Efficient verification of hypergraph states

Huangjun Zhu[1, 2, 3, 4, 5, *] and Masahito Hayashi[6, 7, 8]

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

(Dated: May 9, 2019)

Multipartite entangled quantum states, 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, yet its efficiency is comparable to the best strategy based on entangling measurements. For a given state, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. Our protocol is dramatically more efficient than all known candidates based on local measurements, including tomography and direct fidelity estimation. It enables the verification of hypergraph states of thousands of qubits. The protocol can also be applied in the adversarial scenario with almost the same efficiency and is thus particularly appealing to applications like blind measurement-based quantum computation.

Introduction.—Entanglement is the characteristic feature of quantum theory and a key resource in quantum information processing [1, 2]. As an archetypal example of multipartite entangled quantum states, graph states are of central interest to (blind) quantum computation [3–7], quantum error correction [8, 9], quantum networks [10–12], and foundational studies on nonlocality [13–15]. Hypergraph states [16–20], as a generalization of graph states, are equally useful in these research areas [21–25]. Moreover, certain hypergraph states, like Union Jack states, are universal for measurement-based quantum computation (MBQC) under only Pauli measurements [21, 22, 25, 26], which is impossible for graph states; in addition, they possess symmetry-protected topological orders, which are a focus of ongoing research [21, 22, 27]. Furthermore, hypergraph states are attractive for demonstrating quantum supremacy [23, 28].

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 [7, 12, 29–31]. In general, the resource required in traditional tomography increases exponentially with the number of qubits. The same is true for popular alternatives, such as compressed sensing [32] and direct fidelity estimation (DFE) [33]. Although recent approaches tailored for hypergraph states [23, 34] can achieve polynomial scaling behavior with high-order polynomials, it is still too prohibitive to verify any hypergraph state of practical interest. The situation is much worse in the adversarial scenario, which is crucial to many quantum information processing tasks that entail high security conditions, including blind MBQC [6, 7, 26, 29, 30] and quantum networks [10–12]. In this case, to verify the simplest nontrivial hypergraph states (say of three qubits) already entails astronomical number of measurements.

Here we propose a simple and efficient 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 $m = n$ (potential) measurement settings and $m \ln \delta^{-1}/\epsilon$ tests in total, where ϵ and δ denote the infidelity and significance level, which characterize the precision required. For a given state, m can be replaced by the chromatic number or degree of the underlying hypergraph. For many interesting graph and hypergraph states, including cluster states and Union Jack states, the number of measurement settings and that of tests in total do not increase with the number of qubits. For example, Union Jack states can be verified with only three measurement settings and $3 \ln \delta^{-1}/\epsilon$ tests in total.

Our protocol for verifying hypergraph states is dramatically more efficient than known candidates, including tomography and DFE [33], as well as recent protocols tailored for hypergraph states [23, 34]. This protocol enables efficient verification of hypergraph states of thousands of qubits, which are more than enough for demonstrating quantum supremacy. Moreover, our protocol can be applied to the the adversarial scenario and achieves almost the same efficiency. Now the advantage over previous approaches is even more dramatic. In the special case of graph states and stabilizer states, our approach is also much more efficient than known candidates. Our approach is particularly appealing to applications which

* zhuhuangjun@fudan.edu.cn

entail high security requirements, such as blind MBQC and quantum networks.

Setting the stage.—Consider a device that is supposed to produce the target state $|\Psi\rangle$ in the Hilbert space $\mathcal{H}$. In practice, the device may actually produce $\sigma_1, \sigma_2, \dots, \sigma_N$ in N runs. We assume that the fidelity $\langle\Psi|\sigma_j|\Psi\rangle$ is either 1 for all j or satisfies $\langle\Psi|\sigma_j|\Psi\rangle \le 1-\epsilon$ for all j [31]. Now the task is to determine which is the case. To achieve this task we can perform two-outcome tests $\{P_l, 1-P_l\}$ based on local projective measurements. Each test is specified by a test projector P_l, which corresponds to passing the test and satisfies the condition $P_l|\Psi\rangle = |\Psi\rangle$, so that the target state will never fail the test. Suppose the test P_l is performed with probability μ_l, then the passing probability of a general state σ is $\mathrm{tr}(\Omega\sigma)$, where $\Omega := \sum_l \mu_l P_l$ is the verification operator and also called a strategy. In the bad case, we have [31, 35]

$$\max_{\langle\Psi|\sigma|\Psi\rangle\le 1-\epsilon} \mathrm{tr}(\Omega\sigma) = 1-[1-\beta(\Omega)]\epsilon = 1-\nu(\Omega)\epsilon, \quad (1)$$

where $\beta(\Omega)$ is the second largest eigenvalue of Ω, and $\nu(\Omega) := 1-\beta(\Omega)$ is the spectral gap. The probability of passing N tests in the bad case is at most $[1-\nu(\Omega)\epsilon]^N$. To ensure the condition $\langle\Psi|\sigma_{N+1}|\Psi\rangle > 1-\epsilon$ with significance level δ, the minimum number of tests reads [31, 35]

$$N_{\mathrm{NA}}(\epsilon,\delta,\Omega) = \left\lceil \frac{1}{\ln[1-\nu(\Omega)\epsilon]}\ln\delta \right\rceil \le \left\lceil \frac{1}{\nu(\Omega)\epsilon}\ln\frac{1}{\delta}\right\rceil. \quad (2)$$

Hypergraphs.—A hypergraph $G = (V, E)$ is characterized by a set of vertices $V = \{1, 2, \dots, n\}$ and a set of hyperedges $E \subset \mathscr{P}(V)$, where $\mathscr{P}(V)$ is the power set of V [17, 18]; see Fig. 1 for some examples. The order of a hyperedge is the number of vertices it connects, and the order of a hypergraph is the maximum 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 $\deg(j)$ of a vertex j is the number of vertices that are adjacent to it; the degree $\Delta(G)$ of G is the maximum vertex degree. A subset of the vertex set V is a clique if every two vertices in the set are adjacent. The clique number $\varpi(G)$ of G is the maximum number of vertices over all cliques. By contrast, a subset is an independent set if no two vertices are adjacent. The independence number $\alpha(G)$ of G is the maximum number of vertices over all independent sets.

A set $\mathscr{A} = \{A_1, A_2, \dots, A_m\}$ of independent sets of G is an independence cover if $\cup_{l=1}^m A_l = V$. The cover $\mathscr{A}$ also defines a coloring of G with m colors when $\mathscr{A}$ forms a partition of V, that is, when A_l are pairwise disjoint (assuming no A_l is empty). A hypergraph G is k-colorable if its vertices can be colored using k different colors such that any two adjacent vertices have different colors. A 2-colorable graph is also a bipartite graph. The chromatic number $\chi(G)$ is the minimum number of colors in any coloring of G or, equivalently, the minimum number of elements in any independence cover of G.

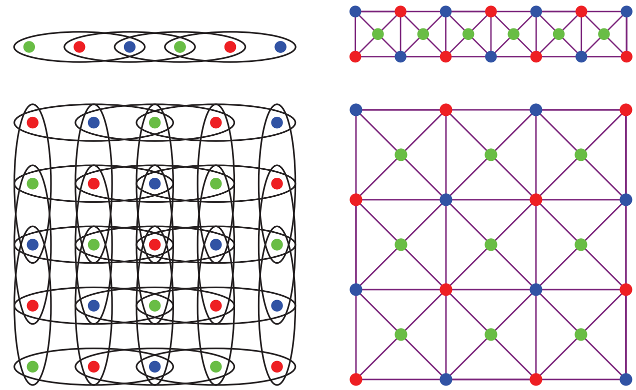

FIG. 1. (color online) Examples of hypergraphs and associated hypergraph states. Left plot: 1D and 2D order-3 cluster states; every three neighboring vertices on a row or column are connected by an order-3 hyperedge. Right plot: Union Jack states on a chain and on a 2D lattice, respectively; the three vertices of each elementary triangle are connected by an order-3 hyperedge [21]. All four hypergraphs are 3-colorable as illustrated.

A weighted independence cover $(\mathscr{A}, \mu)$ of G is a cover together with weights μ_l for $A_l \in \mathscr{A}$, where μ_l form a probability distribution. The cover strength of the cover $(\mathscr{A}, \mu)$ is defined as

$$s(\mathscr{A}, \mu) = \min_{j\in V} \sum_{l|A_l\ni j} \mu_l. \quad (3)$$

The independence degree $\gamma(G)$ of G is the maximum of $s(\mathscr{A}, \mu)$ over all weighted independence covers. The following proposition is proved in the supplement.

