_\rho$ as $\text{tr}[(\Omega \otimes N \otimes P) \rho]$. Such extension is useful when we want to verify whether the resultant state is correctable in a fault-tolerant way [24].
III. HYPERGRAPHS

A hypergraph \( G = (V, E) \) is characterized by a set of vertices \( V = \{1, 2, \ldots, n\} \) and a set of hyperedges \( E \subseteq \mathcal{P}(V) \), where \( \mathcal{P}(V) \) is the power set of \( V \) \cite{13, 14}. The order of a hyperedge is the number of vertices it connects, and the order of a hypergraph is the maximal order of its hyperedges. A graph is a special hypergraph in which all hyperedges have order 2 as ordinary edges.

Two distinct vertices of \( G \) are adjacent if they are connected by a hyperedge. The degree of a vertex is the number of vertices that are adjacent to it; the degree \( \Delta(G) \) of \( G \) is the maximal vertex degree. A subset of the vertex set \( V \) is a clique if every two vertices are adjacent. The clique number \( \varpi(G) \) of \( G \) is the maximal number of vertices over all cliques. By contrast, a subset is an independence set if no two vertices are adjacent. The independence number \( \alpha(G) \) of \( G \) is the maximal number of vertices over all independence sets.

A set of independence sets \( \mathcal{A} = \{A_1, A_2, \ldots, A_m\} \) of \( G \) is an independence cover if \( \bigcup_{j=1}^{m} A_j = V \). The cover \( \mathcal{A} \) also defines a coloring of \( G \) with \( m \) colors when \( \mathcal{A} \) forms a partition of \( V \), that is, when \( A_j \) are pairwise disjoint (assuming no \( A_j \) is empty). The chromatic number \( \chi(G) \) of \( G \) is the minimal number of colors in any coloring of \( G \). A weighted independence cover \((\mathcal{A}, \mu)\) is a cover together with weights \( \mu_l \) for \( A_l \in \mathcal{A} \). Throughout this paper, we assume that \( \mu_k \) form a probability distribution, that is, \( \mu_k \geq 0 \) and \( \sum_l \mu_l = 1 \). The cover strength of \((\mathcal{A}, \mu)\) is defined as

\[
s(\mathcal{A}, \mu) = \min_{j \in V} \sum_{l|A_l \ni j} \mu_l.
\]

The independence degree \( \gamma(G) \) of \( G \) is the maximum of \( s(\mathcal{A}, \mu) \) over all weighted independence covers. The following result is proved in the supplementary material.

**Proposition 1.** Any hypergraph \( G = (V, E) \) satisfies

\[
\frac{1}{\Delta(G) + 1} \leq \frac{1}{\chi(G)} \leq \gamma(G) \leq \min \left\{ \frac{\alpha(G)}{|V|}, \frac{1}{\varpi(G)} \right\}.
\]

IV. HYPERGRAPH STATES

Let \( X := \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \) and \( Z := \text{diag}(1, -1) \) be two Pauli matrices for a qubit. The Pauli matrices for the \( j \)th qubit are indexed by the subscript \( j \). Given any hypergraph \( G \) with \( n \) vertices, we can construct an \( n \)-qubit hypergraph state \(|G\rangle\) as follows: prepare the state \(|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \) (eigenstate of \( X \) with eigenvalue 1) for each vertex of \( G \) and apply the generalized controlled-\( Z \) operation \( CZ_e \) on the vertices of each hyperedge \( e \) \cite{13, 14}, that is, \(|G\rangle = (\prod_{e \in E} CZ_e)|+\rangle^{\otimes n} \). Here \( CZ_e = \bigotimes_{j \in e} 1_j - 2 \bigotimes_{j \in e} |1\rangle\langle 1|_j \), which acts trivially on \( V \setminus e \). When \( e \) contains a single vertex, \( CZ_e \) reduces to the Pauli operator \( Z \) on the vertex, which is local. In addition, \( CZ_e \) is the familiar controlled-\( Z \) operation when \( e \) connects two vertices. Alternatively, \(|G\rangle \) is the unique eigenstate (up to a global phase factor) of the \( n \) commuting (non-local) stabilizer operators \cite{13, 14}

\[
K_j = X_j \otimes \prod_{e \in E | e \ni j} CZ_e, \quad j = 1, 2, \ldots, n.
\]

This alternative definition will play a key role in the verification of hypergraph states. The definition of hypergraph states can also be generalized to the qudit setting \cite{15, 16}; see the supplementary material for more details.

The order of a hypergraph state is defined as the order of the underlying hypergraph; similar convention applies to many other graph theoretic quantities, such as the degree, clique number, independence number, chromatic number, and independence degree. Any hypergraph state of a connected hypergraph is genuinely multipartite entangled (GME) in the sense that it cannot be written as a tensor product of two states \cite{13}. Hypergraph states are particularly appealing because of many merits. In particular, certain hypergraph states, such as Union Jack states shown in Fig. 1 are universal for MBQC under Pauli measurements \cite{17, 18, 19}. When \( G \) is an ordinary graph, \(|G\rangle \) reduces to a graph state. All stabilizer states are equivalent to graph states under local Clifford transformations (LC) \cite{20, 21}. In addition, any graph state of a 2-colorable graph can be turned into a Calderbank-Shor-Steane (CSS) state under LC, and vice versa \cite{22}.

V. VERIFICATION OF HYPERGRAPH STATES

Before introducing the verification protocol for hypergraph states, it is instructive to determine the minimal
number of measurement settings for each party. The following result is proved in the supplementary material.

**Proposition 2.** To verify a connected hypergraph state, each party needs at least two projective measurements.

Surprisingly, two measurement settings for each party are also sufficient for verifying any hypergraph state. Let \( G = (V,E) \) be a hypergraph and \( (G) \) the associated hypergraph state. Choose an independence cover \( \mathcal{A} = \{A_1, A_2, \ldots, A_m\} \) of \( G \) and let \( \mathcal{A}_i := V \setminus A_i \) be the complement of \( A_i \) in \( V \). Then we can construct a verification protocol with \( m \) tests (measurement settings): the \( l \)th test consists in measuring \( X_j \) for all \( j \in A_l \) and measuring \( Z_k \) for all \( k \in \mathcal{A}_l \). The measurement outcome on the \( a \)th qubit for \( a = 1, 2, \ldots, n \) can be written as \((-1)^{\alpha_a}\), where the Boolean variable \( \alpha_a \) is either 0 or 1. Note that \( X_j \) and \( Z_k \) commute with \( K_i \) for all \( i, j \in A_l \) and \( k \in \mathcal{A}_l \). In addition, the joint eigenstate of \( X_j \) and \( Z_k \) corresponding to the outcome \( \alpha_a \) is an eigenstate of \( K_i \), whose eigenvalue is \((-1)^{l_i}\) with \( l_i = \alpha_l + \sum_{l \in E} \prod_{l \in E, k \neq i} o_k \) according to Eq. (11). The test is passed if \((-1)^{l_i} = 1\) for all \( i \in A_l \)

The projector onto the pass eigenspace associated with the \( l \)th test reads

\[
P_l = \prod_{i \in A_l} \frac{1 + K_i}{2}.
\]

A state can pass all \( m \) tests if it is stabilized by \( K_i \) for all \( i \in \bigcup_{l=1}^m A_l = V \). So only the target state \( |G\rangle \) can pass all tests with certainty as desired. This verification protocol will be referred to as the cover protocol (or coloring protocol when \( \mathcal{A} \) defines a coloring of \( G \)).

Suppose the \( l \)th test is applied with probability \( \mu_i \). The efficiency of the resulting protocol is determined by the spectral gap of \( \Omega(\mathcal{A}, \mu) = \sum_{l=1}^m \mu_l P_l \). Note that the common eigenbasis of \( K_i \) for \( i \in V \) also form an eigenbasis of \( \Omega(\mathcal{A}, \mu) \). Each eigenstate \( |\Psi_x\rangle \) in this basis is specified by an \( n \) bit string \( x \in \{0,1\}^n \) and satisfies \( K_i |\Psi_x\rangle = (-1)^{x_i} |\Psi_x\rangle \). The corresponding eigenvalue of \( \Omega(\mathcal{A}, \mu) \) reads \( \lambda_x = \sum_{x \in \text{supp}(x) \subseteq \mathcal{A}} \mu_i \), where \( \text{supp}(x) := \{ i | x_i \neq 0 \} \). The second largest eigenvalue of \( \Omega(\mathcal{A}, \mu) \) can be attained when \( x \) has only one bit equal to 1, so that \( \nu(\Omega(\mathcal{A}, \mu)) = \min_{x \in V} \sum_{i} \mu_i = s(\mathcal{A}, \mu) \), which confirms the following theorem.

**Theorem 2.**

\[
\nu(\Omega(\mathcal{A}, \mu)) = s(\mathcal{A}, \mu), \quad \max_{\mathcal{A}, \mu} \nu(\Omega(\mathcal{A}, \mu)) = \gamma(G). \tag{13}
\]

This theorem reveals the operational meanings of cover strength and independence degree in the verification of hypergraph states. To verify \( (G) \) within infidelity \( \epsilon \) and significance level \( \delta \), the number of tests required is about \( s(\mathcal{A}, \mu) \epsilon^{-1} \ln \delta^{-1} \). This number is minimized for optimal independence covers, with the result

\[
N \approx \frac{1}{\gamma(G)} \ln \delta^{-1} \leq \frac{\chi(G)}{\epsilon} \ln \delta^{-1} \leq \frac{\Delta(G) + 1}{\epsilon} \ln \delta^{-1}, \tag{14}
\]

where the upper bound \( \chi(G) \epsilon^{-1} \ln \delta^{-1} \) can be achieved by any cover (or coloring) of \( \gamma(G) \) elements and with uniform weights. In general, it is not easy to find an optimal independence cover or to compute \( \gamma(G), \gamma(G) \). Fortunately, the rightmost bound in Eq. (14) is very easy to compute and can be achieved by a coloring constructed from a simple greedy algorithm as presented in the proof of Proposition 1 in the supplementary material. By virtue of Eq. (14), we can also provide upper and lower bounds for the infidelity. In addition, Theorem 2 also applies to qudit hypergraph states, as shown in the supplementary material.

The above analysis shows that any hypergraph state can be verified with only \( m = \Delta(G) + 1 \) settings of Pauli measurements in which each party performs either \( X \) or \( Z \) measurement. The total number of tests scales as \( 1/\epsilon \) and is at most \( m \) times as large as the best nonlocal collective protocol. The cover protocol for verifying hypergraph states is exponentially more efficient than protocols known before \( [19, 25] \); cf. Fig. 2 and the supplementary material. Consider the protocol of Ref. [19] for example, both the number of measurement settings and the total number of tests increase exponentially with \( \Delta(G) \); in addition, the total number of tests scales as \( 1/\epsilon^2 \) instead of \( 1/\epsilon \). For graph states, although several methods are available \( [26, 25] \), our protocol is appealing as it usually requires much fewer measurement settings compared with known candidates. Since all stabilizer states are equivalent to graph states under LC \( [29, 30] \), our protocol can easily be adapted for general stabilizer states.

For many interesting families of hypergraph states, the chromatic numbers do not grow with the number of qubits. Most hypergraph states of practical interest are generated by short-range interactions, so their degrees and chromatic numbers are upper bounded by a small constant. In this case, the cover protocol has optimal scaling behavior as the best nonlocal collective strategy. For example, only two measurement settings are necessary for all graph states of 2-colorable graphs, including GHZ states, cluster states (of arbitrary dimensions), CSS states (up to LC), tree graph states, and graph states associated with even cycles. Only three measurement settings are necessary for order-3 cluster states and Union Jack states. The efficiency of the cover protocol is illustrated in Fig. 2.
VI. DETECTION OF GENUINE MULTIPARTITE ENTANGLEMENT

Here we show that the cover protocol can also be applied to detecting GME of hypergraph states, although it is not necessarily optimized for this purpose. Recall that a multipartite pure state is GME if it is not biseparable, that is, if it cannot be written as a tensor product of two pure states. A mixed state is GME if it cannot be written as a convex mixture of biseparable states [32].

Theorem 3. Let G be a connected order-k hypergraph and |G⟩ the corresponding hypergraph state. If the state ρ satisfies ⟨G|ρ|G⟩ > 1 − 2k−k, then ρ is GME.

