Optimal Verification of Greenberger-Horne-Zeilinger States

Zihao Li\textsuperscript{1,2}, Yun-Guang Han\textsuperscript{1,2} and Huangjun Zhu\textsuperscript{1,2,3,4}
\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
E-mail: zhuhuangjun@fudan.edu.cn

Abstract. We construct optimal protocols for verifying both qubit and qudit GHZ states using local projective measurements. When the local dimension is a prime, an optimal protocol is constructed from Pauli measurements only. Our protocols provide a highly efficient way for estimating the fidelity and certifying genuine multipartite entanglement. In particular, they enable the certification of genuine multipartite entanglement using only one test when the local dimension is sufficiently large. By virtue of adaptive local projective measurements, we then construct protocols for verifying GHZ-like states that are optimal over all protocols based on one-way communication. The efficiency can be improved further if additional communications are allowed. Finally, we construct optimal protocols for verifying GHZ states and nearly optimal protocols for GHZ-like states in the adversarial scenario.

Keywords: quantum state verification, local projective measurement, GHZ state, GHZ-like state, genuine multipartite entanglement, entanglement certification, adversarial scenario
1. Introduction

Greenberger-Horne-Zeilinger (GHZ) states \cite{1, 2} are typical examples of quantum states with genuine multipartite entanglement (GME) \cite{3}. They play key roles both in quantum information processing and in foundational studies, such as quantum secret sharing \cite{4, 5}, open-destination teleportation \cite{6}, quantum networks \cite{7}, and multipartite nonlocality tests \cite{8, 9}. The significance of GHZ states are witnessed by numerous experiments devoted to preparing them in various platforms, with ever increasing number of particles \cite{9, 10, 11, 12, 13, 14, 15}. In practice, multipartite quantum states prepared in experiments are never perfect. So it is crucial to verify these states with high precision using limited resources. However, traditional tomographic approaches are known to be resource consuming and very inefficient \cite{14, 15, 16}.

Recently, an alternative approach known as quantum state verification has attracted increasing attention \cite{17, 18, 19}. Efficient verification protocols based on local operations and classical communication (LOCC) have been constructed for stabilizer states \cite{18, 19}, hypergraph states \cite{19}, and Dicke states \cite{20}. However, optimal protocols are known only for maximally entangled states \cite{17, 21, 22} and bipartite pure states under restricted LOCC \cite{18, 23, 24, 25}. For quantum states with GME, such as GHZ states, no optimal protocol has been found so far because such optimization problems are usually extremely difficult. Any progress in this direction is of interest to both theoretical studies and practical applications.

In this paper, we construct optimal verification protocols for (qubit and qudit) GHZ states with local projective measurements. When the local dimension is a prime, only Pauli measurements are required. Our protocols offer a highly efficient tool for fidelity estimation and entanglement certification. Surprisingly, the GME can be certified with any given significance level using only one test when the local dimension is sufficiently large, which has never been achieved or even anticipated before. By virtue of adaptive local projective measurements, our protocols can be generalized to GHZ-like states, while retaining the high efficiency. Moreover, our protocols can be applied to the adversarial scenario with minor modification. In this case, our protocols for verifying GHZ states based on local projective measurements are actually optimal among all possible protocols without locality restriction.

2. Pure state verification

Before proposing protocols for verifying GHZ states, let us take a brief review on the general framework of pure state verification \cite{18, 26, 27}. Consider a quantum device that is supposed to produce the target state $|\Psi\rangle\langle\Psi|$, but actually produces the states $\sigma_1, \sigma_2, \ldots, \sigma_N$ in $N$ runs. Our task is to verify whether these states are sufficiently close to the target state on average. To achieve this task, we can perform two-outcome projective measurements $\{P_1, 1 - P_1\}$ from a set of accessible measurements. Each measurement represents a test, and the outcome $P_1$ corresponds to passing the test.
Here we require that the target state $|\Psi\rangle$ can always pass the test, that is, $P_l|\Psi\rangle = |\Psi\rangle$.

Suppose the test $\{P_l, 1 - P_l\}$ is performed with probability $p_l$, then the verification operator (also called a strategy) is given by $\Omega = \sum_l p_l P_l$. If $\langle \Psi | \sigma_j | \Psi \rangle \leq 1 - \varepsilon$, then the maximum probability that $\sigma_j$ can pass the test reads \[ \max_{\langle \Psi | \sigma | \Psi \rangle \leq 1 - \varepsilon} \text{tr}(\Omega \sigma) = 1 - [1 - \beta(\Omega)]\varepsilon = 1 - \nu(\Omega)\varepsilon. \] (1)

Here $\beta(\Omega)$ denotes the second largest eigenvalue of $\Omega$, and $\nu(\Omega) := 1 - \beta(\Omega)$ is the spectral gap from the maximal eigenvalue. Suppose the states $\sigma_1, \sigma_2, \ldots, \sigma_N$ are independent of each other and let $\varepsilon_j = 1 - \langle \Psi | \sigma_j | \Psi \rangle$. Then these states can pass all $N$ tests with probability at most $\prod_j [1 - \nu(\Omega)\varepsilon_j] \leq [1 - \nu(\Omega)\bar{\varepsilon}]^N$, where $\bar{\varepsilon} = \sum_j \varepsilon_j / N$ is the average infidelity. In order to insure the condition $\sum_j \langle \Psi | \sigma_j | \Psi \rangle / N > 1 - \varepsilon$ with significance level $\delta$, it suffices to choose \[ N = \left\lceil \frac{\ln \delta}{\ln [1 - \nu(\Omega)\varepsilon]} \right\rceil \approx \frac{\ln \delta^{-1}}{\nu(\Omega)\varepsilon}. \] (2)

To minimize the number of tests, we need to maximize the value of the spectral gap $\nu(\Omega)$ under LOCC. However, this task is usually extremely difficult if not impossible.