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

$$\frac{1}{\Delta(G)+1} \le \frac{1}{\chi(G)} \le \gamma(G) \le \min\left\{\frac{\alpha(G)}{|V|}, \frac{1}{\varpi(G)}\right\}. \quad (4)$$

Hypergraph states. The Pauli group for a qubit is generated by $X := \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and $Z := \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$. The Pauli matrices for the jth qubit are indexed by the subscript j. Given any hypergraph $G = (V, E)$ with n vertices, we can construct an n-qubit hypergraph state $|G\rangle$: 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 $e \in E$ [17, 18], that is, $|G\rangle = \left(\prod_{e\in E} CZ_e\right)|+\rangle^{\otimes n}$. 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 is empty, CZ_e is equal to the minus identity -1 by convention. When e contains a single vertex, CZ_e reduces to the Pauli operator Z on the vertex, which is local. When e connects two vertices, CZ_e is the familiar controlled-Z operation. Alternatively, the hypergraph state $|G\rangle$ is the unique eigenstate with eigenvalue 1 (up to a global phase factor) of the following n

commuting (nonlocal) stabilizer operators [17, 18],

$$K_j = X_j \otimes \prod_{e\in E|\, e\ni j} CZ_{e\setminus\{j\}}, \quad j = 1, 2, \ldots, n. \tag{5}$$

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, chromatic number, independence number, and independence degree.

Tests for hypergraph states.—Let $G = (V, E)$ be a hypergraph with n vertices and $|G\rangle$ the associated hypergraph state. Given any nonempty independent set A of G, we can devise a test for $|G\rangle$ based on two types of Pauli measurements. The test consists in measuring X_j for $j \in A$ and measuring Z_k for $k \in \overline{A}$, where $\overline{A} := V \setminus A$ is the complement of A in V. The measurement outcome on the ath qubit for $a = 1, 2, \ldots, n$ can be written as $(-1)^{o_a}$, where the Boolean variable o_a is either 0 or 1. Since A is an independent set, X_j and Z_k commute with K_i for all $i, j \in A$ and $k \in \overline{A}$. The joint eigenstate of X_j and Z_k corresponding to the outcome $\{o_a\}$ is an eigenstate of K_i, whose eigenvalue is $(-1)^{t_i}$ with

$$t_i = o_i + \sum_{e\in E|e\ni i} \Biggl(\prod_{k\in e, k\neq i} o_k\Biggr). \tag{6}$$

Now we set the criterion that the test is passed iff $(-1)^{t_i} = 1$ for all $i \in A$, then the test effectively measures all the stabilizer operators K_i for $i \in A$. The projector onto the pass eigenspace reads

$$P = \prod_{i\in A} \frac{1 + K_i}{2}. \tag{7}$$

A state ρ can pass the test with certainty iff it is stabilized by K_i for all $i \in A$. In particular, the target state $|G\rangle$ can always pass the test.

The cover protocol. Let $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ be an independence cover of G that is composed of m nonempty independent sets, then we can devise a verification protocol for $|G\rangle$ with m distinct tests. For each independent set A_l, we can construct a test with the test projector $P_l = \prod_{i\in A_l} \frac{1+K_i}{2}$. A state can pass all m tests iff it is stabilized by K_i for all $i \in \cup_{l=1}^m A_l = V$. 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* since it is based on an independence cover.

Suppose the lth test (associated with A_l) is applied with probability μ_l. Then the cover protocol is specified by the weighted independence cover $(\mathscr{A}, \mu)$. Its efficiency is determined by the spectral gap of the verification operator $\Omega(\mathscr{A}, \mu) = \sum_{l=1} \mu_l P_l$. Note that the common eigenbasis of K_i for $i \in V$ also forms an eigenbasis of $\Omega(\mathscr{A}, \mu)$. Each eigenstate $|\Psi_x\rangle$ in this basis is specified by an n bit string $x \in \{0, 1\}^n$ and satisfies the equation $K_i|\Psi_x\rangle = (-1)^{x_i}|\Psi_x\rangle$. The corresponding eigenvalue of $\Omega(\mathscr{A}, \mu)$ reads $\lambda_x = \sum_{l|\mathrm{supp}(x)\subset\overline{A}_l} \mu_l$, where $\mathrm{supp}(x) := \{i\,|\,x_i \neq 0\}$. To attain the second largest eigenvalue of $\Omega(\mathscr{A}, \mu)$, it suffices to consider the case in which x has only one bit equal to 1, which means $\beta(\Omega(\mathscr{A}, \mu)) = \max_{i\in V} \sum_{l|\overline{A}_l\ni i} \mu_l$. Similarly, the smallest eigenvalue of $\Omega(\mathscr{A}, \mu)$ is attained when all bits of x are equal to 1, in which case we have $\lambda_x = 0$. So the verification operator $\Omega(\mathscr{A}, \mu)$ is always singular. These observations confirm the following theorem.

Theorem 1. The cover protocol has the spectral gap

$$\nu(\Omega(\mathscr{A}, \mu)) = s(\mathscr{A}, \mu), \quad \tau(\Omega(\mathscr{A}, \mu)) = 0, \tag{8}$$

$$\max_{(\mathscr{A},\mu)} \nu(\Omega(\mathscr{A}, \mu)) = \gamma(G). \tag{9}$$

When $A_1, A_2, \ldots, A_m$ are pairwise disjoint, $\mathscr{A}$ defines a coloring of G, in which case the verification protocol $(\mathscr{A}, \mu)$ is also called a *coloring protocol*. Each test of the coloring protocol is associated with a color (cf. Fig. 1): X measurement is performed on all qubits associated with a given color, while Z measurement is performed on all qubits associated with other colors. The number of distinct tests is equal to the number of colors. The spectral gap of the coloring protocol $(\mathscr{A}, \mu)$ reads

$$\nu(\Omega(\mathscr{A}, \mu)) = \min_l \mu_l \leq |\mathscr{A}|^{-1} \leq \chi(G)^{-1}. \tag{10}$$

Here the first inequality is saturated iff all weights μ_l are equal; the second one is saturated iff $|\mathscr{A}| = \chi(G)$, in which case the coloring $\mathscr{A}$ is optimal (cf. the supplement). In view of this observation, by a coloring protocol, we usually assume that all weights μ_l are equal, that is, all distinct tests are performed with the same probability. Then the coloring protocol $(\mathscr{A}, \mu)$ is also referred by $\mathscr{A}$.

Theorem 1 reveals operational meanings of cover strength and independence degree in the verification of hypergraph states. Given a cover protocol $(\mathscr{A}, \mu)$ with cover strength $s(\mathscr{A}, \mu) > 0$, to verify $|G\rangle$ within infidelity ϵ and significance level δ, the number of required tests is

$$N = \left\lceil \frac{\ln \delta}{\ln[1 - s(\mathscr{A}, \mu)\epsilon]} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{s(\mathscr{A}, \mu)\epsilon} \right\rceil \tag{11}$$

according to Eq. (2). This number is minimized when the cover $(\mathscr{A}, \mu)$ is optimal, so that $s(\mathscr{A}, \mu) = \gamma(G)$ and

$$N = \left\lceil \frac{\ln \delta}{\ln[1 - \gamma(G)\epsilon]} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{\gamma(G)\epsilon} \right\rceil. \tag{12}$$

According to Proposition 1, we have

$$N \leq \left\lceil \frac{\chi(G)}{\epsilon} \ln \frac{1}{\delta} \right\rceil \leq \left\lceil \frac{\Delta(G) + 1}{\epsilon} \ln \frac{1}{\delta} \right\rceil \leq \left\lceil \frac{n}{\epsilon} \ln \frac{1}{\delta} \right\rceil. \tag{13}$$

Here the first upper bound can be achieved by an optimal coloring protocol; the second one can be achieved by a coloring constructed from a simple greedy algorithm as presented in the proof of Proposition 1.