This theorem was proved in Ref. [33]; see the supplementary material for an independent proof. When |G⟩ is a graph state, Theorem 3 is known much earlier [32, 34, 35, in which case ρ is GME if its fidelity with |G⟩ is larger than one half. In view of Eq. (14), to certify GME of |G⟩ with significance level δ, it suffices to perform

\[ N \approx 2^{k-1} \chi(G) \ln \delta^{-1} \]

tests, that is, \( 3 \times 2^{k-1} \chi(G) \) tests when \( \delta = 0.05 \). This number is independent of the number of qubits as long as the order and chromatic number are fixed. For example, GME of 2-colorable graph states can be certified with only 4 ln δ−1 tests (12 tests when \( \delta = 0.05 \)); for order-3 cluster states and Union jack states, it suffices to perform 12 ln δ−1 tests (36 tests when \( \delta = 0.05 \)).

Although detection of GME has been discussed in many works, our approach is appealing for at least three reasons. First, our approach is based on state verification, which can provide more precise information about the state than entanglement detection usually based on witness operators. Such information is crucial to many practical applications, such as MBQC. Second, our approach requires much fewer measurement settings and tests than most previous works on the detection of GME. Third, given a significance level, we can determine the number of required tests explicitly, which is not the case for most previous works.

In summary, we introduced a simple method for verifying (qubit and qudit) hypergraph states which requires only two distinct Pauli measurements for each party. Our protocol is exponentially more efficient than known candidates based on local measurements and is comparable to the best nonlocal collective strategy. In general, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. Our protocol enables the verification of hypergraph states and GME of thousands of qubits, which is instrumental in quantum information processing and in demonstrating quantum supremacy. Moreover, our protocol can be applied in the adversarial scenario and is thus particularly appealing to blind MBQC. Besides quantum information processing, our work and its generalization may find potential applications in studying many-body physics.

ACKNOWLEDGMENTS

HZ is grateful to Zhibo Hou and Jiangwei Shang for discussions. HZ acknowledges financial support from the Excellence Initiative of the German Federal and State Governments Zukunftskonzept (ZUK 81) and the Deutsche Forschungsgemeinschaft (DFG) in the early stage of this work. MH was 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.
[1] R. Raussendorf and H. J. Briegel, “A one-way quantum computer,” Phys. Rev. Lett. 86, 5188–5191 (2001).
[2] R. Raussendorf, D. E. Browne, and H. J. Briegel, “Measurement-based quantum computation on cluster states,” Phys. Rev. A 68, 022312 (2003).
[3] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal blind quantum computation,” in Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS’09 (2009) pp. 517–526.
[4] T. Morimae and K. Fujii, “Blind quantum computation protocol in which Alice only makes measurements,” Phys. Rev. A 87, 050301 (2013).
[5] M. Hayashi and T. Morimae, “Verifiable measurement-only blind quantum computing with stabilizer testing,” Phys. Rev. Lett. 115, 220502 (2015).
[6] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. thesis, California Institute of Technology (1997), available at http://arxiv.org/abs/quant-ph/9705052.
[7] D. Schlingemann and R. F. Werner, “Quantum error-correcting codes associated with graphs,” Phys. Rev. A 65, 012308 (2001).
[8] S. Perseguers, G. J. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, and A. Acín, “Distribution of entanglement in large-scale quantum networks,” Rep. Prog. Phys. 76, 096001 (2013).
[9] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, “Bell’s theorem without inequalities,” American J. Phys. 58, 1131–1143 (1990).
[10] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, “Nonlocality of cluster states of qubits,” Phys. Rev. A 71, 042325 (2005).
[11] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, “Bell inequalities for graph states,” Phys. Rev. Lett. 95, 120405 (2005).
[12] C. Kruszynska and B. Kraus, “Local entanglability and multipartite entanglement,” Phys. Rev. A 79, 020320 (2009).
[13] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, “Encoding hypergraphs into quantum states,” Phys. Rev. A 87, 022311 (2013).
[14] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, “Quantum hypergraph states,” New J. Phys. 15, 113022 (2013).
[15] F. E. S. Steinhoff, C. Ritz, N. I. Miklin, and O. Gühne, “Qudit hypergraph states,” Phys. Rev. A 95, 052340 (2017).
[16] F.-L. Xiong, Y.-Z. Zhen, W.-F. Cao, K. Chen, and Z.-B. Chen, “Qudit hypergraph states and their properties,” Phys. Rev. A 97, 012323 (2018).
[17] J. Miller and A. Miyake, “Hierarchy of universal entanglement in 2d measurement-based quantum computation,” npj Quantum Information 2, 16036 (2016).
[18] J. Miller and A. Miyake, “Latent computational complexity of symmetry-protected topological order with fractional symmetry,” Phys. Rev. Lett. 120, 170503 (2018).
[19] T. Morimae, Y. Takeuchi, and M. Hayashi, “Verification of hypergraph states,” Phys. Rev. A 96, 062321 (2017).
[20] M. Gachechiladze, C. Budroni, and O. Gühne, “Extreme violation of local realism in quantum hypergraph states,” Phys. Rev. Lett. 116, 070401 (2016).
[21] M. Gachechiladze, O. Gühne, and A. Miyake, “Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states,” (2018), arXiv:1805.12093.
[22] B. Yoshida, “Topological phases with generalized global symmetries,” Phys. Rev. B 93, 155131 (2016).
[23] M. J. Brenner, A. Montanaro, and D. J. Shepherd, “Average-case complexity versus approximate simulation of commuting quantum computations,” Phys. Rev. Lett. 117, 080501 (2016).
[24] K. Fujii and M. Hayashi, “Verifiable fault tolerance in measurement-based quantum computation,” Phys. Rev. A 96, 030301 (2017).
[25] M. Hayashi and M. Hajdušek, “Self-guaranteed measurement-based quantum computation,” Phys. Rev. A 97, 052308 (2018).
[26] S. Pallister, N. Linden, and A. Montanaro, “Optimal verification of entangled states with local measurements,” Phys. Rev. Lett. 120, 170502 (2018).
[27] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, “Quantum state tomography via compressed sensing,” Phys. Rev. Lett. 105, 150401 (2010).
[28] S. T. Flammia and Y.-K. Liu, “Direct fidelity estimation from few Pauli measurements,” Phys. Rev. Lett. 106, 230501 (2011).
[29] D. Schlingemann, “Stabilizer codes can be realized as graph codes,” Quantum Info. Comput. 2, 307–323 (2002).
[30] M. Grassl, A. Klappenecker, and M. Rötteler, “Graphs, quadratic forms, and quantum codes,” in Proceedings of the 2002 IEEE International Symposium on Information Theory (Lausanne, Switzerland, 2002) available at arXiv:quant-ph/0703112.
[31] K. Chen and H.-K. Lo, “Multi-partite quantum cryptographic protocols with noisy GHZ states,” Quantum Info. Comput. 7, 689–715 (2007).
[32] O. Gühne and G. Tóth, “Entanglement detection,” Phys. Rep. 474, 1 (2009).
[33] M. Ghio, D. Malpetti, M. Rossi, D. Bruß, and C. Macchiavello, “Multipartite entanglement detection for hypergraph states,” J. Phys. A: Math. Theor. 51, 045302 (2018).
[34] G. Tóth and O. Gühne, “Detecting genuine multipartite entanglement with two local measurements,” Phys. Rev. Lett. 94, 060501 (2005).
[35] G. Tóth and O. Gühne, “Entanglement detection in the stabilizer formalism,” Phys. Rev. A 72, 022340 (2005).
[36] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, “Local unitary symmetries of hypergraph states,” J. Phys. A: Math. Theor. 48, 095301 (2015).
Efficient verification of hypergraph states: Supplementary material

In this supplementary material, we present a simpler proof of Eq. (1), which was originally proved in Ref. [26]. We then provide more details about state verification in the adversarial scenario and prove Theorem 1 presented in the main text. Next, we prove Proposition 1 and determine the independence degrees of odd cycles. In addition, we prove Proposition 2 and Theorem 3, and provide more details on the verification of GHZ states. Furthermore, we generalize the cover protocol to verify qudit hypergraph states. Finally, we compare our approach with existing works.

I. PROOF OF EQ. (1)

Here we present a simpler proof of Eq. (1), which was originally proved in Ref. [26].

Proof. Suppose the verification operator \( \Omega \) has spectral decomposition \( \Omega = \sum_{j=1}^{D} \lambda_j \Pi_j \), where \( D \) is the dimension of the Hilbert space of interest, \( \lambda_j \) are the eigenvalues of \( \Omega \) arranged in decreasing order \( 1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D \), and \( \Pi_j \) are mutually orthogonal rank-1 projectors with \( \Pi_1 = |\Psi \rangle \langle \Psi| \). Without loss of generality, we may assume that \( \sigma \) is diagonal in the eigenbasis of \( \Omega \) because both \( \text{tr}(\Omega \sigma) \) and \( \langle \Psi | \sigma | \Psi \rangle \) only depend on the diagonal elements of \( \sigma \) in this basis. Suppose \( \sigma = \sum_{j=1}^{D} x_j \Pi_j \) with \( x_j \geq 0 \) and \( \sum_j x_j = 1 \).

\[
\langle \Psi | \sigma | \Psi \rangle = x_1, \quad \text{tr}(\Omega \sigma) = \sum_j \lambda_j x_j. \tag{S1}
\]

Therefore,

\[
\max_{\langle \Psi | \sigma | \Psi \rangle \leq 1-\epsilon} \text{tr}(\Omega \sigma) = \max_{x_j \geq 0, \sum_j x_j = 1, x_1 \leq 1-\epsilon} \sum_j \lambda_j x_j \leq 1 + \lambda_2(1 - x_1) \leq 1 - \nu(\Omega) \epsilon, \tag{S2}
\]

where \( \nu(\Omega) := 1 - \lambda_2 \).

II. STATE VERIFICATION IN THE ADVERSARIAL SCENARIO

In this section we provide more details on state verification in the adversarial scenario and provide an alternative definition of \( F(N, \delta, \Omega) \). We then prove Theorem 1 presented in the main text.

A. Preliminaries

Suppose we want to create the pure state \( |\Psi \rangle \in \mathcal{H} \), where \( \mathcal{H} \) has dimension \( D \), and ask the adversary to produce \( N + 1 \) copies of \( |\Psi \rangle \langle \Psi| \), that is, \( (|\Psi \rangle \langle \Psi|)^{\otimes (N+1)} \). In reality, the adversary may produce a correlated or even entangled state \( \rho \) on \( \mathcal{H}^{\otimes (N+1)} \). To verify the state produced by the adversary, we randomly choose \( N \) systems among the \( N + 1 \) systems and apply a certain test to each system chosen. The reduced state on the remaining system is kept if all tests are passed. Since \( N \) systems are chosen randomly, without loss of generality, we may assume that \( \rho \) is permutation invariant.

Suppose each test is determined by the verification operator \( \Omega \), then the probability that \( \rho \) can pass \( N \) tests is given by

\[
p_\rho = \text{tr}((\Omega^{\otimes N} \otimes 1) \rho). \tag{S3}
\]

The reduced state on system \( N + 1 \) (assuming \( p_\rho > 0 \)) is given by

\[
\sigma_{N+1} = \frac{\text{tr}_{1,\ldots,N}((\Omega^{\otimes N} \otimes 1) \rho)}{p_\rho}, \tag{S4}
\]

where \( \text{tr}_{1,\ldots,N} \) means the partial trace over the systems \( 1,2,\ldots,N \). The fidelity between \( \sigma_{N+1} \) and \( |\Psi \rangle \) reads

\[
F_\rho = \langle \Psi | \sigma_{N+1} | \Psi \rangle = \frac{f_\rho}{p_\rho}, \tag{S5}
\]
where
\[ f_\rho = \text{tr}[(\Omega^\otimes N \otimes |\Psi\rangle\langle\Psi|)\rho]. \tag{S6} \]

Our task is to minimize \( F_\rho \) for a given passing probability \( p_\rho = \delta \).

As in the proof of Eq. (11), suppose the verification operator \( \Omega \) has spectral decomposition \( \Omega = \sum_{j=1}^{D} \lambda_j \Pi_j \), where \( \lambda_j \) are the eigenvalues of \( \Omega \) arranged in decreasing order \( 1 = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_D \), and \( \Pi_j \) are mutually orthogonal rank-1 projectors with \( \Pi_1 = |\Psi\rangle\langle\Psi| \). Without loss of generality, we may assume that \( \rho \) is diagonal in the product basis constructed from the eigenbasis of \( \Omega \) (as determined by the projectors \( \Pi_j \)), since \( p_\rho, f_\rho \), and \( F_\rho \) only depend on the diagonal elements of \( \rho \). As mentioned above, \( \rho \) is also permutation invariant.