The above analysis shows that any hypergraph state $|G\rangle$ can be verified with at most $m = \Delta(G) + 1$ measurement settings in which each party performs either X or

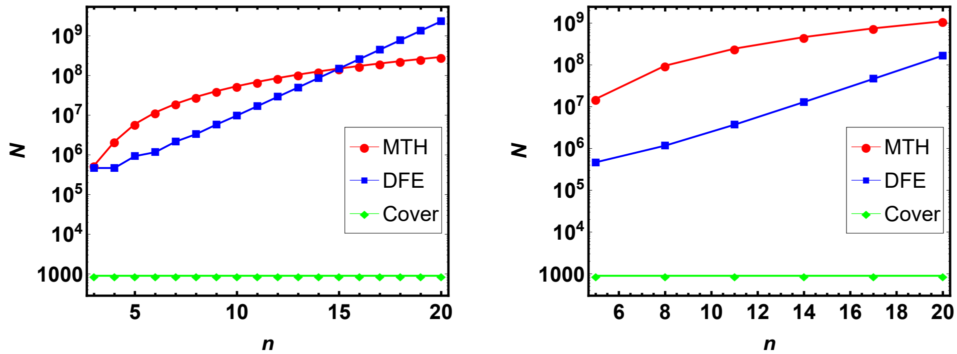

FIG. 2. (color online) Resource costs for verifying hypergraph states in the nonadversarial scenario. Left plot: 1D order-3 cluster states; right plot: Union Jack states on a chain. Here n is the number of qubits of the hypergraph state, and N is the (expected) number of tests required to verify the state within infidelity $\epsilon = 0.01$ and significance level $\delta = 0.05$. In the case of the MTH protocol proposed in Ref. [23], only a lower bound for N is given (cf. Appendix E 3). The lines are guides for the eye. Our cover protocol dramatically outperforms direct fidelity estimation (DFE) [33] and the MTH protocol (cf. Appendix E).

Z measurement. Note that m is upper bounded by the number n of qubits. The total number of tests is only $\lceil m \ln \delta^{-1}/\epsilon \rceil$ and is at most m times as large as the number for the best protocol based on entangling measurements. The cover protocol for hypergraph states is dramatically more efficient than previous protocols [23, 33], as illustrated in Fig. 2 and discussed in detail in the supplement. Consider the protocol of Ref. [23] for example, both the number of measurement settings and the total number of tests increase exponentially with $\Delta(G)$; in addition, the number of tests scales as $1/\epsilon^2$ instead of $1/\epsilon$.

For many interesting 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 small constants. In this case, the cover protocol can achieve the optimal scaling behavior as the best protocol based on entangling measurements. For example, only two measurement settings are necessary for all graph states of 2-colorable graphs (equivalent to Calderbank-Shor-Steane state [36]), including GHZ states, cluster states (of arbitrary dimensions), 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 cover protocol for the adversarial scenario.— Thanks to Theorem 5 and Corollary 5 in Ref. [35], the cover protocol can also be applied in the adversarial scenario. Now the number of tests required to verify the hypergraph state $|G\rangle$ within infidelity ϵ and significance level δ satisfies

$$\min\left\{\left\lceil \frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil, \left\lceil \frac{1}{\delta\epsilon}-1\right\rceil\right\} \le N \le \left\lceil \frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil, \quad (14)$$

where $\nu(\Omega) = s(\mathscr{A}, \mu)$. This is much more efficient than all protocols known in the literature. Nevertheless, the scaling with δ is suboptimal.

To improve the scaling behavior, here we propose a *hedged cover protocol* $(\mathscr{A}, \mu)_p$, which is characterized

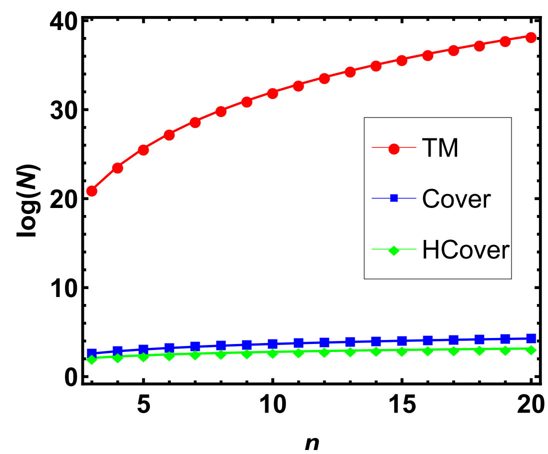

FIG. 3. (color online) Resource costs for verifying 3-colorable hypergraph states in the adversarial scenario. Here n is the number of qubits, and N is the number of tests required to verify the state within infidelity $\epsilon = 1/(4n)$ and significance level $\delta = 1/(4n)$; here "log" has base 10. The lines are guides for the eye. Our cover protocol (Cover) and hedged cover protocol (HCover) outperform the TM protocol proposed in Ref. [34] by at least 18 orders of magnitude.

by the verification operator $\Omega_p = (1-p)\Omega + p$ with $\Omega = \Omega(\mathscr{A}, \mu)$. The name "hedged cover protocol" reflects the fact that the trivial test is introduced to hedge the influence of small eigenvalues of the operator Ω. When $p = p_*(\nu)$ is the optimal probability determined by $\nu = s(\mathscr{A}, \mu)$ (see the supplement for more details), the hedged cover protocol $(\mathscr{A}, \mu)_p$ is also denoted by $(\mathscr{A}, \mu)_*$. The protocol $(\mathscr{A}, \mu)_p$ is called a *hedged coloring protocol* if $\mathscr{A}$ is a coloring of G and all μ_l are equal. If $(\mathscr{A}, \mu)$ denotes the optimal coloring protocol, then $\nu = 1/\chi(G)$ and the number of tests required by $(\mathscr{A}, \mu)_*$ satisfies

$$N \le \frac{[\chi(G) + \mathrm{e} - 1]\ln(F\delta)^{-1}}{\epsilon} \le \frac{[\Delta(G) + \mathrm{e}]\ln(F\delta)^{-1}}{\epsilon}, \quad (15)$$

which is comparable to the nonadversarial scenario.

To illustrate the advantage of the cover protocol and hedged cover protocol, consider the verification of n-qubit 3-colorable hypergraph states (including order-3 cluster states and Union Jack states) in the adversarial scenario. To achieve infidelity $\epsilon = 1/(4n)$ and significance level $\delta = 1/(4n)$, the protocol proposed in a recent paper Ref. [34] requires at least $9.5 \times 10^{10} n^{21}$ tests (cf. the supplement), which is already astronomical in the simplest nontrivial scenario. By contrast, the optimal cover or coloring protocol with $\nu(\Omega) = \gamma(G) = 1/\chi(G) = 1/3$ requires at most $12n(4n-1)$ tests by Eq. (14), which outperforms Ref. [34] by at least 18 orders of magnitude even when $n = 3$, and the advantage increases rapidly with n. The hedged cover protocol can further reduce the number to $\lfloor 16.3n \ln \frac{16n^2}{4n-1} \rfloor$ as shown in the supplement.

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 dramatically more efficient than all known candidates based on local measurements and is comparable to the best protocols based on entangling measurements. In general, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. This protocol enables the verification of hypergraph states of thousands of qubits, which is instrumental to quantum information processing and to demonstrating quantum supremacy. Moreover, this protocol can be applied to the adversarial scenario and is thus particularly appealing to blind MBQC and quantum networks.

ACKNOWLEDGEMENTS

HZ is grateful to Zhibo Hou and Jiangwei Shang for discussions. This work is supported by the National Natural Science Foundation of China (Grant No. 11875110). 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. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865 (2009).

[2] O. Gühne and G. Tóth, "Entanglement detection," Phys. Rep. **474**, 1 (2009).

[3] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188–5191 (2001).

[4] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," Phys. Rev. A **68**, 022312 (2003).

[5] 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.

[6] T. Morimae and K. Fujii, "Blind quantum computation protocol in which Alice only makes measurements," Phys. Rev. A **87**, 050301 (2013).

[7] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing," Phys. Rev. Lett. **115**, 220502 (2015).

[8] 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`.

[9] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," Phys. Rev. A **65**, 012308 (2001).

[10] 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).

[11] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, "Experimental verification of multipartite entanglement in quantum networks," Nature Commun. **7**, 13251 (2016).

[12] D. Markham and A. Krause, "A simple protocol for certifying graph states and applications in quantum networks," (2018), arXiv:1801.05057.

[13] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," American J. Phys. **58**, 1131–1143 (1990).

[14] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, "Nonlocality of cluster states of qubits," Phys. Rev. A **71**, 042325 (2005).

[15] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, "Bell inequalities for graph states," Phys. Rev. Lett. **95**, 120405 (2005).

[16] C. Kruszynska and B. Kraus, "Local entanglability and multipartite entanglement," Phys. Rev. A **79**, 052304 (2009).

[17] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, "Encoding hypergraphs into quantum states," Phys. Rev. A **87**, 022311 (2013).

[18] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, "Quantum hypergraph states," New J. Phys. **15**, 113022 (2013).

[19] F. E. S. Steinhoff, C. Ritz, N. I. Miklin, and O. Gühne, "Qudit hypergraph states," Phys. Rev. A **95**, 052340 (2017).

[20] 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).

[21] J. Miller and A. Miyake, "Hierarchy of universal entanglement in 2D measurement-based quantum computation," npj Quantum Inf. **2**, 16036 (2016).
[22] J. Miller and A. Miyake, "Latent computational complexity of symmetry-protected topological order with fractional symmetry," Phys. Rev. Lett. **120**, 170503 (2018).
[23] T. Morimae, Y. Takeuchi, and M. Hayashi, "Verification of hypergraph states," Phys. Rev. A **96**, 062321 (2017).
[24] M. Gachechiladze, C. Budroni, and O. Gühne, "Extreme violation of local realism in quantum hypergraph states," Phys. Rev. Lett. **116**, 070401 (2016).
[25] M. Gachechiladze, O. Gühne, and A. Miyake, "Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states," (2018), arXiv:1805.12093.
[26] Y. Takeuchi, T. Morimae, and M. Hayashi, "Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements," (2018), arXiv:1809.07552.
[27] B. Yoshida, "Topological phases with generalized global symmetries," Phys. Rev. B **93**, 155131 (2016).
[28] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-case complexity versus approximate simulation of commuting quantum computations," Phys. Rev. Lett. **117**, 080501 (2016).
[29] K. Fujii and M. Hayashi, "Verifiable fault tolerance in measurement-based quantum computation," Phys. Rev. A **96**, 030301 (2017).
[30] M. Hayashi and M. Hajdušek, "Self-guaranteed measurement-based quantum computation," Phys. Rev. A **97**, 052308 (2018).
[31] S. Pallister, N. Linden, and A. Montanaro, "Optimal verification of entangled states with local measurements," Phys. Rev. Lett. **120**, 170502 (2018).
[32] 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).
[33] S. T. Flammia and Y.-K. Liu, "Direct fidelity estimation from few Pauli measurements," Phys. Rev. Lett. **106**, 230501 (2011).
[34] Y. Takeuchi and T. Morimae, "Verification of many-qubit states," Phys. Rev. X **8**, 021060 (2018).
[35] H. Zhu and M. Hayashi, "Efficient verification of pure quantum states in the adversarial scenario," In preparation.
[36] K. Chen and H.-K. Lo, "Multi-partite quantum cryptographic protocols with noisy GHZ states," Quantum Info. Comput. **7**, 689–715 (2007).
[37] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, "Resource-efficient verification of quantum computing using Serfling's bound," (2018), arXiv:1806.09138.
[38] D. Schlingemann, "Stabilizer codes can be realized as graph codes," Quantum Info. Comput. **2**, 307–323 (2002).
[39] 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.

APPENDIX

In this supplement, we provide additional results and more details on hypergraphs and the cover protocol (non-adversarial and adversarial scenario). We then generalize the cover protocol to qudit hypergraph states. Finally, we compare our work with previous works.

Appendix A: Cover strengths and independence degrees of Hypergraphs

1. Proof of Proposition 1

Proof. The inequality $\frac{1}{\Delta(G)+1} \leq \frac{1}{\chi(G)}$ is equivalent to $\chi(G) \leq \Delta(G)+1$ and 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 j is at most $\min\{\deg(v_j)+1, j\}$. Therefore,

$$\chi(G) \leq \max_j \min\{\deg(v_j)+1, j\} \leq \Delta(G)+1. \tag{A1}$$

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 $(\mathscr{A}, \mu)$ be an arbitrary independence cover. Then

$$\begin{aligned} |V|s(\mathscr{A},\mu) &= |V| \min_{j\in V} \sum_{l|A_l \ni j} \mu_l \leq \sum_j \sum_{l|A_l\ni j} \mu_l \\ &= \sum_l \mu_l |A_l| \leq \alpha(G) \sum_l \mu_l = \alpha(G), \end{aligned} \tag{A2}$$

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

$$\begin{aligned} &\varpi(G)s(\mathscr{A},\mu) = \varpi(G) \min_{j\in V} \sum_{l|A_l\ni j} \mu_l \leq \sum_{j\in V_{\mathrm{C}}} \sum_{l|A_l\ni j} \mu_l \\ &\leq \sum_l \mu_l = 1, \end{aligned} \tag{A3}$$

where the second inequality follows from the fact that each independent set A_l can contain at most one vertex in the clique V_{C}. $\square$

TABLE I. Degrees $\Delta(G)$, clique numbers $\varpi(G)$, independence numbers $\alpha(G)$, chromatic numbers $\chi(G)$, and independence degrees $\gamma(G)$ of common graphs and hypergraphs of n vertices. A graph is complete if every two vertices are adjacent. Note that the odd cycle of three vertices is complete. Here we assume that each 2-colorable graph has at least one edge, while each 3-colorable hypergraph has at least one hyperedge of order 3, as illustrated in Fig. 1.

hypergraphs G	$\Delta(G)$	$\varpi(G)$	$\alpha(G)$	$\chi(G)$	$\gamma(G)$
square lattice	4	2	$\lceil n/2 \rceil$	2	1/2
cubic lattice in dimension k	$2k$	2	$\lceil n/2 \rceil$	2	1/2
triangular lattice	6	3	$\geq n/3$	3	1/3
even cycle	2	2	$n/2$	2	1/2
odd cycle ($n \geq 5$)	2	2	$(n-1)/2$	3	$(n-1)/(2n)$
complete graph	$n-1$	n	1	n	$1/n$
2-colorable graph	-	2	$\geq n/2$	2	1/2
3-colorable hypergraph	-	3	$\geq n/3$	3	1/3

As an implication of Proposition 1, $\gamma(G) \geq 1/n$ for any hypergraph of n vertices since $\Delta(G) \leq n-1$ and $\chi(G) \leq n$. In addition, $\gamma(G) = 1/m$ if the hypergraph G has chromatic number and clique number both equal to 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 square lattice (or analogs in higher dimensions) or an even cycle; $\gamma(G) = 1/3$ when G is a triangular lattice.

The degrees, clique numbers, independence numbers, chromatic numbers, and independence degrees of common graphs and hypergraphs are shown in Table I.

2. Cover strengths of colorings and minimal covers

Let $G = (V, E)$ be a hypergraph and $(\mathscr{A}, \mu)$ a weighted independence cover constructed from a coloring $\mathscr{A}$, assuming that no independent set in $\mathscr{A}$ is empty (note that empty independent sets cannot increase the cover strength). Then each vertex of V is contained in only one independent set in $\mathscr{A}$, which implies that

$$s(\mathscr{A}, \mu) = \min_l \mu_l \leq |\mathscr{A}|^{-1} \leq \chi(G)^{-1}. \tag{A4}$$

Here the first inequality is saturated iff all weights μ_l are equal, and the second inequality is saturated iff the coloring $\mathscr{A}$ is optimal in the sense that no other coloring of G requires fewer colors.

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

$$s(\mathscr{A}, \mu) = \min_l \mu_l \leq |\mathscr{A}|^{-1} \leq \chi(G)^{-1} \tag{A5}$$

as in Eq. (A4). Again the first inequality is saturated iff all weights μ_l are equal; the second inequality is saturated iff $|\mathscr{A}| = \chi(G)$, in which case an optimal coloring of G can be constructed from $\mathscr{A}$ by deleting some vertices in some independent sets if $\mathscr{A}$ is not yet a coloring.

In view of the above discussion, to maximize the cover strength it is always beneficial to choose uniform weights when $\mathscr{A}$ 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.

3. Independence degrees of odd cycles

Here we determine the independence degrees of odd cycles, which indicate 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.

Let C_n be a cycle with n vertices, where n is an odd integer. Then we have $\alpha(C_n) = (n-1)/2$, 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

$$A_j = \{j, j+2, \ldots, j+n-3\}, \quad j = 1, 2, \ldots, n. \tag{A6}$$

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

$$\gamma(C_n) = \frac{n-1}{2n} = \frac{1}{2} - \frac{1}{2n}, \tag{A7}$$

which increases monotonically with n. 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. These observations are of interest to constructing efficient verification protocols for hypergraph states (including graph states in particular).

Appendix B: Properties of test projectors for hypergraph states

Given any independent set A of a hypergraph $G = (V, E)$, we can construct a test for the hypergraph state $|G\rangle$, with the test projector given in Eq. (7) in the main text. Denote by $\mathscr{N}(A)$ the neighborhood of A in the graph G, that is, the set of vertices in G that are adjacent to at least one vertex in A. Note that $\mathscr{N}(A)$ and A are disjoint, that is, $\mathscr{N}(A) \subset \overline{A}$, given that A is an independent set. The complement $\overline{A}$ used in constructing the test can be replaced by $\mathscr{N}(A)$ because Eq. (6) only involves measurement outcomes associated with vertices in the set $A \cup \mathscr{N}(A)$. In other words, Z measurement associated with vertices in $\overline{A} \setminus \mathscr{N}(A)$ is redundant.