Let \( k = (k_1, k_2, \ldots, k_D) \) be a sequence of \( D \) nonnegative integers that sum up to \( N + 1 \), that is, \( \sum_j k_j = N + 1 \). Let \( \mathcal{S} \) be the set of all such sequences and let \( \mathcal{S}^* \) be the subset with the sequence \( k_0 := (N+1,0,\ldots,0) \) deleted. For each \( k \), we can define a permutation invariant diagonal density matrix \( \rho_k \) as the uniform mixture of all permutations of \( D \). Then any permutation invariant diagonal density matrix \( \rho \) can be expressed as \( \rho = \sum_k c_k \rho_k \), where \( c_k \) form a probability distribution on \( \mathcal{S} \). In addition,
\[
P_\rho = \sum_k c_k \eta_k(\lambda), \quad f_\rho = \sum_k c_k \zeta_k(\lambda), \quad F_\rho = \frac{f_\rho}{p_\rho} = \frac{\sum_k c_k \zeta_k(\lambda)}{\sum_k c_k \eta_k(\lambda)}, \tag{S7}\]
where \( \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_D) \) and
\[
\eta_k(\lambda) := p_{\rho_k} = \sum_{i,k_i \geq 1}^{k_i} \frac{k_i(N+1)}{\lambda_i + 1} \prod_{j \neq i,k_j \geq 1} \lambda_j^{k_j}, \quad \zeta_k(\lambda) := f_{\rho_k} = \frac{k_1}{N+1} \prod_{i,k_i \geq 1} \lambda_i^{k_i}. \tag{S8}\]

Here \( \lambda_i^{k_i-1} = 1 \) when \( k_i = 1 \) even if \( \lambda_i = 0 \). Note that \( \lambda_1 = 1 \) and \( \zeta_k(\lambda) \leq \eta_k(\lambda) \leq 1 \); the second inequality is saturated if \( k = k_0 \), in which case both inequalities are saturated, that is, \( \zeta_{k_0}(\lambda) = \eta_{k_0}(\lambda) = 1 \). Another sequence in \( \mathcal{S} \) that is of special interest is \( k_1 := (N+1,0,\ldots,0) \), at which we have
\[
\eta_{k_1}(\lambda) = \frac{1 + N\lambda_2}{N+1} = \frac{1 + N(1-\nu)}{N+1}, \quad \zeta_{k_1}(\lambda) = \frac{N\lambda_2}{N+1} = \frac{N(1-\nu)}{N+1}. \tag{S9}\]
where \( \nu \) is a shorthand of \( \nu(\Omega) = 1 - \lambda_2 \).

Define the region
\[
R_{N,\Omega} := \{ (p_\rho, f_\rho) | \forall \rho \}. \tag{S10}\]

Then \( R_{N,\Omega} \) is a convex hull of \( (\eta_k(\lambda), \zeta_k(\lambda)) \) for all \( k \in \mathcal{S} \). The function \( F(N,\delta,\Omega) \) is completely determined by \( R_{N,\Omega} \), although in general it is not easy to find an explicit analytical formula. In any case, the properties of \( \eta_k(\lambda) \) and \( \zeta_k(\lambda) \) will play an important role in the following discussions.

### B. Alternative definition of \( F(N,\delta,\Omega) \)

Before proving Theorem 1, we recall the definition of \( F(N,\delta,\Omega) \),
\[
F(N,\delta,\Omega) := \min_\rho \left\{ \frac{f_\rho}{p_\rho} \mid p_\rho \geq \delta \right\} = \min_\rho \left\{ \frac{\text{tr}[(\Omega^\otimes N \otimes |\Psi\rangle\langle\Psi|)\rho]}{\text{tr}[(\Omega^\otimes N \otimes 1)\rho]} \mid \text{tr}[(\Omega^\otimes N \otimes 1)\rho] \geq \delta \right\}. \tag{S11}\]

Note that \( F(N,\delta,\Omega) \) is nondecreasing in \( \delta \) by definition. Here we have an alternative definition, which is sometimes easier to use.
\[
\tilde{F}(N,\delta,\Omega) := \left\{ \min_\rho \left\{ \delta^{-1} f_\rho \mid p_\rho = \delta \right\} \mid \lambda_2^N < \delta \leq 1, \right. \tag{S12}
\begin{align*}
& 0 < \delta \leq \lambda_2^N. \left. \right\}
\end{align*}

**Lemma S1.** \( F(N,\delta,\Omega) = \tilde{F}(N,\delta,\Omega) \) for \( 0 < \delta \leq 1 \).
As an implication of Lemma [S1]

\[
\delta F(N, \delta, \Omega) := \begin{cases} 
\min_{p} \{ f_{\rho} | p_{\rho} = \delta \} & \lambda_{N}^\delta < \delta \leq 1, \\
0 & 0 < \delta \leq \lambda_{2}^N.
\end{cases}
\] (S13)

which implies that \( \delta F(N, \delta, \Omega) \) is convex in \( \delta \).

**Proof of Lemma [S2]** When \( 0 < \delta \leq \lambda_{N}^\delta \), we have \( F(N, \delta, \Omega) = 0 = \tilde{F}(N, \delta, \Omega) \). To see this, let \( \rho = \Pi_{2}^{(N+1)} \), then \( p_{\rho} = \lambda_{N}^\delta \) and \( F_{\rho} = f_{\rho} = 0 \), which implies that \( F(N, \delta, \Omega) = 0 \) for \( 0 < \delta \leq \lambda_{N}^\delta \).

When \( \delta > \lambda_{N}^\delta \), we have

\[ F(N, \delta, \Omega) = \min_{\delta' \geq \delta} \tilde{F}(N, \delta', \Omega), \] (S14)

which implies that \( F(N, \delta, \Omega) \leq \tilde{F}(N, \delta, \Omega) \). To prove the equality \( F(N, \delta, \Omega) = \tilde{F}(N, \delta, \Omega) \), it suffices to prove that \( \tilde{F}(N, \delta, \Omega) \) is nondecreasing in \( \delta \). Let \( \lambda_{N}^\delta < \delta_{2} \leq \delta \leq 1 \), suppose the minimum in the definition of \( \tilde{F}(N, \delta, \Omega) \) is attained at \( \rho \), that is, \( p_{\rho} = \delta \) and \( f_{\rho} = \delta \tilde{F}(N, \delta, \Omega) \). By assumption \( \delta_{2} \) can be expressed as a convex combination of \( \delta \) and \( \lambda_{N}^\delta \), that is, \( \delta_{2} = s\delta + (1-s)\lambda_{N}^\delta \) with \( 0 \leq s \leq 1 \). Let \( \rho_{2} = s\rho + (1-s)\Pi_{2}^{(N+1)} \), then

\[ p_{\rho_{2}} = s\delta + (1-s)\lambda_{N}^\delta = \delta_{2}, \quad f_{\rho_{2}} = s\delta \tilde{F}(N, \delta, \Omega). \] (S15)

Therefore,

\[ \tilde{F}(N, \delta_{2}, \Omega) \leq f_{\rho_{2}} = \frac{f_{\rho_{2}}}{p_{\rho_{2}}} = \frac{s\delta \tilde{F}(N, \delta, \Omega)}{s\delta + (1-s)\lambda_{N}^\delta} \leq \tilde{F}(N, \delta, \Omega). \] (S16)

Therefore, \( \tilde{F}(N, \delta, \Omega) \) is nondecreasing in \( \delta \), which implies the equality \( F(N, \delta, \Omega) = \tilde{F}(N, \delta, \Omega) \).

\( \square \)

**Proof of Theorem [I]**

First, we prove the inequality in Eq. (6). Let \( \rho = \sum_k c_k \rho_k \). If \( p_{\rho} = 1 \), then \( c_{k_{0}} = \delta_{k,k_{0}} \) and \( F_{\rho} = f_{\rho} = 1 \), so that \( F(N, \delta = 1, \Omega) = 1 \) and Eq. (6) holds. If \( 0 < p_{\rho} < 1 \), then \( c_{k_{0}} < 1 \),

\[
\frac{1 - p_{\rho}}{1 - f_{\rho}} = \frac{1 - \sum_{k \in \mathcal{I}^*} c_k \eta_k(\lambda)}{1 - \sum_{k \in \mathcal{I}^*} c_k \zeta_k(\lambda)} = \frac{1 - c_{k_{0}} - \sum_{k \in \mathcal{I}^*} c_k' \eta_k(\lambda)}{1 - c_{k_{0}} - \sum_{k \in \mathcal{I}^*} c_k' \zeta_k(\lambda)}
= \frac{1 - \sum_{k \in \mathcal{I}^*} c_k' \eta_k(\lambda)}{1 - \sum_{k \in \mathcal{I}^*} c_k' \zeta_k(\lambda)} = \sum_{k \in \mathcal{I}^*} c_k' \frac{[1 - \eta_k(\lambda)]}{\sum_{k \in \mathcal{I}^*} c_k' [1 - \zeta_k(\lambda)]},
\] (S17)

where \( c_k' := c_k/(1 - c_{k_{0}}) \) form a probability distribution on \( \mathcal{I}^* \). According to Lemma [S4] below, we have

\[
\frac{1 - p_{\rho}}{1 - f_{\rho}} \geq \min_{k \in \mathcal{I}^*} \frac{1 - \eta_k(\lambda)}{1 - \zeta_k(\lambda)} = \frac{1 - \eta_{k_{0}}(\lambda)}{1 - \zeta_{k_{0}}(\lambda)} = \frac{N\nu}{N\nu + 1},
\] (S18)

which implies that

\[
f_{\rho} \geq p_{\rho} - \frac{1 - p_{\rho}}{N\nu},
\] (S19)

so that

\[
F_{\rho} = \frac{f_{\rho}}{p_{\rho}} \geq 1 - \frac{1 - p_{\rho}}{N\nu p_{\rho} \nu}
\] (S20)

In view of Eq. (5) or Eq. (S11), we conclude that

\[
F(N, \delta, \Omega) \geq 1 - \frac{1 - \delta}{N\nu \delta},
\] (S21)
Incidentally, the above bound is negative and thus trivial when \( \delta \leq \lambda_2^N \) since \( \lambda_2^N < 1/(N\nu + 1) \).

Next, we show that the inequality in Eq. (21) that is, Eq. (S21) is saturated when \( \delta \geq \delta^* = \eta_{k_1}(\lambda) \).

To this end, it suffices to show that the inequality in Eq. (S19) can be saturated when \( p_\rho \geq \eta_{k_1}(\lambda) \).

When \( c_k = \delta_{k,k_0} \), that is, \( \rho = \rho_{k_0} = (|\Psi\rangle\langle\Psi|^\otimes(N+1)) \), we have \( p_\rho = 1 \) and \( f_\rho = 1 \), so Eq. (S19) is saturated. When \( c_k = \delta_{k,k_1} \), that is, \( \rho = \rho_{k_1} \), we have \( p_\rho = \eta_{k_1}(\lambda) \) and \( f_\rho = c_{k_1}(\lambda) \), so Eq. (S19) is also saturated. Since both \( p_\rho \) and \( f_\rho \) are linear in \( \rho \), it follows that the inequality in Eq. (S19) can be saturated by a convex combination of \( \rho_{k_0} \) and \( \rho_{k_1} \), whenever \( p_\rho \geq \eta_{k_1}(\lambda) \).

Next, we prove the inequality in Eq. (7) when \( \nu(\Omega) \geq \frac{1}{2} \). To this end, note that

\[
p_\rho - f_\rho = \sum_k c_k \eta_k(\lambda) - \sum_k c_k \zeta_k(\lambda) = \sum_k c_k [\eta_k(\lambda) - \zeta_k(\lambda)] \leq \frac{1}{N+1},
\]

(S22)

where the last inequality follows from Lemma S2 below. Therefore,

\[
F_\rho \geq 1 - \frac{1}{(N+1)p_\rho},
\]

(S23)

which implies that

\[
F(N,\delta,\Omega) \geq 1 - \frac{1}{(N+1)\delta}
\]

(S24)

and confirms Eq. (7). If \( \Omega \) has an eigenvalue equal to zero and \( 1/(N+1) \leq \delta \leq \delta^* \), then this bound is saturated according to Lemma S3 below.

\[\square\]

D. Auxiliary lemmas

Lemma S2. If \( \nu(\Omega) \geq 1/2 \), then \( \eta_k(\lambda) - \zeta_k(\lambda) \leq 1/(N+1) \) for all \( k \in S \).