The rank of the test projector P in Eq. (7) is

$$\mathrm{rank}(P) = \mathrm{tr}(P) = 2^{n-|A|}, \tag{B1}$$

where $|A|$ denotes the cardinality of the set A; the larger is $|A|$, the smaller is $\mathrm{rank}(P)$. In view of this observation, it is beneficial to choose large independent sets for constructing test projectors for the hypergraph state $|G\rangle$. In particular, the independent set A can be enlarged when $A \cup \mathscr{N}(A)$ is a proper subset of the vertex set V. Conversely, if $A \cup \mathscr{N}(A) = V$, then $\mathscr{N}(A) = \overline{A}$, and A cannot be contained in any larger independent set. Incidentally, the cardinality $|A|$ is upper bounded by the independence number $\alpha(G)$. Suppose G has at least one nontrivial hyperedge or edge; then $\alpha(G) \leq n-1$, which implies that $\mathrm{rank}(P) \geq 2$. So at least two distinct tests are necessary to verify $|G\rangle$ as expected.

Appendix C: The cover protocol for the adversarial scenario

In this section we provide more details on the cover protocol and hedged cover protocol for the adversarial scenario. Thanks to Theorem 5 and Corollary 5 in Ref. [35], the cover protocol can also be applied to verifying hypergraph states in the adversarial scenario, which is very important to many quantum information processing tasks that entail high-security requirements, such as blind MBQC. Let $\Omega = \Omega(\mathscr{A}, \mu)$ be the verification operator associated with the cover protocol $(\mathscr{A}, \mu)$, then $\nu(\Omega) = s(\mathscr{A}, \mu)$ and $\tau(\Omega) = 0$ according to Theorem 1. By Corollary 5 in Ref. [35], the number of tests required to verify $|G\rangle$ within infidelity ϵ and significance level δ satisfies

$$\min\left\{\left\lceil \frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil, \left\lceil \frac{1}{\delta\epsilon} - 1\right\rceil\right\} \leq N \leq \left\lceil \frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil. \tag{C1}$$

For the optimal coloring protocol with $\nu(\Omega) = 1/\chi(G)$, we have

$$N \leq \left\lceil \frac{\chi(G)(1-\delta)}{\delta\epsilon}\right\rceil \leq \left\lceil \frac{\Delta(G)+1}{\delta\epsilon}\right\rceil \leq \left\lceil \frac{n}{\delta\epsilon}\right\rceil. \tag{C2}$$

If in addition G is a 2-colorable graph, then $\nu(\Omega) = 1/2$ and the lower bound in Eq. (C1) is saturated according to Ref. [35].

Since $\Omega(\mathscr{A}, \mu)$ is singular according to Theorem 1, the suboptimal scaling of N with δ in Eq. (C1) cannot be improved without modifying the protocol. Fortunately, it is easy to improve the scaling behavior by performing the trivial test with a suitable probability according to Ref. [35]. As an alternative to $(\mathscr{A}, \mu)$, the hedged cover protocol $(\mathscr{A}, \mu)_p$ is characterized by the following verification operator

$$\Omega_p = (1-p)\Omega + p. \tag{C3}$$

The name "hedged cover protocol" reflects the fact that the trivial test is introduced to hedge the influence of small eigenvalues of the operator $\Omega = \Omega(\mathscr{A}, \mu)$. To achieve high efficiency, the value of p can be chosen as follows according to Ref. [35],

$$p_*(\nu) = \min\{p > 0 | p \ln p^{-1} \geq \beta_p \ln \beta_p^{-1}\}, \tag{C4}$$

where

$$\beta_p = (1-p)\beta + p = (1-p)(1-\nu) + p \tag{C5}$$

is a function of $\nu = s(\mathscr{A}, \mu)$. When $p = p_*(\nu)$, the hedged cover protocol $(\mathscr{A}, \mu)_p$ is also denoted by $(\mathscr{A}, \mu)_*$.

Thanks to Theorem 6 in Ref. [35], by virtue of the hedged cover protocol $(\mathscr{A}, \mu)_*$, that is, $(\mathscr{A}, \mu)_p$ with $p = p_*(\nu)$, the number of tests in Eq. (C1) can be reduced to

$$\begin{aligned} N &= \left\lceil \frac{h_*(\nu)\ln(F\delta)^{-1}}{\epsilon}\right\rceil \leq \frac{\ln(F\delta)^{-1}}{(1-\nu+\mathrm{e}^{-1}\nu^2)\nu\epsilon} \\ &\leq \frac{(1+\mathrm{e}\nu-\nu)\ln(F\delta)^{-1}}{\nu\epsilon} \leq \frac{\mathrm{e}\ln(F\delta)^{-1}}{\nu\epsilon}, \end{aligned} \tag{C6}$$

where $\nu = s(\mathscr{A}, \mu)$, $F = 1-\epsilon$,

$$h_*(\nu) = -p_*(\nu)\ln p_*(\nu), \tag{C7}$$

and e is the base of the natural logarithm. Here the three upper bounds still apply if we choose the hedged cover protocol $(\mathscr{A}, \mu)_p$ with $p = \nu/\mathrm{e}$. If $(\mathscr{A}, \mu)$ denotes the optimal cover protocol, then $\nu = \gamma(G)$. If $(\mathscr{A}, \mu)$ denotes the optimal coloring protocol, then $\nu = 1/\chi(G)$ and the number of tests required by $(\mathscr{A}, \mu)_*$ satisfies

$$\begin{aligned} N &\leq \frac{[\chi(G)+\mathrm{e}-1]\ln(F\delta)^{-1}}{\epsilon} \leq \frac{[\Delta(G)+\mathrm{e}]\ln(F\delta)^{-1}}{\epsilon} \\ &\leq \frac{(n+\mathrm{e}-1)\ln(F\delta)^{-1}}{\epsilon}. \end{aligned} \tag{C8}$$

The second bound still applies if the optimal coloring is replaced by a coloring with $\chi(G)+1$ colors. Although in general it is not easy to find an optimal coloring of the hypergraph G, it is easy to find a coloring with $\chi(G)+1$ colors by virtue of the greedy algorithm (see the proof of Proposition 1). Therefore, the hedged cover (or coloring) protocol can achieve the same optimal scaling behavior in the number N of tests with ϵ^{-1} and δ^{-1} as the counterpart in the nonadversarial scenario; cf. Eq. (13). Accordingly, all the conclusions on the cover protocol presented in the main text can easily be adapted for the adversarial scenario. For many hypergraph states of practical interest, $\chi(G)$ is upper bounded by a small constant, so the number of tests required by the hedged cover protocol is comparable to the best protocol based on entangling measurements.

To illustrate the advantage of the cover protocol and hedged cover protocol, consider the verification of n-qubit 3-colorable hypergraph states (including order-3 cluster states and Union Jack states) in the adversarial scenario. To achieve infidelity $\epsilon = 1/(4n)$ and significance level $\delta = 1/(4n)$, the protocol proposed by Takeuchi and Morimae in a recent paper [34] requires at least $9.5 \times 10^{10} n^{21}$ tests (cf. Appendix E 5), which is already astronomical in the simplest nontrivial scenario. By contrast, the optimal cover or coloring protocol with $\nu(\Omega) = \gamma(G) = 1/\chi(G) = 1/3$ requires at most $12n(4n-1)$ tests according to Eq. (C1), which outperforms Ref. [34] by at least 18 orders of magnitude even when $n = 3$, and the advantage increases rapidly with the number n of qubits. According to Eq. (C6), the hedged cover protocol can further reduce the number to

$$\left\lfloor 4nh_*(\nu)\ln\frac{16n^2}{4n-1}\right\rfloor \leq \left\lfloor 16.3n\ln\frac{16n^2}{4n-1}\right\rfloor; \tag{C9}$$

the inequality holds because $h_*(\nu = 1/3) < 4.052$, which can be verified by numerical calculation based on Eqs. (C4) and (C4).

Appendix D: Verification of qudit hypergraph states

Most previous verification protocols only apply to qubit hypergraph states [23, 34]. Here we show that the cover protocol for verifying hypergraph states can also be applied to qudit hypergraph states with minor modifications, and most conclusions on the verification of qubit hypergraph states remain the same. This merit is appealing to both theoretical studies and practical applications.

1. Qudit hypergraphs

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 $E \subset \mathscr{P}(V)$ together with multiplicities specified by $m_E = (m_e)_{e\in E}$, where $m_e \in \mathbb{Z}_d$ with $m_e \neq 0$ and $\mathbb{Z}_d$ is the ring of integers modulo d [19, 20]. 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, independent set and independence number, (weighted) independence cover, cover strength, and independence degree. Therefore, Proposition 1 and its proof are applicable without any modification.

2. Qudit hypergraph states

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

$$X = \sum_{j\in\mathbb{Z}_d} |j+1\rangle\langle j|, \quad Z = \sum_{j\in\mathbb{Z}_d} \omega^j |j\rangle\langle j|, \tag{D1}$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$ is a primitive dth 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 $|+\rangle := \frac{1}{\sqrt{d}}\sum_{j\in\mathbb{Z}_d}|j\rangle$ (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 [19, 20], that is,

$$|G\rangle = \left(\prod_{e\in E} CZ_e^{m_e}\right)|+\rangle^{\otimes n}. \tag{D2}$$

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

$$CZ_e := \sum_{j_1,j_2,\ldots,j_k\in\mathbb{Z}_d} \omega^{j_1 j_2\ldots j_k}|j_1, j_2, \ldots, j_k\rangle\langle j_1, j_2, \ldots, j_k|; \tag{D3}$$

the general case is defined analogously. Alternatively, $|G\rangle$ is the unique eigenstate with eigenvalue 1 (up to a global phase factor) of the n commuting (nonlocal) stabilizer operators [19, 20]

$$K_j = X_j \otimes \prod_{e\in E\,|\, e\ni j} CZ_{e\setminus\{j\}}^{m_e}, \quad j = 1, 2, \ldots, n. \tag{D4}$$

Note that $K_j^d = 1$, so all eigenvalues of K_j are powers of ω. As in the qubit case, graph theoretic concepts related to the hypergraph G also apply to the corresponding state $|G\rangle$.

3. 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 $\mathscr{A} = \{A_1, A_2, \ldots\}$ of G and let $\overline{A}_l := V \setminus A_l$ be the complement of A_l in V. Then we can construct a verification protocol with $|\mathscr{A}|$ distinct tests (measurement settings): the lth 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 ath qubit for $a = 1, 2, \ldots, n$ can be written as ω^{o_a}, where $o_a \in \mathbb{Z}_d$. 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 ω^{t_i} with

$$t_i = o_i + \sum_{e\in E|e\ni i} m_e \prod_{k\in e, k\neq i} o_k \tag{D5}$$

according to Eq. (D4). The test is passed if $\omega^{t_i} = 1$ for all $i \in A_l$. The projector onto the pass eigenspace associated with the lth test reads

$$P_l = \prod_{i\in A_l}\left(\frac{1}{d}\sum_{b\in\mathbb{Z}_d} K_i^b\right). \tag{D6}$$

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 lth test is applied with probability μ_l. The efficiency of the resulting protocol is determined by the spectral gap of $\Omega(\mathscr{A},\mu) = \sum_{l=1}\mu_l P_l$. Here the common eigenbasis of K_i for $i \in V$ also form an eigenbasis of $\Omega(\mathscr{A},\mu)$. 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 $\Omega(\mathscr{A},\mu)$ reads

$$\lambda_x = \sum_{l|\mathrm{supp}(x)\subset\overline{A}_l} \mu_l, \tag{D7}$$

where $\mathrm{supp}(x) := \{i\,|\,x_i \neq 0\}$. The second largest eigenvalue of $\Omega(\mathscr{A},\mu)$ can be attained when $x_i = 0$ for all $i \in V$ except for one of them, so that

$$\beta(\Omega(\mathscr{A},\mu)) = \max_{i\in V}\sum_{l|\overline{A}_l\ni i}\mu_l, \tag{D8}$$

$$\nu(\Omega(\mathscr{A},\mu)) = \min_{i\in V}\sum_{l|A_l\ni i}\mu_l = s(\mathscr{A},\mu), \tag{D9}$$

as in the case of qubit hypergraph states. Similarly, the smallest eigenvalue of $\Omega(\mathscr{A},\mu)$ is attained when all bits of x are nonzero, in which case we have $\lambda_x = 0$. Again, the verification operator $\Omega(\mathscr{A},\mu)$ is always singular. Therefore, Theorem 1 and Eqs. (10)-(15) in the main text as well as Eqs. (C1)-(C8) in the supplement are also applicable in the qudit case.

Appendix E: Comparison with existing works

In this section we discuss the connections and distinctions between our work and entanglement detection. We then compare our approach to state verification with a number of existing works, including direct fidelity estimation (DFE) [33] and Refs. [23, 30, 34, 37].

1. State verification and 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 necessarily optimized for this purpose. In the literature, there are many works on the detection of entanglement, including GME in particular [2]. 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 in 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 and practical questions directly. Crucial to achieving this task is efficient state verification, which is the 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 explicit number of tests required. In addition, our approach can be applied to the adversarial scenario, which is appealing to many applications.

2. Comparison with direct fidelity estimation

In this section we compare our cover protocol with DFE introduced by Flammia and Liu [33]. Compared with the cover protocol, 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 of more than 15 qubits.

1. To apply DFE it is necessary to sample from the squared characteristic function defined on the dis-

crete 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 target infidelity ϵ and significance level δ. 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

$$\begin{aligned} N_{\mathrm{DFE}} &\approx 1+\frac{1}{\epsilon^2\delta}+\frac{2g}{D\epsilon^2}\ln(2/\delta) \\ &= 1+\frac{1}{\epsilon^2\delta}+\frac{2\tilde{g}}{\epsilon^2}\ln(2/\delta), \end{aligned} \tag{E1}$$

where $D=2^n$, $\tilde{g}=g/2^n$, and g is the number of points at which the characteristic function is nonzero [33]. It is known that $g\geq D$ and the lower bound is saturated iff 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 many hypergraph states.

The number N_{DFE} in Eq. (E1) can be reduced for a well-conditioned state ρ, which means either $|\operatorname{tr}(\rho W_{x,z})|=0$ or $|\operatorname{tr}(\rho W_{x,z})|\geq c$ for all Pauli operators $W_{x,z}$ [cf. Eq. (E4) 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 $O\big(\ln(1/\delta)/(c^2\epsilon^2)\big)$, 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 for determining 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 [17, 18]. In other words, any n-qubit hypergraph state can be written as

$$|\Psi_f\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle, \tag{E2}$$

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

$$f(x)=\sum_{e\in E}\prod_{j\in e}x_j, \tag{E3}$$

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

$$W_{x,z}:=\left(\prod_{j=1}^n X_j^{x_j}\right)\left(\prod_{j=1}^n Z_j^{z_j}\right),\quad x,z\in\{0,1\}^n, \tag{E4}$$

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

$$\langle\Psi_f|W_{x,z}|\Psi_f\rangle=\frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{f(u)+f(u+x)}(-1)^{z\cdot u}, \tag{E5}$$

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

$$g(f)=\big|\big\{(x,z)\in\{0,1\}^{2n}\,|\,\langle\Psi_f|W_{x,z}|\Psi_f\rangle\neq 0\big\}\big|. \tag{E6}$$

In the rest of this section, we provide several concrete examples of hypergraph states for which $\tilde{g}=g/2^n$ increases exponentially with the number n of qubits, which means N_{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

$$f_n(u):=\prod_{j=1}^n u_j=\begin{cases}1 & u=11\cdots 1,\\ 0 & \text{otherwise.}\end{cases} \tag{E7}$$

In this case, we have

$$2^n\big|\langle\Psi_{f_n}|W_{x,z}|\Psi_{f_n}\rangle\big|=\begin{cases}2^n & x=z=0,\\ 2^n-4 & z=0, x\neq 0,\\ 4 & x\neq 0, z\neq 0, x\cdot z=0,\\ 0 & x\cdot z=1,\ \text{or } x=0, z\neq 0,\end{cases} \tag{E8}$$

which implies that

$$g(f_n)=2^{2n-1}-2^{n-1}+1,\quad \tilde{g}\approx 2^{n-1}-2^{-1}. \tag{E9}$$

So the number of measurements in Eq. (E1) reduces to

$$N_{\mathrm{DFE}}\approx 1+\frac{1}{\epsilon^2\delta}+\frac{2^n-1}{\epsilon^2}\ln(2/\delta), \tag{E10}$$

which increases exponentially with the number of qubits. By contrast, the number of tests required by our cover protocol is at most $\lceil (n/\epsilon)\ln(1/\delta)\rceil$ by Eq. (13) in the main text, which is exponentially smaller than $N_{\rm DFE}$.

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,

$$g = g(f_3)^{n/3} = 29^{n/3} > 3^n, \quad \tilde{g} = \frac{29^{n/3}}{2^n} > \left(\frac{3}{2}\right)^n. \tag{E11}$$

So the number of measurements in Eq. (E1) reduces to

$$\begin{aligned} N_{\rm DFE} &\approx 1 + \frac{1}{\epsilon^2\delta} + \frac{2\times 29^{n/3}}{2^n\epsilon^2}\ln(2/\delta) \\ &> 1 + \frac{1}{\epsilon^2\delta} + \frac{2\left(\frac{3}{2}\right)^n}{\epsilon^2}\ln(2/\delta), \end{aligned} \tag{E12}$$

which also increases exponentially with the number of qubits. By contrast, the number of tests required by the cover protocol is $\lceil (3/\epsilon)\ln(1/\delta)\rceil$, which is again exponentially smaller than $N_{\rm DFE}$.