Proof. If \( k = k_0 \), then \( \eta_k(\lambda) = \zeta_k(\lambda) = 1 \), so we have \( \eta_k(\lambda) - \zeta_k(\lambda) = 0 \leq 1/(N+1) \). If \( k \neq k_0 \), then

\[
\eta_k(\lambda) - \zeta_k(\lambda) = \sum_{i \geq 1} k_i \frac{\lambda_i^{k_i-1}}{(N+1)} \prod_{j \neq i} \lambda_j \leq \frac{N+1-k_1}{N+1} \lambda_2^{N-k_1} 
\]

(S25)

Here the second last inequality follows from the assumption \( \nu(\Omega) \geq 1/2 \), which means \( \lambda_2 \leq 1/2 \).

Lemma S3. If \( \Omega \) has an eigenvalue equal to zero and \( 1/(N+1) \leq \delta \leq \delta^* = \eta_{k_1}(\lambda) \), then

\[
F(N,\delta,\Omega) \leq 1 - \frac{1}{\delta(N+1)}.
\]

(S26)

Proof. To prove the inequality, it suffices to find a state \( \rho \) such \( p_\rho = \delta \) and

\[
f_\rho = p_\rho - \frac{1}{N+1}.
\]

(S27)

Since \( p_\rho \) and \( f_\rho \) are linear in \( \rho \), it suffices to find such a state in the cases \( \delta = 1/(N+1) \) and \( \delta = \delta^* = \eta_{k_1}(\lambda) \). When \( \delta = 1/(N+1) \), we can choose \( \rho = \rho_{k_0} \) with \( k = (N,0,\ldots,0,1) \), in which case we have \( p_\rho = 1/(N+1) \) and \( f_\rho = 0 \) as desired, note that \( \lambda_2 = 0 \) by assumption. When \( \delta = \delta^* \), we can choose \( \rho = \rho_{k_1} \), in which case \( p_\rho = \eta_{k_1}(\lambda) \) and \( f_\rho = \zeta_{k_1}(\lambda) \), so that

\[
p_\rho - f_\rho = \eta_{k_1}(\lambda) - \zeta_{k_1}(\lambda) = \frac{1}{N+1}.
\]

(S28)

This observation completes the proof of the lemma.

\[\square\]
Lemma S4. For any $k \in \mathcal{S}$, we have
\[
h_k(\lambda) := \frac{1 - \eta_k(\lambda)}{1 - \zeta_k(\lambda)} \geq 1 - \frac{N\nu}{N\nu + 1}, \tag{S29}
\]
where $k_1 = (N, 1, 0, \ldots, 0)$ and $\nu$ is a short hand for $\nu(\Omega)$.

Proof. By the assumption $k \in \mathcal{S}$ we have $\sum_j k_j = N + 1$ and $k_1 \leq N$. According to Lemma S5 below,
\[
h_k(\lambda) \geq h_k(\lambda_1, \lambda_2, \ldots, \lambda_2) = h_k(\lambda_1, \lambda_2, \lambda_2) \geq h_k(\lambda_1, \lambda_1, \lambda_2) = 1 - \frac{N(1 - \lambda_2)}{N(1 - \lambda_2) + 1} = \frac{N\nu}{N\nu + 1}. \tag{S30}
\]
Note that the definition of $h_k(\lambda)$ (as well as that of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$) can be extended as long as $k$ and $\lambda$ have the same number of components.

It is instructive to take a look at the special scenario $\zeta_k(\lambda) = 0$, which means $k_1 = 0$, or $\lambda_i = 0$ and $k_i \geq 1$ for some $2 \leq i \leq D$. In the first case, we have $\eta_k(\lambda) \leq \lambda_2^N$, so that
\[
h_k(\lambda) = 1 - \eta_k(\lambda) \geq 1 - \lambda_2^N = 1 - (1 - \nu)^N \geq \frac{N\nu}{N\nu + 1}. \tag{S31}
\]
In the second case,
\[
\eta_k(\lambda) = \frac{k_1\lambda_1^{k_1-1}}{N + 1} \prod_{j \neq i, k_j \geq 1} \lambda_j^{k_j} \leq \frac{1}{N + 1}, \tag{S32}
\]
which implies that
\[
h_k(\lambda) = 1 - \eta_k(\lambda) \geq \frac{N}{N + 1} \geq \frac{N\nu}{N\nu + 1}. \tag{S33}
\]
These results are compatible with Lemma S4 as expected.

Lemma S5. Suppose $k = (k_1, k_2, \ldots, k_m)$ is a sequence of $m$ nonnegative integers that satisfies $\sum_i k_j = N + 1$ and $k_1 \leq N$. Let $u, v$ be two $m$-component vectors that satisfy $0 \leq u \leq v \leq u_1 \leq 1$. Then we have $h_k(u) \geq h_k(v)$.

The inequality $0 \leq u \leq v \leq 1$ in the above lemma means $0 \leq u_j \leq v_j \leq 1$ for all $j = 1, 2, \ldots, m$. Note that the constraints on $u, v$ are different from that on $\lambda$.

Proof. By the assumption $0 \leq u \leq v \leq 1$ and Eq. (S8), we have $\zeta_k(u) \leq \zeta_k(v) \leq k_1/(N + 1) < 1$. According to Eq. (S29), $h_k(u)$ is continuous in $u$ for $0 \leq u \leq 1$. So it suffices to prove the lemma in the case $0 < u \leq v \leq 1$.

For $j \geq 2$, calculation shows that
\[
\frac{\partial \eta_k(u)}{\partial u_j} = \frac{\theta}{N + 1} \left( \frac{k_j \sum_i k_i u_i - k_j u_j^2}{u_j} \right), \quad \frac{\partial \zeta_k(u)}{\partial u_j} = \frac{\theta}{N + 1} \frac{k_1 k_j}{u_j}, \tag{S34}
\]
where $\theta := \prod_i u_i^{k_i}$. Incidentally, these derivatives have well-defined limits when some components $u_i$ go to zero; this fact would be clear if we insert the expression of $\theta$ and adopt lengthier expressions. In addition,
\[
\frac{\partial h_k(u)}{\partial u_j} = \frac{(N + 1)\theta k_j u_j \sum_{i \geq 1} k_i u_i - (N + 1)\theta k_j + k_1 k_j \theta^2}{(N + 1 - k_1 \theta)^2 u_j^2} < 0, \tag{S35}
\]
note that $N + 1 - k_1 \theta \geq 1$. Therefore, $h_k(u)$ is monotonically decreasing in $u_j$ for $j \geq 2$; in other words, $h_k(u) \geq h_k(v)$ whenever $0 < u \leq v \leq 1$ and $u_1 = v_1 = 1$. The condition $0 < u \leq v \leq 1$ can be relaxed to $0 \leq u \leq v \leq 1$ by continuity. \hfill \square
III. INDEPENDENCE DEGREES OF HYPERGRAPHS

In this section we prove Proposition 1 which sets upper and lower bounds for the independence degrees of hypergraphs. We then discuss the independence degrees of colorings and minimal independence covers. Finally, we determine independence degrees of odd cycles, which indicate that the optimal cover protocol is in general more efficient than the optimal coloring protocol for verifying hypergraph states.

A. Proof of Proposition 1

Proof. The inequality \( \frac{1}{\Delta(G)+1} \leq \frac{1}{\chi(G)} \), that is, \( \chi(G) \leq \Delta(G) + 1 \), follows from a well-known greedy algorithm which produces a coloring of \( G \) with no more than \( \Delta(G) + 1 \) colors. Let \( v_1, v_2, \ldots, v_n \) be the vertices of \( G \) whose degrees are in decreasing order. Use natural numbers to represent colors and assign color 1 to \( v_1 \). The colors of other vertices are assigned inductively as follows. Suppose the colors of \( v_1, v_2, \ldots, v_{j-1} \) for \( j \leq n \) have been assigned. Then the color number of \( v_j \) is the smallest natural number that is different from the color numbers of those vertices in the set \( \{v_1, v_2, \ldots, v_{j-1}\} \) that are adjacent to \( v_j \). Since \( v_j \) has at most \( \min\{\deg(v_j), j-1\} \) neighbors in this set, where \( \deg(v_j) \) is the degree of \( v_j \), it follows that the color number of \( v_j \) is at most \( \min\{\deg(v_j) + 1, j\} \). Therefore,

\[
\chi(G) \leq \max_j \min\{\deg(v_j) + 1, j\} \leq \Delta(G) + 1.
\]

The inequality \( \gamma(G) \geq 1/\chi(G) \) follows from the observation that any independence cover (or coloring) of \( G \) with \( \chi(G) \) elements and uniform weights has cover strength \( 1/\chi(G) \).

To prove the inequality \( \gamma(G) \leq \alpha(G)/|V| \), let \( (\mathcal{A}, \mu) \) be an arbitrary independence cover. Then

\[
|V|s(\mathcal{A}, \mu) = |V| \min_{j \in V} \sum_{l : A_l \ni j} \mu_l \leq \sum_{j \in V} \sum_{l : A_l \ni j} \mu_l = \sum_l \mu_l |A_l| \leq \alpha(G) \sum_l \mu_l = \alpha(G),
\]

which implies that \( \gamma(G) \leq \alpha(G)/|V| \). To prove the inequality \( \gamma(G) \leq 1/\varpi(G) \), let \( V_C \) be a subset of \( \varpi(G) \) vertices in \( V \) that forms a clique. Then

\[
\varpi(G)s(\mathcal{A}, \mu) = \varpi(G) \min_{j \in V} \sum_{l : A_l \ni j} \mu_l \leq \sum_{j \in V_C} \sum_{l : A_l \ni j} \mu_l \leq \sum_l \mu_l = 1,
\]

where the second inequality follows from the fact that each \( A_l \) can contain at most one vertex in \( V_C \) because \( V_C \) forms a clique, while \( A_l \) is an independence set.

As an implication of Proposition 1 if a hypergraph has chromatic number and clique number both equal to \( m \), then \( \gamma(G) = 1/m \). In particular, \( \gamma(G) \) can attain the maximum 1 iff \( G \) has no nontrivial hyperedges. Here a hyperedge is nontrivial if its order is larger than or equal to 2. Any 2-colorable graph \( G \) with at least one nontrivial edge has \( \gamma(G) = 1/2 \). For example \( \gamma(G) = 1/2 \) when \( |G| \) is a cluster state (of any dimension) or a graph state associated with an even cycle; \( \gamma(G) = 1/3 \) when \( |G| \) is an order-3 cluster state (of any dimension) or a Union Jack state.

B. Cover strengths of colorings and minimal covers

Let \( G = (V, E) \) be a hypergraph and \( (\mathcal{A}, \mu) \) a weighted independence cover constructed from a coloring \( \mathcal{A} \), assuming that all independence sets in \( \mathcal{A} \) are nonempty. Then each vertex of \( V \) is contained in only one independence set in \( \mathcal{A} \), which implies that

\[
s(\mathcal{A}, \mu) = \min_l \mu_l \leq |\mathcal{A}|^{-1} \leq \chi(G)^{-1}.
\]

Here the first inequality is saturated iff all weights \( \mu_l \) are equal, and the second inequality is saturated iff the coloring \( \mathcal{A} \) is optimal in the sense that no other coloring of \( G \) uses fewer colors.

Next, let \( (\mathcal{A}, \mu) \) be a weighted independence cover of \( G \) constructed from a minimal cover \( \mathcal{A} \). By “minimal” we mean that any proper subset \( \mathcal{A}' \) of \( \mathcal{A} \) is not a cover of \( G \) because the union of sets in
\( \mathcal{A} \) does not coincide with the vertex set \( V \). In other words, for any \( A_l \) in \( \mathcal{A} \), there exists a vertex \( j \in V \) such that \( j \in A_l \) and \( j \notin A_k \) for all \( k \neq l \). Therefore,

\[
s(\mathcal{A}, \mu) = \min_{l} \mu_{l} \leq |\mathcal{A}|^{-1} \leq \chi(G)^{-1}
\]  

(S40)

as in Eq. (S39). Again the first inequality is saturated iff all weights \( \mu_{l} \) are equal; the second inequality is saturated iff \( |\mathcal{A}| = \chi(G) \), in which case an optimal coloring of \( G \) can be constructed from \( \mathcal{A} \) by deleting some vertices in some independence sets in \( \mathcal{A} \).

In summary, it is always beneficial to choose equal weights when \( \mathcal{A} \) is a coloring or minimal independence cover. In addition, the cover strength of any such cover is upper bounded by \( 1/\chi(G) \), which can be saturated. As we shall see in the next section, it is sometimes advantageous to consider overcomplete covers.

### C. Independence degrees of odd cycles

In this section we determine the independence degrees of odd cycles, which show that overcomplete covers of some hypergraph \( G \) can have cover strengths larger than \( 1/\chi(G) \) and that the inequality \( \gamma(G) \geq 1/\chi(G) \) in Proposition 1 is in general strict. Therefore, the optimal cover protocol is more efficient than the optimal coloring protocol for verifying some graph and hypergraph states.

Let \( C_n \) be a cycle with \( n \) vertices, where \( n \) is an odd integer. Then \( \alpha(C_n) = (n - 1)/2 \), so that \( \gamma(C_n) \leq (n - 1)/(2n) \) according to Proposition 1. This upper bound can be saturated by the equal-weight cover composed of the \( n \) sets

\[
A_j = \{j, j + 2, \ldots, j + n - 3\}, \quad j = 1, 2, \ldots, n.
\]  

(S41)

Here vertex labels \( j \) and \( j + n \) are taken to be the same. Therefore, the independence degree of the odd cycle \( C_n \) is given by

\[
\gamma(C_n) = \frac{n - 1}{2n} = \frac{1}{2} - \frac{1}{2n},
\]  

(S42)

which increases monotonically with \( n \). As an implication, to verify the graph state associated with the odd cycle within given infidelity and significance level, the total number of tests required decreases monotonically with \( n \) if the optimal cover protocol is adopted. By contrast, the cover strength of any coloring or minimal cover of \( C_n \) is upper bounded by \( 1/3 \) given that \( \chi(C_n) = 3 \). So it is indeed advantageous to consider independence covers beyond colorings for some hypergraphs. This observation is of interest to constructing an efficient verification protocol for hypergraph states.

### IV. PROOF OF PROPOSITION 2

**Proof.** Suppose on the contrary that party \( j \) performs only one projective measurement \( \{P_0, P_1\} \), where \( P_0 \) and \( P_1 \) are rank-1 projectors that satisfy \( P_0 + P_1 = 1 \). Then the projector onto the pass eigenspace has the form \( P_0 \otimes Q_0 + P_1 \otimes Q_1 \), where \( Q_0, Q_1 \) are projectors for the remaining parties \( V \setminus \{j\} \) with \( V \) being the vertex set of the underlying hypergraph. Both \( Q_0, Q_1 \) have rank at least one since, otherwise, the hypergraph state is supported on the support of either \( P_0 \otimes Q_0 \) or \( P_1 \otimes Q_1 \) and is thus biseparable, in contradiction with the fact that any connected hypergraph state is GME [13]. Consequently, the pass eigenspace has dimension at least 2, so the hypergraph state cannot be verified reliably. This contradiction completes the proof.

According to the same reasoning presented above, to verify any \( n \)-qubit pure state that is not biseparable over the partition \( \{\{j\}, V \setminus \{j\}\} \), party \( j \) needs at least two measurement settings (here we only consider projective measurements). In the case of a hypergraph state, any party corresponding to a nonisolated vertex needs at least two measurement settings. Surprisingly, two measurement settings for each party are also sufficient for verifying any hypergraph state, as shown in the main text.
V. PROOF OF THEOREM

In this section we present an independent proof of Theorem 3, which was originally proved in Ref. 33. This theorem is an immediate consequence of Lemmas S7 and S8 presented below. Before stating and proving these auxiliary results, we need to introduce a few additional concepts. Let \(|\Psi\rangle\langle\Psi|\) be an \(n\)-partite pure state of the parties \(V = \{1, 2, \ldots, n\}\). For each nonempty proper subset \(A\) of \(V\), denote by \(\varrho_A\) the reduced state of \(|\Psi\rangle\langle\Psi|\) over the parties in \(A\), that is, \(\varrho_A = \text{tr}_{V \setminus A}(|\Psi\rangle\langle\Psi|)\). Define
\[
\kappa(|\Psi|) := \max_A \|\varrho_A\|, \tag{S43}
\]
where \(\|\varrho_A\|\) denotes the operator norm (the largest eigenvalue) of \(\varrho_A\) and the maximum is taken over all nonempty proper subsets \(A\) of \(V\). Note that \(\kappa(|\Psi|)\) is invariant under local unitary transformations. Given a hypergraph \(G\), define \(\kappa(G) := \kappa(|\Psi|)\).

Lemmas S6 and S7 below are known before 32, but we provide self-contained proofs for completeness.

Lemma S6. The state \(|\Psi\rangle\) is GME iff \(\kappa(|\Psi|) < 1\).

Proof. To prove the lemma, it is equivalent to prove that the state \(|\Psi\rangle\) is biseparable iff \(\kappa(|\Psi|) = 1\). If \(\kappa(|\Psi|) = 1\), then \(|\Psi\rangle\) has a nontrivial reduced state that is pure, which implies that \(|\Psi\rangle\) is biseparable. Conversely, if \(|\Psi\rangle\) is biseparable, then it has a nontrivial reduced state that is pure, which implies that \(\kappa(|\Psi|) = 1\). □

Lemma S7. Suppose \(|\Psi\rangle\) is GME and the state \(\rho\) satisfies \(\langle\Psi|\rho|\Psi\rangle > \kappa(|\Psi|)\). Then \(\rho\) is GME.

Proof. Suppose \(|\Phi\rangle\) is an arbitrary pure state that is biseparable over the partition \(A \cup V \setminus A\), that is \(|\Psi\rangle = |\Phi_A\rangle \otimes |\Phi_{V \setminus A}\rangle\). Then \(\langle\Psi|\Phi\rangle^2 \leq \langle\Phi_A|\varrho_A|\Phi_A\rangle \leq \|\varrho_A\| \leq \kappa(|\Psi|)\), where \(\varrho_A\) is the reduced state of \(|\Psi\rangle\) over the parties in \(A\). If \(\rho\) is not GME, then it is a convex combination of biseparable states, so that \(\langle\Psi|\rho|\Psi\rangle \leq \kappa(|\Psi|)\). Therefore, \(\rho\) is GME whenever \(\langle\Psi|\rho|\Psi\rangle > \kappa(|\Psi|)\). □

Lemma S8. Suppose \(G\) is a connected order-\(k\) hypergraph with \(n \geq k \geq 2\). Then \(\kappa(G) \leq 1 - 2^{1-k}\).

Proof. This lemma is an easy consequence of Lemma S9 below. When \(|G\rangle\) is a connected graph state, Lemma S8 is known much earlier 32 34 35, in which case the bound \(\kappa(G) \leq 1 - 2^{1-k}\) is always saturated. This conclusion follows from the fact that any nontrivial reduced density of \(|G\rangle\) is proportional to a projector of rank at least 2. □

Besides the application in proving Theorem 3, Lemma S8 shows that any order-\(k\) hypergraph state \(|G\rangle\) with \(k \geq 2\) and \(\kappa(G) = 1 - 2^{1-k}\) is not equivalent to any order-\(k'\) hypergraph state with \(k' < k\) under local unitary transformations.

The bound \(\kappa(G) \leq 1 - 2^{1-k}\) is saturated if \(G\) contains an order-\(k\) leaf. Here a leaf of \(G\) is a vertex that belongs to only one hyperedge with order at least 2. The order of the leaf is the order of this unique hyperedge. In this case \(\|\varrho_A\| = 1 - 2^{1-k}\) when \(A\) is composed of the leaf. To verify this claim, it suffices to consider the scenario in which \(n = k\) and \(G\) contains a single hyperedge (which necessarily has order \(k\)). Now it is straightforward to verify that each single-qubit reduced state of \(|G\rangle\) has two eigenvalues equal to \(1 - 2^{1-k}\) and \(2^{1-k}\), respectively, so the bound \(\kappa(G) \leq 1 - 2^{1-k}\) is indeed saturated. In particular, the above observation implies that \(\kappa(G) = 1 - 2^{1-k}\) when \(|G\rangle\) is a 1D order-\(k\) cluster state. Straightforward calculations also show that the bound \(\kappa(G) \leq 1 - 2^{1-k}\) is saturated for 2D order-3 cluster states and Union Jack states, that is, \(\kappa(G) = 3/4\) in these cases.

Lemma S9. Suppose \(G = (V, E)\) is a hypergraph and \(A\) is any nonempty proper subset of \(V\) that is adjacent to \(V \setminus A\). Let \(\varrho_A\) be the reduced state of \(|G\rangle\) over the parties in \(A\). Then \(\|\varrho_A\| \leq 1 - 2^{1-k}\), where \(k\) is the maximal order of hyperedges that connect \(A\) and \(V \setminus A\).

Here two disjoint nonempty subsets \(A\) and \(B\) of the vertex set \(V\) of \(G\) are adjacent if \(E\) contains a hyperedge that connects a vertex in \(A\) and a vertex in \(B\).

Proof. We shall prove Lemma S9 by induction. Note that \(n \geq k \geq 2\) by assumption, where \(n = |V|\). It is straightforward to verify that the lemma holds when \(n = k = 2\). Suppose the lemma holds for \(2 \leq k \leq n \leq n_0\) with \(n_0 \geq 2\). We shall prove that the lemma also holds for \(2 \leq k \leq n = n_0 + 1\).

It is instructive to note that \(\|\varrho_A\|\) does not change if we add or delete hyperedges among vertices in \(A\) or hyperedges among vertices in \(V \setminus A\). So we may assume that \(G\) has neither hyperedges among
vertices in $A$ nor hyperedges among vertices in $V \setminus A$; in other words, every hyperedge of $G$ contains at least one vertex in $A$ and one vertex in $V \setminus A$. Then $k$ is equal to the order of $G$. In addition, we may assume that $G$ has no isolated vertices. Note that the order of $G$ does not change if any isolated vertex, say $j$, is deleted; meanwhile, $\|\varrho_A\|$ does not change after this deletion if $j \notin V \setminus A$, while $\|\varrho_A\| = \|\varrho_{A \setminus \{j\}}\|$ if $j \in A$. Furthermore, given that $\|\varrho_A\| = \|\varrho_{V \setminus A}\|$, we may assume $|A| \leq n - 2$ without loss of generality. By relabeling the parties if necessary, we may assume that $n \notin A$, that is, $n \in V \setminus A$.

According to Proposition 7.16 of Ref. [36],
\[
\varrho_{V \setminus \{n\}} = \frac{1}{2}(\langle G_0 \rangle \langle G_0 \rangle + \langle G_1 \rangle \langle G_1 \rangle),
\tag{S44}
\]
where $G_0, G_1$ are subhypergraphs of $G$ defined as follows
\[
G_0 = (V \setminus \{n\}, \{e \in E \mid n \notin e\}),
G_1 = (V \setminus \{n\}, \{e \in E \mid n \notin e\} \Delta \{e \setminus \{n\} \mid n \in e \in E\}).
\tag{S45}
\]
Here $A \Delta B$ denotes the symmetric difference of $A$ and $B$, that is, $(A \cup B) \setminus (A \cap B)$. Literally, $G_0$ is the subhypergraph of $G$ obtained by deleting the vertex $n$ and all the hyperedges containing $n$; $G_1$ is the subhypergraph of $G$ obtained by deleting the vertex $n$, shrinking all the hyperedges containing $n$, and then deleting repeated hyperedges.

Let $B = V \setminus \{n\} \setminus A$; note that $B$ is nonempty due to the assumption $|A| \leq n - 2$. In addition, $A \cup B = V \setminus \{n\}$ is the vertex set of both $G_0$ and $G_1$. Let $\varrho_0 = \text{tr}_B(\langle G_0 \rangle \langle G_0 \rangle)$ and $\varrho_1 = \text{tr}_B(\langle G_1 \rangle \langle G_1 \rangle)$. Then $\varrho_A = (\varrho_0 + \varrho_1)/2$ and
\[
\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|).
\tag{S46}
\]
If $A$ is connected to $B$ with respect to both $G_0$ and $G_1$, then the induction hypothesis implies that
\[
\|\varrho_0\| \leq 1 - 2^{1-k_0} \leq 1 - 2^{1-k},
\|\varrho_1\| \leq 1 - 2^{1-k_1} \leq 1 - 2^{1-k},
\tag{S47}
\]
which in turn implies that $\|\varrho_A\| \leq 1 - 2^{1-k}$. Here $k_0$ and $k_1$ denote the orders of $G_0$ and $G_1$, respectively, which satisfy $k_0, k_1 \leq k$.