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. 2), so $N_{\rm DFE}$ also increases exponentially with n for these states. The number of tests required by the cover protocol is still $\lceil (3/\epsilon)\ln(1/\delta)\rceil$.

3. Comparison with Ref. [23]

Recently, Morimae, Takeuchi, and Hayashi (MTH) [23] 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. (5) 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 $\sum_{j=1}^n 4^{r_j}$, which increases exponentially with the number of order-3 hyperedges. MTH also set a criterion such that the probability of a state ρ to satisfy the criterion is given by

$$p = \frac{1}{2} + \frac{\operatorname{tr}(\rho K_j)}{2^{r_j+1}} = \frac{1}{2} + \frac{1-a_j}{2^{r_j+1}}, \tag{E13}$$

where $a_j := 1 - \operatorname{tr}(\rho K_j)$. Although the target state $|G\rangle$ can attain the maximum probability $(1/2) + (1/2^{r_j+1})$, 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

$$f_j \geq \frac{1}{2} + \frac{1-\theta}{2^{r_j+1}}, \tag{E14}$$

where θ is a small positive constant. The state ρ is accepted if it can pass all the stabilizer tests. The choice of θ 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 ρ can pass the stabilizer test associated with K_j can be upper bounded as follows,

$$\begin{aligned} &\Pr\left(f_j \geq \frac{1}{2} + \frac{1-\theta}{2^{r_j+1}}\right) = \Pr\left(f_j \geq p + \frac{a_j-\theta}{2^{r_j+1}}\right) \\ &\leq \exp\left(-2\frac{(a_j-\theta)^2}{4^{r_j+1}}N_j\right), \end{aligned} \tag{E15}$$

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 ϵ and significance level δ. They considered a related, but different verification problem with a different criterion, which requires about $nk+1+m$ tests, where $k = 2^{2r+3}n^7$, $m \geq 2n^7k^2\ln 2$, and $r = \max_j r_j$. In other words, the number of required tests satisfies

$$\begin{aligned} nk+1+m &\geq nk+1+2n^7k^2\ln 2 \cong 2n^7k^2\ln 2 \\ &= 2^{4r+7}n^{21}\ln 2. \end{aligned} \tag{E16}$$

While this number is still polynomial in n if r does not increase with n, it grows rapidly with n. Actually, it 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 by our cover protocol satisfies

$$N \leq \left\lceil \frac{\Delta(G)+1}{\delta\epsilon}\right\rceil \leq \left\lceil \frac{2r+1}{\delta\epsilon}\right\rceil \tag{E17}$$

according to Eq. (C2), which is independent of n and outperforms the MTH protocol dramatically. According to Eq. (C8), the hedged cover protocol can further reduce the number of tests to

$$N \leq \frac{[\Delta(G)+\mathrm{e}]\ln(F\delta)^{-1}}{\epsilon} \leq \frac{(2r+\mathrm{e})\ln(F\delta)^{-1}}{\epsilon}. \tag{E18}$$

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

$$\prod_j \Pr\left(f_j \geq \frac{1}{2}+\frac{1-\theta}{2^{r_j+1}}\right) = \Pr\left(f_j \geq p+\frac{a_j-\theta}{2^{r_j+1}}\right) \leq \delta. \tag{E19}$$

According to Eq. (E15), it suffices to guarantee that

$$\prod_{j|a_j\geq\theta} \exp\left(-2\frac{(a_j-\theta)^2}{4^{r_j+1}}N_j\right) \leq \delta. \tag{E20}$$

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

$$\begin{aligned} 1-\langle G|\rho|G\rangle &= 1-\operatorname{tr}\left(\rho\prod_j\frac{K_j+1}{2}\right)\\ &\leq \sum_j\left[1-\operatorname{tr}\left(\rho\frac{K_j+1}{2}\right)\right]=\frac{1}{2}\sum_j a_j. \end{aligned} \tag{E21}$$

If the infidelity is at least ϵ, then $(\sum_j a_j)/2 \geq \epsilon$. We need to determine the minimum of $\sum_j N_j$ under the requirement that Eq. (E20) holds whenever $(\sum_j a_j)/2 \geq \epsilon$. Choose

$$a_j = \frac{2\epsilon\times 2^{r_j}}{\sum_k 2^{r_k}}, \tag{E22}$$

then Eq. (E20) implies that

$$\exp\left(-\frac{2\epsilon^2\sum_j N_j}{\left(\sum_j 2^{r_j}\right)^2}\right) \leq \delta, \tag{E23}$$

which in turn implies that

$$N_{\mathrm{MTH}} = \sum_j N_j \geq \frac{\left(\sum_j 2^{r_j}\right)^2 \ln\delta^{-1}}{2\epsilon^2}. \tag{E24}$$

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

$$N_{\mathrm{MTH}} \geq \frac{4^r n^2\ln\delta^{-1}}{2\epsilon^2} \tag{E25}$$

tests. The bounds in the above two equations have much better scaling behavior with n compared with the bound in Eq. (E16). 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. (E24) and (E25). 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. (E24) is based on Eqs. (E15) and (E21). Note that the bound in (E21) is tight. The Hoeffding inequality in Eq. (E15) may potentially be improved, thereby reducing N_{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 nonadversarial 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,

$$N_{\mathrm{MTH}} \geq \frac{2^{(n-1)(n-2)}n^2\ln\delta^{-1}}{2\epsilon^2}. \tag{E26}$$

Here 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 at most n potential measurement settings and $\lceil (n/\epsilon)\ln(1/\delta)\rceil$ tests according to Eq. (13).

The rest examples considered below are 3-colorable, so our cover protocol requires three measurement settings and $\lceil (3/\epsilon)\ln(1/\delta)\rceil$ tests to verify each hypergraph state within infidelity ϵ and significance level δ. First, consider the tensor power $|\Psi_{f_3}\rangle^{\otimes n/3}$ introduced in Appendix E 2, assuming n is divisible by 3. In this case $r_j=r=1$ for all $j=1,2,\ldots,n$. Therefore, Eq. (E25) reduces to

$$N_{\mathrm{MTH}} \geq \frac{2n^2\ln\delta^{-1}}{\epsilon^2}. \tag{E27}$$

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

$$r_j = \begin{cases} 1 & n=3 \text{ or } j=1 \text{ or } j=n,\\ 2 & n\geq 4, j=2 \text{ or } j=n-1,\\ 3 & j\neq 1,2,n-1,n. \end{cases} \tag{E28}$$

Therefore,

$$\sum_j 2^{r_j} = \begin{cases} 6 & n=3, \\ 8n-20 & n\geq 4, \end{cases} \tag{E29}$$

which implies that

$$N_{\mathrm{MTH}} \geq \begin{cases} \frac{18\ln\delta^{-1}}{\epsilon^2} & n=3, \\ \frac{8(2n-5)^2\ln\delta^{-1}}{\epsilon^2} & n\geq 4. \end{cases} \tag{E30}$$

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,

$$\sum_j 2^{r_j} = 16n - 48, \quad N_{\mathrm{MTH}} \geq \frac{128(n-3)^2\ln\delta^{-1}}{\epsilon^2}. \tag{E31}$$

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

$$\begin{aligned}\sum_j 2^{r_j} &= 2^8(\tilde{n}-1)^2 + 2^4[\tilde{n}^2 + 4(\tilde{n}-1)] + 2^2\times 4 \\ &= 16(17\tilde{n}^2 - 28\tilde{n} + 13),\end{aligned} \tag{E32}$$

so that

$$N_{\mathrm{MTH}} \geq \frac{128(17\tilde{n}^2 - 28\tilde{n}+13)^2\ln\delta^{-1}}{\epsilon^2}. \tag{E33}$$

4. Comparison with Ref. [30]

Here, in the adversarial setting, we compare our method with the method proposed by Hayashi and Hajdušek (HH) [30], 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. [30] 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 trusty.