If $A$ is not connected to $B$ with respect to $G_0$, then $G_0$ has no hyperedges, which implies that all hyperedges of $G$ contain the vertex $n$. Recall that by assumption $G$ has neither hyperedges among vertices in $A$ nor hyperedges among vertices in $V \setminus A$. Consequently $G_1$ has order at most $k - 1$. If, in addition, $A$ is connected to $B$ with respect to $G_1$, then $\|\varrho_1\| \leq 1 - 2^{2-k}$, which implies that
\[
\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|) \leq \frac{1}{2}(1 + 1 - 2^{2-k}) = 1 - 2^{1-k}.
\tag{S48}
\]
Otherwise, if $A$ is not connected to $B$ with respect to $G_1$, then no hyperedge of $G$ contains any vertex in $B$; in other words, all vertices of $B$ are isolated with respect to $G$, which contradicts our assumption.

It remains to consider the case in which $A$ is connected to $B$ with respect to $G_0$, but not connected to $B$ with respect to $G_1$. In view of Eq. (S15), we conclude that $G_0$ has order at most $k - 1$ since, otherwise, any order $k$ hyperedge of $G_0$ (which necessarily connects $A$ and $B$) would also be a hyperedge of $G_1$. Therefore,
\[
\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|) \leq \frac{1}{2}(1 - 2^{2-k} + 1) = 1 - 2^{1-k}.
\tag{S49}
\]
This observation completes the proof of Lemma S9.

\[\square\]

VI. VERIFICATION OF GHZ STATES

In this section we provide more details on the verification of GHZ states and discuss connections with previous works.
Let \( G = (V, E) \) be the star graph in which vertex 1 is adjacent to the rest \( n-1 \) vertices, which are themselves not adjacent pairwise. In other words, the edge set \( E \) is composed of \( \{1, j\} \) for \( j = 2, 3, \ldots, n \). The corresponding graph state has the form

\[
|G\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle \otimes |+\rangle^{\otimes(n-1)} + |1\rangle \otimes |-\rangle^{\otimes(n-1)} \right),
\]  

(S50)

where \(|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}\). The graph state \(|G\rangle\) is stabilized by the following \( n \) stabilizer generators,

\[
K_1 = X_1 \prod_{i=2}^{n} Z_i, \quad K_j = Z_1 X_j, \quad \forall j = 2, \ldots, n.
\]  

(S51)

In addition, it is equivalent to the more familiar form of the GHZ state under local unitary transformations. More precisely, we have

\[
\left( \prod_{j=2}^{n} H_j \right) |G\rangle = |GHZ\rangle := \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n}).
\]  

(S52)

where \( H_j \) is the Hadamard gate \( H \) acting on the \( j \)th qubit, recall that \( H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \).

It is straightforward to verify that \( \chi (G) = \varpi (G) = 2 \) and \( \gamma (G) = 1/2 \). An optimal independence cover of \( G \) can be constructed from the coloring composed of the two sets \( \{1\} \) and \( \{2, 3, \ldots, n\} \) with equal weight \( 1/2 \). Based on this observation, we can construct a verification protocol with only two distinct tests. Each test is based on Pauli measurements on individual qubits. The measurement outcome on the \( j \)th qubit will be denoted by \( \tilde{o}_j \), which can take on two possible values, that is, \( \tilde{o}_j = \pm 1 \). In the first test, we measure \( X \) on the first qubit and measure \( Z \) on the rest qubits. The test is passed if the measurement outcomes have even parity, that is, \( \prod_{j=1}^{n} \tilde{o}_j = 1 \). In the second test, we measure \( Z \) on the first qubit and measure \( X \) on the rest qubits. The test is passed if all outcomes coincide, that is, \( \tilde{o}_1 = \tilde{o}_2 = \cdots = \tilde{o}_n \). The projectors onto the pass eigenspaces are respectively given by

\[
P_1 = \frac{1 + K_1}{2}, \quad P_2 = \prod_{j=2}^{n} \frac{1 + K_j}{2},
\]  

(S53)

which satisfy \( P_1 P_2 = |G\rangle\langle G| \). The verification operator \( \Omega \) has the form

\[
\Omega = \frac{1}{2} (P_1 + P_2) = \frac{1}{2} \left( \frac{1 + K_1}{2} + \prod_{j=2}^{n} \frac{1 + K_j}{2} \right).
\]  

(S54)

It is straightforward to verify that \( \nu (\Omega) = 1/2 \), in agreement with Theorem 2. To verify \( |G\rangle \) within infidelity \( \epsilon \) and significance level \( \delta \), it suffices to perform

\[
\frac{2}{\epsilon} \ln \delta^{-1}
\]  

(S55)

tests.

The cover protocol for verifying \( |G\rangle \) can be adapted for \( |GHZ\rangle \) immediately by a simple change of measurement bases in view of Eq. (S52). To be specific, in the first test, we measure \( X \) on all qubits, and the test is passed if the measurement outcomes have even parity. In the second test, we measure \( Z \) on all qubits, and the test is passed if all outcomes coincide. The projectors onto the pass eigenspaces are respectively given by

\[
P_1 = \frac{1 + X^{\otimes n}}{2}, \quad P_2 = (|0\rangle\langle 0|)^{\otimes n} + (|1\rangle\langle 1|)^{\otimes n}.
\]  

(S56)

The total number of tests required is still determined by Eq. (S55). In addition, to certify GME of the GHZ state with significance level \( \delta \), it suffices to perform \( 4 \ln \delta^{-1} \) tests according to Theorem 3.

In the case of GHZ states, the measurements employed above for state verification have been applied to entanglement detection [34, 35]. However, the number of required tests was not discussed as in our paper. Our approach is appealing because it follows from a universal recipe, which applies to all hypergraph states and has a simple graph theoretic interpretation. Furthermore, our protocol can be applied in the adversarial scenario, which was not considered previously.
VII. VERIFICATION OF QUDIT HYPERGRAPH STATES

Here we show that the cover protocol for verifying hypergraph states can also be applied to qudit hypergraph states with minor modifications. The consideration of qudit hypergraph states is restricted to this section only.

A. Qudit hypergraph

In the case of qudit, we need to revise the definition of hypergraphs to take into account multiplicities of hyperedges. Now a hypergraph \( G = (V, E, m_E) \) (also known as multihypergraph in the literature) is characterized by a set of vertices \( V \) and a set of hyperedges \( E \subset \mathcal{P}(V) \) together with multiplicities specified by \( m_E = (m_e)_{e \in E} \), where \( m_e \in \mathbb{Z}_d \) and \( m_e \neq 0 \) with \( \mathbb{Z}_d \) being the ring of integers modulo \( d \) \[15, 16\]. Nevertheless, almost all graph theoretic concepts considered in this work do not depend on the multiplicity vector \( m_E \) and are defined in the same way as in the qubit case. To be specific, these concepts include the order of a hyperedge and the hypergraph, the adjacency relation, the degree of a vertex and the hypergraph, clique and clique number, independence set and independence number, (weighted) independence cover, cover strength, and independence degree. Therefore, Proposition 1 and its proof are applicable without modification.

B. Qudit hypergraph states

The qudit Pauli group (also known as the Heisenberg-Weyl group) is generated by the following two generalized Pauli operators

\[
X = \sum_{j \in \mathbb{Z}_d} |j + 1\rangle\langle j|, \quad Z = \sum_{j \in \mathbb{Z}_d} \omega^j |j\rangle\langle j|, \tag{S57}
\]

where \( \omega = e^{2\pi i/d} \) is a primitive \( d \)th root of unity. Given any qudit hypergraph \( G = (V, E, m_E) \) with \( n \) vertices, we can construct an \( n \)-qudit hypergraph state \( |G\rangle \) as follows: prepare the quantum state \( |+\rangle := \frac{1}{\sqrt{d}} \sum_j |j\rangle \) (eigenstate of \( X \) with eigenvalue 1) for each vertex of \( G \) and apply \( m_e \) times the generalized controlled-Z operation \( CZ_e \) on the vertices of each hyperedge \( e \) \[15, 16\], that is,

\[
|G\rangle = \left( \prod_{e \in E} CZ_e^{m_e} \right) |+\rangle^\otimes n. \tag{S58}
\]

To simplify the notation, here we only give the expression of \( CZ_e \) when \( e = \{1, 2, \ldots, k\} \), in which case we have

\[
CZ_e := \sum_{j_1, j_2, \ldots, j_k \in \mathbb{Z}_d} \omega^{j_1 j_2 \cdots j_k} |j_1, j_2, \ldots, j_k\rangle\langle j_1, j_2, \ldots, j_k|; \tag{S59}
\]

the general case is defined analogously. Alternatively, \( |G\rangle \) is the unique eigenstate (up to a global phase factor) of the \( n \) commuting (nonlocal) stabilizer operators \[15, 16\]

\[
K_j = X_j \otimes \prod_{e \in E| e \ni j} CZ_e^{m_e}, \quad j = 1, 2, \ldots, n, \tag{S60}
\]

which satisfy \( K_j^d = 1 \). As in the qubit case, graph theoretic concepts related to the hypergraph \( G \) also apply to the corresponding state \( |G\rangle \).

C. Verification of qudit hypergraph states

The following protocol for verifying qudit hypergraph states is a simple variation of the cover protocol for verifying qubit hypergraph states presented in the main text.
Let $G = (V, E, m_E)$ be a qudit hypergraph and $|G\rangle$ the associated hypergraph state. Choose an independence cover $\mathcal{A} = \{A_1, A_2, \ldots \}$ of $G$ and let $\overline{A_i} := V \setminus A_i$ be the complement of $A_i$ in $V$. Then we can construct a verification protocol with $|\mathcal{A}|$ tests (measurement settings): the $l$th test consists in measuring $X_j$ for all $j \in A_l$ and measuring $Z_k$ for all $k \in \overline{A_l}$. By measuring $X_j$ ($Z_k$) we mean the measurement on the eigenbasis of $X_j$ ($Z_k$). The measurement outcome on the $a$th qubit for $a = 1, 2, \ldots, n$ can be written as by $\omega_{a}$, where $a_0 \in \mathbb{Z}_d$. Note that $X_j$ and $Z_k$ commute with $K_i$ for all $i, j \in A_l$ and $k \in \overline{A_l}$. In addition, the joint eigenstate of $X_j$ and $Z_k$ corresponding to the outcome $\{o_a\}$ is an eigenstate of $K_i$, whose eigenvalue is given by $\omega^{|i|}$ with

$$t_i = o_i + \sum_{e \in E, e \ni i} m_e \prod_{k \in e, k \neq i} o_k$$

(S61)

according to Eq. (S60). The test is passed if $\omega^{|i|} = 1$ for all $i \in A_l$. The projector onto the pass eigenbasis associated with the $l$th test reads

$$P_l = \prod_{i \in A_l} \left( \frac{1}{d} \sum_{b \in \mathbb{Z}_d} K_i^b \right).$$

(S62)

A state can pass all tests iff it is stabilized by $K_i$ for all $i \in V$. So only the target state $|G\rangle$ can pass all tests with certainty as desired.

Suppose the $l$th test is applied with probability $\mu_l$. The efficiency of the resulting protocol is determined by the spectral gap of $\Omega(\mathcal{A}, \mu) = \sum_{l=1}^{|\mathcal{A}|} \mu_l P_l$. Note that the common eigenbasis of $K_i$ for $i \in V$ also form an eigenbasis of $\Omega(\mathcal{A}, \mu)$. Each eigenstate $|\Psi_x\rangle$ in this basis is specified by a string $x \in \mathbb{Z}_d^n$ and satisfies $K_i |\Psi_x\rangle = \omega^{|x_i|} |\Psi_x\rangle$. The corresponding eigenvalue of $\Omega(\mathcal{A}, \mu)$ reads $\lambda_x = \sum_{i \in \text{supp}(x) \subseteq \mathcal{A}} \mu_i$, where $\text{supp}(x) := \{i \mid x_i \neq 0\}$. The second largest eigenvalue of $\Omega(\mathcal{A}, \mu)$ can be attained when $x_i = 0$ for all $i \in V$ except for one of them, so that

$$\nu(\Omega(\mathcal{A}, \mu)) = \min_{i \in V} \sum_{l: A_l \ni i} \mu_l = s(\mathcal{A}, \mu).$$

(S63)

Therefore, Theorem 2 as well as Eqs. (14) and (15) are applicable in the qudit case too.

VIII. COMPARISON WITH EXISTING WORKS

In this section we discuss the connection between our work and entanglement detection. We then compare our approach for state verification with a number of existing works, including direct fidelity estimation (DFE) [28] and Refs. [19] [25] [26].

A. Connection with entanglement detection

In the main text, we introduced a simple and efficient protocol for verifying general hypergraph states. Our protocol can also be applied to detecting GME, though it is not optimized for this purpose. In the literature, there are many works on the detection of entanglement, including GME in particular [32]. The main distinction between state verification and entanglement detection lies in the motivations, which are reflected in the following two questions.

1. Is the quantum state prepared good enough for a given task, such as quantum computation, quantum communication, or quantum metrology?

2. Is the quantum state prepared GME?

The main motivation of the current work is to provide an efficient tool for answering the first question, while most works on entanglement detection focus on the second question directly. Question 2 is definitely interesting in itself since GME is a key resource in quantum information processing and a focus of foundational studies. In addition, demonstrating GME in experiments is usually highly nontrivial and may serve as a signature of the advance of quantum information science. On the other hand, although there are intimate connections between the two questions, the answer to question 2 is
in general far from enough for answering question 1, which usually entails high fidelity with the target state. Instead of demonstrating certain quantum signature, eventually, we need to answer more specific questions directly. Crucial to achieving this task is efficient state verification, which is a focus of this work.

In addition, most works on entanglement detection are based on the expectation values of certain witness operators and usually do not discuss the number of tests required to make a conclusion. With the cover protocol, by contrast, we can not only provide more precise information about the quantum state prepared, but also determine the number of tests required.

**B. Comparison with direct fidelity estimation**

In this section we compare our approach with DFE introduced by Flammia and Liu [28]. Compared with our method, DFE can be applied to any pure state and thus has wider applications. The number of measurements required by DFE is smaller than tomography by a factor of $D = 2^n$, where $n$ is the number of qubits. Moreover, this number does not increase with the number of qubits in the case of stabilizer states. From this perspective, DFE is very efficient and very useful. However, DFE has several drawbacks as mentioned below which limit its applications to hypergraph states and many other states of quantum systems with more than 15 qubits.

1. To apply DFE it is necessary to sample from the squared characteristic function defined on the discrete phase space of $2^{2n}$ points. In general, it is not easy to compute and store this function for large quantum systems; also, it is not easy to implement the sampling even if the characteristic function is determined.

2. The number of potential measurement settings increases exponentially with the number of qubits even for stabilizer states. The number of actual measurement settings $\lceil 1/(\epsilon^2 \delta) \rceil$ depends on the infidelity $\epsilon$ and significance level $\delta$. Specific measurement settings cannot be determined before implementing the protocol. Also, the total number of measurements cannot be determined in advance.

3. The average total number of measurements reads [28]

$$N_{DFE} \approx 1 + \frac{1}{c^2 \delta} + \frac{2g}{D \epsilon^2} \ln(2/\delta) = 1 + \frac{1}{c^2 \delta} + \frac{2\tilde{g}}{c^2 \epsilon^2} \ln(2/\delta),$$

(S64)

where $D = 2^n$, $\tilde{g} = g/2^n$, and $g$ is the number of points at which the characteristic function is nonzero. It is known that $g \geq D$ and the lower bound is saturated if the target state is a stabilizer state. For a generic state $g \approx D^2$, so the number of measurements increases exponentially with $n$. As we shall see shortly, the exponential growth is also inevitable for general hypergraph states.

The number $N_{DFE}$ in Eq. (S64) can be reduced for a well-conditioned state $\rho$, which means either $|\text{tr}(\rho W_{x,z})| = 0$ or $|\text{tr}(\rho W_{x,z})| \geq c$ for all Pauli operators $W_{x,z}$ [cf. Eq. (S67) below], where $c$ is a positive constant whose inverse is upper bounded by a polynomial of $n$. In this case, $N_{DFE}$ can be reduced to $O(\ln(1/\delta)/(c^2 \epsilon^2))$, though the quadratic scaling behavior with $1/\epsilon$ does not change. However, many hypergraph states are not well-conditioned. In addition, no simple way is known to determine whether a generic hypergraph state is well-conditioned or not when the number of qubits is large.

To analyze the supports of the characteristic functions of hypergraph states, it is instructive to point out that any hypergraph state is a real equally weighted state and vice versa [13, 14]. In other words, any $n$-qubit hypergraph state can be written as

$$|\Psi_f\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle,$$

(S65)

where $f$ is a Boolean function from $\{0,1\}^n$ to $\{0,1\}$. For example, the Boolean function corresponding to the hypergraph state $|G\rangle = (\prod_{e \in E} CZ_e) |+\rangle ^n$ is given by

$$f(x) = \prod_{e \in E} x_j,$$

(S66)
where the addition is modulo 2. Up to a phase factor, any $n$-qubit Pauli operator can be written as

$$W_{x,z} := \left( \prod_{j=1}^{n} X_j^{x_j} \right) \left( \prod_{j=1}^{n} Z_j^{z_j} \right), \quad x, z \in \{0, 1\}^n,$$

where $X_j$ and $Z_j$ are the Pauli $X$ and $Z$ operators for the $j$th qubit. Here we are mainly interested in the absolute value of the characteristic function, so the phase factor does not matter. Calculation shows that

$$\langle \Psi_f | W_{x,z} | \Psi_f \rangle = \frac{1}{2^n} \sum_{u=0}^{2^n-1} (-1)^{f(u) + f(u + x) - z \cdot u},$$

where the addition $u + x$ is modulo 2 and $z \cdot u := \sum_{j=1}^{n} z_j u_j$ with addition also modulo 2. The cardinality of the support of the characteristic function reads

$$g(f) = |\{(x, z) \in \{0, 1\}^{2n} | \langle \Psi_f | W_{x,z} | \Psi_f \rangle \neq 0\}|.$$

In the rest of this section, we provide several concrete examples of hypergraph states for which $\tilde{g}$ increases exponentially with the number $n$ of qubits, which means $N_{\text{DFE}}$ increases exponentially with $n$. First, consider the special hypergraph with only one hyperedge, which contains all $n$ vertices. The corresponding Boolean function $f_n$ reads

$$f_n(u) := \prod_{j=1}^{n} u_j = \begin{cases} 1 & u = 11 \cdots 1, \\ 0 & \text{otherwise}. \end{cases}$$

In this case, we have

$$2^n |\langle \Psi_{f_n} | W_{x,z} | \Psi_{f_n} \rangle| = \begin{cases} 2^n & x = z = 0, \\ 2^n - 4 & z = 0, x \neq 0, \\ 4 & x \neq 0, z \neq 0, x \cdot z = 0, \\ 0 & x \cdot z = 1, \text{ or } x = 0, z \neq 0, \end{cases}$$

which implies that

$$g(f_n) = 2^{2n-1} - 2^{n-1} + 1, \quad \tilde{g} \approx 2^{n-1} - 2^{-1}.$$

So the number of measurements in Eq. (S64) reduces to

$$N_{\text{DFE}} \approx 1 + \frac{1}{\epsilon^2 \delta} + \frac{2^{n-1} - 1}{\epsilon^2} \ln(2/\delta),$$

which increases exponentially with the number of qubits. By contrast, the number of tests required by our cover protocol is

$$\frac{n}{\epsilon} \ln(1/\delta),$$

which is exponentially smaller than $N_{\text{DFE}}$.

As another example, consider the tensor power $|\Psi_{f_3}\rangle^{\otimes n/3}$, which corresponds to the hypergraph state with $n/3$ disjoint hyperedges of order 3, assuming that $n$ is divisible by 3. In this case,

$$g = g(f_3)^{n/3} = 29^{n/3} > 3^n, \quad \tilde{g} = \frac{29^{n/3}}{2^n} \geq \left( \frac{3}{2} \right)^n.$$

So the number of measurements in Eq. (S64) reduces to

$$N_{\text{DFE}} \approx 1 + \frac{1}{\epsilon^2 \delta} + \frac{2 \times 29^{n/3}}{2^n \epsilon^2} \ln(2/\delta) \geq 1 + \frac{1}{\epsilon^2 \delta} + \frac{2 \times \left( \frac{3}{2} \right)^n}{\epsilon^2} \ln(2/\delta),$$

(76)
which also increases exponentially with the number of qubits. By contrast, the number of tests required by the cover protocol is
\[
\frac{3}{\epsilon} \ln(1/\delta),
\]
(S77)
which is again exponentially smaller than \(N_{DFE}\).

Furthermore, numerical calculations show that \(\tilde{g}\) increases exponentially with \(n\) for order-3 cluster states and Union Jack states on a chain or on a two-dimensional lattice (cf. Fig. 3), so \(N_{DFE}\) also increases exponentially with \(n\) for these states. The number of tests required by the cover protocol is still \((3/\epsilon) \ln(1/\delta)\).

C. Comparison with Ref. [19]

Very recently, Morimae, Takeuchi, and Hayashi (MTH) [19] introduced a method for verifying hypergraph states in the adversarial scenario. They only considered the case in which all hyperedges have orders at most three. Although their method may potentially be extended to more general settings, a direct extension of their approach entails exponential increase in the resource overhead with the order of the hypergraph. Even for order-3 hypergraph states, the resource overhead increases exponentially with the number of hyperedges (and thus the degree of the hypergraph). Another drawback of the MTH protocol is that even the target hypergraph state \(|G\rangle\) cannot pass the test with certainty. Consequently, the number of tests required increases quadratically with the inverse infidelity.

More specifically, suppose \(|G\rangle\) is an \(n\)-qubit hypergraph state to be verified. Let \(K_j\) be the stabilizer operator corresponding to vertex \(j\) as defined in Eq. (11) in the main text; let \(r_j\) be the number of order-3 hyperedges that contain the vertex \(j\). The MTH verification protocol is composed of \(n\) stabilizer tests. For each stabilizer \(K_j\), MTH devised a test, which requires \(4^{r_j}\) potential measurement settings. The total number of potential measurement settings is given by
\[
\sum_{j=1}^{n} 4^{r_j},
\]
(S78)
which increases exponentially with the number of order-3 hyperedges. MTH also set a criterion such that the probability of a state \(\rho\) to satisfy the criterion is given by
\[
\rho = \frac{1}{2} + \frac{\text{tr}(\rho K_j)}{2^{r_j+1}} = \frac{1}{2} + \frac{1 - a_j}{2^{r_j+1}}.
\]
(S79)
where \(a_j := 1 - \text{tr}(\rho K_j)\). Although the target state \(|G\rangle\) can attain the maximum \((1/2) + (1/2^{r_j+1})\), it generally cannot satisfy the criterion with certainty. Suppose the test is performed \(N_j\) times, and the criterion is satisfied \(t_j\) times. Then the stabilizer test is passed if the frequency \(f_j = t_j/N_j\) satisfies
\[
f_j \geq \frac{1}{2} + \frac{1 - \theta}{2^{r_j+1}},
\]
(S80)
where \(\theta\) is a small positive constant. The state \(\rho\) is accepted if it can pass all the stabilizer tests. The choice of \(\theta\) needs to guarantee that the target state \(|G\rangle\) can pass all the tests with high probability; meanwhile, any state that has low fidelity with \(|G\rangle\) should fail some test with high probability. When \(a_j \geq \theta\), the probability that \(\rho\) can pass the stabilizer test associated with \(K_j\) can be upper bounded as follows,
\[
\Pr \left( f_j \geq \frac{1}{2} + \frac{1 - \theta}{2^{r_j+1}} \right) = \Pr \left( f_j \geq \rho + \frac{a_j - \theta}{2^{r_j+1}} \right) \leq \exp \left( -\frac{(a_j - \theta)^2}{4^{r_j+1}N_j} \right),
\]
(S81)
where the last step follows from the Hoeffding inequality. Similarly, the probability that the target state \(|G\rangle\) passes the test can be lower bounded by virtue of the Hoeffding inequality.