Suppose $|G\rangle$ is a graph state associated with the graph G. When G is m-colorable, HH (Appendix F of Ref. [30]) proposed the following verification protocol, which consists of m stabilizer tests. Given a coloring $\mathscr{A} = \{A_1, A_2, \dots, A_m\}$ 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 lth group for $l = 1, 2, \dots, m$ are subjected to the stabilizer test with P_l [cf. Eq. (7) in the main text] as the projector onto the pass eigenspace. Let σ be the reduced state of the remaining system after all these tests are passed. If the lth test P_l is passed with significance level δ', then one can guarantee that $\mathrm{tr}[\sigma(1-P_l)] \leq \frac{1}{\delta'(N'+1)}$. If all the tests $P_1, \dots, P_m$ are passed, with significance level $\delta := m\delta'$, then one can guarantee that

$$\begin{aligned}\epsilon = \mathrm{tr}[\sigma(1-|G\rangle\langle G|)] &\leq \sum_{l=1}^{m}\mathrm{tr}[\sigma(1-P_l)] \\ &\leq \sum_{l=1}^{m}\frac{1}{\delta'(N'+1)} = \frac{m^2}{\delta(N/m+1)} \cong \frac{m^3}{\delta N}.\end{aligned} \tag{E34}$$

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

Now, we explain how our method outperforms the HH method. If we employ the cover protocol and randomly choose the lth measurement setting with probability $1/m$, then $\nu(\Omega) = 1/m$ according to Theorem 1. If the tests are passed with significance level δ, then Theorem 5 in Ref. [35] guarantees that

$$\epsilon = \mathrm{tr}[\sigma(1-|G\rangle\langle G|)] \leq \frac{m(1-\delta)}{N\delta}. \tag{E35}$$

To verify $|G\rangle$ within infidelity ϵ and significance level δ in the adversarial scenario, the cover protocol requires only $\lceil m(1-\delta)/(\delta\epsilon)\rceil$ tests according to Eq. (C1), which significantly outperforms the HH protocol. Thanks to Eq. (C6), the hedged cover or coloring protocol can further reduce the number of tests to

$$\begin{aligned}N = \left\lfloor\frac{h_*(1/m)\ln(F\delta)^{-1}}{\epsilon}\right\rfloor &\leq \frac{(m+\mathrm{e}-1)\ln(F\delta)^{-1}}{\epsilon} \\ &\approx \frac{(m+\mathrm{e}-1)\ln\delta^{-1}}{\epsilon},\end{aligned} \tag{E36}$$

where $F = 1-\epsilon$. When $m=3$ and $\epsilon = \delta = 0.01$ for example, the protocol of Ref. [30] requires 270000 tests, while the hedged cover protocol requires only 1870 tests, which is smaller by 144 times.

5. Comparison with Ref. [34]

Very recently, Takeuchi and Morimae (TM) [34] introduced a protocol for verifying general hypergraph states whose orders are upper bounded by a constant. Recall that the order of a hypergraph $G = (V, E)$ is the maximum cardinality of hyperedges in the edge set E.

Let $G = (V, E)$ be a hypergraph such that $2 \leq |e| \leq c$ for all $e \in E$, where c is a positive constant. Let $k \geq (4n)^7$ and $m \geq 2n^3k^{18/7}\ln 2$ be positive integers. According to Theorem 5 in Ref. [34], to verify the hypergraph state $|G\rangle$ within infidelity $\epsilon = k^{-1/7}$ and significance level $\delta = k^{-1/7}$, the number of tests required by the TM protocol is given by

$$N_{\mathrm{TM}} = m + nk \geq 2n^3k^{18/7}\ln 2 + nk > 2n^3k^{18/7}\ln 2. \tag{E37}$$

For example, when $k=(4n)^7$, $\epsilon=\delta=k^{-1/7}=1/(4n)$, the number of tests satisfies

$$\begin{aligned}N_{\mathrm{TM}} &\geq 2n^3(4n)^{18}\ln 2+n(4n)^7=2^{37}n^{21}\ln 2+2^{14}n^8\\ &> 2^{37}n^{21}\ln 2>9.5\times 10^{10}n^{21}.\end{aligned} \tag{E38}$$

Although this number is still polynomial in n, it is already astronomical in the simplest nontrivial scenario with $n=3$. So it is too prohibitive to apply the TM protocol in any scenario of practical interest. By contrast, the number of tests required by our coloring protocol satisfies

$$N\leq (16n^2-4n)\chi(G)<16n^2\chi(G)\leq 16n^3 \tag{E39}$$

according to Eq. (C2) in the main text, which is dramatically smaller than N_{TM}. The hedged coloring protocol can further reduce the number of tests according to Eq. (C8).

Our protocols are not only much more efficient than the TM protocol, but also much simpler to apply. In particular, the TM protocol relies on adaptive stabilizer tests, while our protocols do not rely on any adaption. In addition, the data processing in the TM protocol is a bit involved, while it is very simple in our protocols. Furthermore, TM did not derive the explicit number of required tests except for restricted choices of the infidelity ϵ and significance level δ, which makes it difficult to apply their result in many scenarios of practical interest. By contrast, we derive an explicit number of tests required for all valid choices of ϵ and δ.

6. Comparison with Ref. [31]

For stabilizer states, which are equivalent to graph states under LC [38, 39], several methods are available in the literature [31, 33]. The protocol introduced by Pallister, Linden, and Montanaro (PLM) [31] is particularly efficient in terms of the total number of tests. To be specific, the PLM protocol measures all 2^n-1 nontrivial stabilizer operators of $|G\rangle$ in the Pauli group with equal probability. The resulting verification operator reads

$$\Omega_{\mathrm{PLM}}=|G\rangle\langle G|+\frac{2^{n-1}-1}{2^n-1}(1-|G\rangle\langle G|), \tag{E40}$$

which is homogeneous with

$$\beta(\Omega_{\mathrm{PLM}})=\frac{2^{n-1}-1}{2^n-1},\quad \nu(\Omega_{\mathrm{PLM}})=\frac{2^{n-1}}{2^n-1}. \tag{E41}$$

To verify $|G\rangle$ within infidelity ϵ and significance level δ, this protocol requires about

$$\lceil 2^{1-n}(2^n-1)\epsilon^{-1}\ln\delta^{-1}\rceil\leq\lceil 2\epsilon^{-1}\ln\delta^{-1}\rceil \tag{E42}$$

tests, which is smaller than the number $\lceil\chi(G)\epsilon^{-1}\ln\delta^{-1}\rceil$ required by our coloring protocol [cf. Eq. (13)]. However, the number of potential measurement settings of the 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 coloring protocol requires at most n potential measurement settings. 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 is comparable to the PLM protocol. Furthermore, the PLM protocol requires $Y=\mathrm{i}XZ$ measurement because it is necessary to measure all nontrivial stabilizer operators of $|G\rangle$, while our protocol requires only X and Z measurements.

Incidentally, Ref. [31] introduced another protocol for verifying the graph state $|G\rangle$ by measuring n stabilizer generators of $|G\rangle$ with equal probability. The resulting verification operator Ω can achieve $\nu(\Omega)=1/n$. This protocol requires $\lceil n\epsilon^{-1}\ln\delta^{-1}\rceil$ tests in total, which corresponds to the performance of our coloring protocol in the worst case in which the graph is complete (contains all possible edges). In general, the coloring protocol requires much fewer measurement settings and tests in total.

7. Comparison with Ref. [37]

Recently, Takeuchi, Mantri, Morimae, Mizutani, and Fitzsimons [37] introduced a protocol for verifying graph states with a very small significance level. Given a graph state $|G\rangle$ of n qubits, suppose one can perform $N_{\mathrm{TMMMF}}=2n\lceil(5n^4\ln n)/32\rceil$ tests, then the protocol given in Ref. [37] guarantees that the resultant state σ satisfies

$$\langle G|\sigma|G\rangle\geq 1-\frac{2\sqrt{c}+1}{n} \tag{E43}$$

if these tests are passed with significance level $n^{1-5c/64}$. Here, c is a constant that satisfies $\frac{64}{5}<c<\frac{(n-1)^2}{4}$.

Next, we analyze the performance of the hedged cover or coloring protocol proposed in the main text (see also Sec. C). According to Eq. (E36), suppose the graph G is m colorable, then the number of required tests is given by

$$\begin{aligned}N&=\left\lfloor\frac{h_*(1/m)\ln(F\delta)^{-1}}{\epsilon}\right\rfloor\leq\frac{(m+\mathrm{e}-1)\ln(F\delta)^{-1}}{\epsilon},\\ &\approx\frac{(m+\mathrm{e}-1)(\frac{5c}{64}-1)n\ln n}{(2\sqrt{c}+1)}=O(n^2\ln n),\end{aligned} \tag{E44}$$

where $F=1-\epsilon$ and the approximation holds as long as $\epsilon,\delta\ll 1$. For most graph states of practical interest, m is upper bounded by a small constant, so $N=O(n\ln n)$. The number of tests is much smaller than N_{TMMMF}. Therefore, our approach is much more efficient that the approach of Ref. [37].