MTH did not give an explicit number of tests needed to verify a hypergraph state within infidelity \(\epsilon\) and significance level \(\delta\). They considered a related, but different verification problem with a different criterion, which requires about \(nk + 1 + m\) tests, where \(k = 2^{2r^j+3}n^7\), \(m \geq 2n^7k^2\ln 2\), and \(r = \max_j r_j\). In other words, the number of required tests satisfies
\[
nk + 1 + m \geq nk + 1 + 2n^7k^2\ln 2 \cong 2n^7k^2\ln 2 = 2^{4r+7}n^{21}\ln 2.
\]
(S82)
While this number is still polynomial in $n$ if $r$ does not increase with $n$, it grows rapidly with $n$. Actually, this number is already astronomical when $n = 5$ and $r = 2$ (note that $r = 8$ for generic Union Jack states on 2D lattices), while any useful MBQC would require more than five qubits. So the MTH protocol is hardly practical. In contrast, the number of tests required in our protocol does not depend on $n$ even in the adversarial scenario and thus outperforms the MTH protocol dramatically. It is natural to ask whether the number of tests can be reduced significantly if the MTH protocol is adapted to the nonadversarial scenario considered in the main text. Here we try to give a rough estimate.

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, suppose $1 - \langle G|\rho|G\rangle \geq \epsilon$, we need to estimate the maximal probability that $\rho$ can pass all the stabilizer tests and make sure that this probability is smaller than $\delta$, that is,

$$\prod_j \Pr\left(f_j \geq \frac{1}{2} + \frac{1 - \theta}{2^{r_j + 1}}\right) = \Pr\left(f_j \geq p + \frac{a_j - \theta}{2^{r_j + 1}}\right) \leq \delta. \quad (S83)$$

According to Eq. (S81), it suffices to guarantee that

$$\prod_j \exp\left(-2 \frac{(a_j - \theta)^2}{4^{r_j + 1} N_j}\right) \leq \delta, \quad (S84)$$

Note that the infidelity of $\rho$ with $|G\rangle$ satisfies

$$1 - \langle G|\rho|G\rangle = 1 - \text{tr} \left(\rho \prod_j \frac{K_j + 1}{2}\right) \leq \sum_j \left[1 - \text{tr} \left(\rho \frac{K_j + 1}{2}\right)\right] = \frac{1}{2} \sum_j a_j. \quad (S85)$$

If the infidelity is at least $\epsilon$, then $(\sum_j a_j)/2 \geq \epsilon$. Now we need to determine the minimum of $\sum_j N_j$ under the requirement that Eq. (S84) holds whenever $(\sum_j a_j)/2 \geq \epsilon$. Choose

$$a_j = \frac{2 \epsilon \times 2^{r_j}}{\sum_k 2^{r_k}}, \quad (S86)$$

then Eq. (S84) implies that

$$\exp\left(-\frac{2 \epsilon^2 \sum_j N_j}{(\sum_j 2^{r_j})^2}\right) \leq \delta, \quad (S87)$$

which in turn implies that

$$N_{\text{MTH}} = \sum_j N_j \geq \frac{(\sum_j 2^{r_j})^2 \ln \delta^{-1}}{2 \epsilon^2}. \quad (S88)$$

If all $r_j$ are equal to $r$, then the MTH protocol requires $4^n n$ potential measurement settings and at least

$$N_{\text{MTH}} \geq \frac{4^n n^2 \ln \delta^{-1}}{2 \epsilon^2}. \quad (S89)$$

tests. The bounds in the above two equations have much better scaling behavior with $n$ compared with the bound in Eq. (S82). However, these bounds are already very large for a small value of $n$ for Union Jack states and many other states for which $r$ is not so small. In general, it is too prohibitive to implement the MTH protocol except for hypergraph states of no more than ten qubits.

A few comments are in order. First, we do not know how tight are the bounds in Eqs. (S88) and (S89). Nevertheless, these bounds are sufficient for comparing the MTH protocol with our protocol, and it is not so important to derive a tighter bound with more involved analysis. Second Eq. (S88) is based on Eqs. (S81) and (S85). Note that the bound in (S85) is tight. The Hoeffding inequality in Eq. (S81) may potentially be improved, thereby reducing $N_{\text{MTH}}$. However, this possibility was not considered by MTH. We are not aware of any simple method for improving the Hoeffding inequality.
either and do not expect a significant improvement even with more sophisticated analysis. In this regard, our protocol is not only much more efficient, but also much easier to implement and to analyze its performance.

In the rest of this section, we consider the performance of the MTH protocol adapted to the non-adversarial scenario for several concrete order-3 hypergraph states. As a start, consider the complete order-3 hypergraph state whose underlying hypergraph contains all possible order-3 hyperedges. In this case, the total number of hyperedges is \((\binom{n}{3}) = n(n-1)(n-2)/6\) and \(r_j = r = \binom{n-1}{2} = (n-1)(n-2)/2\) for \(j = 1, 2, \ldots, n\). Therefore,

\[
N_{\text{MTH}} \geq \frac{2(n-1)(n-2)n^2\ln\delta^{-1}}{e^2}.
\]  

(S90)

In this worst case, both the number of potential measurement settings and the number of tests required by the MTH protocol increase exponentially with the number of qubits. By contrast, our cover protocol requires only \(n\) potential measurement settings and \((n/\epsilon)\ln(1/\delta)\) tests according to Eq. (14). Note that any hypergraph of \(n\) vertices admits a coloring with \(n\) colors.

The rest examples considered below are 3-colorable, so our protocol requires three measurement settings and \((3/\epsilon)\ln(1/\delta)\) tests to verify each hypergraph state within infidelity \(\epsilon\) and significance level \(\delta\). First, consider the tensor power \(|\Psi_{f_1}\rangle^\otimes n/3\) introduced in Sec. VIIIB, assuming \(n\) is divisible by 3. In this case \(r_j = r = 1\) for all \(j = 1, 2, \ldots, n\). Therefore, Eq. (S89) reduces to

\[
N_{\text{MTH}} \geq \frac{2n^2\ln\delta^{-1}}{e^2}.
\]  

(S91)

Next, consider order-3 cluster states. In the 1D case, the vertices of the underlying hypergraph are arranged in a chain and labeled by natural numbers; all hyperedges have the form \(\{j, j+1, j+2\}\) with \(j \geq 1\) and \(j \leq n-2\), assuming \(n \geq 3\). If we use 0, 1, 2 to denote three colors, then the hypergraph can be colored by assigning vertex \(j\) with the color \((j \mod 3)\). Similar analysis applies to 2D and higher-dimensional lattices. For simplicity, here we focus on the 1D case, so that

\[
r_j = \begin{cases} 
1 & n = 3 \text{ or } j = 1 \text{ or } j = n, \\
2 & n \geq 4, j = 2 \text{ or } j = n-1, \\
3 & j \neq 1, 2, n-1, n.
\end{cases}
\]  

(S92)

Therefore,

\[
\sum_j 2^{r_j} = \begin{cases} 
6 & n = 3, \\
8n - 20 & n \geq 4,
\end{cases}
\]  

(S93)

which implies that

\[
N_{\text{MTH}} \geq \begin{cases} 
18\ln\delta^{-1} & n = 3, \\
8(2n-5)^2\ln\delta^{-1} & n \geq 4.
\end{cases}
\]  

(S94)

Now consider the Union Jack state on the Union Jack chain; cf. Fig. [1] in the main text. In this case, we have \(r_j = 2\) when \(j\) corresponds to one of the four corners and \(r_j = 4\) otherwise. Therefore,

\[
\sum_j 2^{r_j} = 16n - 48, \quad N_{\text{MTH}} \geq \frac{128(n-3)^2\ln\delta^{-1}}{e^2}.
\]  

(S95)

Finally, consider the Union Jack state on the Union Jack lattice with \(\tilde{n} \times \tilde{n}\) cells and \(n = \tilde{n}^2 + (\tilde{n} + 1)^2\) qubits. Calculation shows that

\[
\sum_j 2^{r_j} = 2^8(\tilde{n} - 1)^2 + 2^4[\tilde{n}^2 + 4(\tilde{n} - 1)] + 2^2 \times 4 = 16(17\tilde{n}^2 - 28\tilde{n} + 13),
\]  

(S96)

\[
N_{\text{MTH}} \geq \frac{128(17\tilde{n}^2 - 28\tilde{n} + 13)^2\ln\delta^{-1}}{e^2}.
\]  

(S97)
D. Comparison with Ref. [25]

Here, in the adversarial setting, we compare our method with the method proposed by Hayashi and Hajdušek (HH) [25], who considered the verification of graph states, but not hypergraph states. In addition, HH mainly focused on the case in which the graph is 3-colorable. They mentioned the general case briefly, but did not analyze the performance of their protocol in detail. Since the main focus of Ref. [25] is self-testing, HH do not trust their measurement devices. However, after the verification of their measurement devices, they verify their graph state under the assumption that their measurement devices are trusted.

Let \(|G\rangle\) be a graph state associated with the graph \(G\). When \(G\) is \(m\)-colorable, HH (Appendix F of Ref. [25]) proposed the following verification protocol, which consists of \(m\) stabilizer tests. Given a coloring \(A = \{A_1, A_2, \ldots, A_m\}\) of \(G\) with \(m\) colors, the verifier asks the adversary to prepare \(N + 1\) systems with \(N = mN'\). After a random permutation of the \(N + 1\) systems, \(N\) systems are chosen and divided into \(m\) groups each with \(N'\) systems. Then all systems in the \(l\)th group for \(l = 1, 2, \ldots, m\) are subjected to the stabilizer test with \(P_l\) [cf. Eq. (12) in the main text] as the projector onto the pass eigenspace. Let \(\sigma\) be the reduced state of the remaining system after all these tests are passed. If the \(l\)th test \(P_l\) is passed with significance level \(\delta'\), then one can guarantee that \(\text{tr}[\sigma(I - P_l)] \leq \frac{1}{\delta'(N'+1)}\). If all the tests \(P_1, \ldots, P_m\) are passed, with significance level \(\delta := m\delta'\), then one can guarantee that

\[
\epsilon = \text{tr}[\sigma(I - |G\rangle\langle G|)] \leq \sum_{l=1}^{m} \text{tr}[\sigma(I - P_l)] \leq \sum_{l=1}^{m} \frac{1}{\delta'(N'+1)} = \frac{m^2}{\delta(N/m + 1)} \approx \frac{m^3}{\delta N}.
\]

(S98)

To verify \(|G\rangle\) within infidelity \(\epsilon\) and significance level \(\delta\) in the adversarial scenario, the HH protocol requires about \(m^3/(\delta \epsilon)\) tests.

Now, we explain how our method improves the HH method. If we randomly choose the \(l\)th measurement setting with probability \(1/m\), we have \(\nu(\Omega) = 1/m\) in Theorem [1]. If the tests are passed with significance level \(\delta\), then Theorem [1] guarantees that

\[
\epsilon = \text{tr}[\sigma(I - |G\rangle\langle G|)] \leq \frac{m(1 - \delta)}{N\delta}.
\]

(S99)

To verify \(|G\rangle\) within infidelity \(\epsilon\) and significance level \(\delta\) in the adversarial scenario, our protocol requires only \(m(1 - \delta)/(\delta \epsilon)\) tests, which significantly outperforms the HH protocol.

E. Comparison with Ref. [26]

Recently, Pallister, Linden, and Montanaro (PLM) [26] introduced two protocols for verifying stabilizer states, which are equivalent to graph states under local Clifford transformations (LC) [29] [30]. Their protocols are applicable only in the nonadversarial scenario and do not admit direct generalization to hypergraph states.

Let \(|G\rangle\) be an \(n\)-qubit graph state, the first protocol of PLM measure all \(2^n - 1\) nontrivial stabilizer operators of \(|G\rangle\) in the Pauli group with equal probability. To verify \(|G\rangle\) within infidelity \(\epsilon\) and significance level \(\delta\), this protocol requires about \(2^{1-n}(2^n - 1)\epsilon^{-1} \ln \delta^{-1} \approx 2\epsilon^{-1} \ln \delta^{-1}\) tests, which is smaller than the number \(\chi(G)\epsilon^{-1} \ln \delta^{-1}\) for our protocol. However, the number of potential measurement settings of this PLM protocol increases exponentially with the number \(n\) of qubits. When \(n\) is large, this protocol will be impractical if it is costly or time consuming to switch measurement settings. By contrast, our protocol requires at most \(n\) potential measurement settings and only two settings for each party (instead of three settings for the PLM protocol). In addition, when the chromatic number \(\chi(G)\) of \(G\) is small (in particular when \(G\) is 2-colorable), the total number of tests required in our protocol is comparable to the PLM protocol.

The second PLM protocol measures \(n\) stabilizer generators of \(|G\rangle\) with equal probability and requires \(n\epsilon^{-1} \ln \delta^{-1}\) tests in total, which corresponds to the performance of our protocol in the worst case in which the graph is complete (contains all possible edges). In general, our protocol requires much fewer measurement settings and tests in total.