### 3. Verification of GHZ states

Here we are mainly interested in GHZ states \[ |\text{GHZ}_d^n\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle^\otimes n. \] (3)

Previously, a coloring protocol was proposed in Ref. \[19\] which can achieve a spectral gap of $1/2$ using Pauli measurements. For a bipartite maximally entangled state of the same local dimension, the maximal value of the spectral gap of any verification operator based on LOCC (or separable measurements) is $d/(d + 1)$ \[17, 18, 21, 22\]. Obviously, the counterpart for GHZ states cannot be larger. Here we show that this upper bound can always be saturated.

#### 3.1. Optimal verification of the $n$-qubit GHZ state

First, we construct an optimal protocol for verifying the $n$-qubit GHZ state ($d = 2$) based on Pauli measurements. Recall that the Pauli group for each qubit is generated by three Pauli matrices, \[ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \] (4)

Our verification protocol consists of $1 + 2^{n-1}$ distinct tests. In the first test, called the standard test, all parties perform $Z$ measurements, and the test is passed if all the
outcomes coincide; the test projector reads

\[ P_0 = (|0\rangle\langle 0|)^\otimes n + (|1\rangle\langle 1|)^\otimes n. \]  (5)

For each of the rest tests, all parties perform either \(X\) or \(Y\) measurements, and the number of parties that perform \(Y\) measurements is even. Let \(\mathcal{I} \subset \{1, 2, \ldots, n\}\) denote the set of parties that perform \(Y\) measurements with \(|\mathcal{I}| = 2t\), and \(\mathcal{J}\) the complement of \(\mathcal{I}\). Then the test is passed if the total number of outcome \(-1\) (either from \(X\) or \(Y\) measurements) has the same parity as \(t\). The corresponding test projector reads

\[ P_\mathcal{I} = \frac{1}{2} \left[ 1 + (-1)^t \prod_{k \in \mathcal{I}} Y_k \prod_{k' \in \mathcal{J}} X_{k'} \right]. \]  (6)

We perform the test \(P_0\) with probability \(1/3\) and other \(2^{n-1}\) tests with probability \(1/(3 \times 2^{n-2})\) each. The resulting verification operator reads

\[ \Omega_I := \frac{1}{3} \left( P_0 + \frac{1}{2^{n-2}} \sum_{\mathcal{I}} P_\mathcal{I} \right) = \frac{1}{3} (1 + 2 |\text{GHZ}_n^2\rangle\langle \text{GHZ}_n^2|). \]  (7)

The second equality is proved in Appendix A. We have \(\beta(\Omega_I) = 1/3\), and

\[ \nu(\Omega_I) = \frac{2}{3}, \quad N(\Omega_I) \approx \frac{3}{2\varepsilon} \ln \delta^{-1}. \]  (8)

This protocol is optimal among all protocols based on LOCC or separable measurements. Compared with the protocol in Ref. [18] which achieves \(\nu = 2^{n-1}/(2^n - 1)\) with \(2^n - 1\) measurement settings, our protocol not only has a higher efficiency, but also requires fewer measurement settings.

Moreover, our protocol proposed above is essentially the unique optimal protocol based on Pauli measurements as shown in Proposition 1 below and proved in Appendix B. In particular, the number \(1 + 2^{n-1}\) of (potential) measurement settings cannot be reduced. It should be pointed out that there is some freedom in choosing the Pauli group: different choices are related to each other by local unitary transformations. Here we focus on the canonical Pauli group generated by Pauli matrices in Eq. (4) for each qubit; only nonadaptive Pauli measurements associated with this Pauli group are considered. Nevertheless, the test operators are not required to be projectors, although it turns out that this relaxation does not provide any advantage.

\textbf{Proposition 1.} Suppose \(\Omega\) is a verification strategy for \(|\text{GHZ}_n^2\rangle\rangle\) that is based on Pauli measurements. If \(\nu(\Omega) = 2/3\), then \(\Omega = \Omega_I\). In addition, the strategy consists of \(1 + 2^{n-1}\) projective tests: one of them is the standard test \(P_0\) performed with probability \(1/3\), and each of the other tests has the form \(P_\mathcal{I}\) in Eq. (6) with even \(|\mathcal{I}|\) and is performed with probability \(1/(3 \times 2^{n-2})\).
3.2. Optimal verification of the \( n \)-qudit GHZ state

Next, we generalize the above results to the qudit case, assuming that the local dimension \( d \) is an odd prime. The qudit Pauli group is generated by the phase operator \( Z \) and the shift operator \( X \) defined as follows,

\[
Z|j\rangle = \omega^j|j\rangle, \quad X|j\rangle = |j + 1\rangle, \quad \omega = e^{2\pi i/d}, \tag{9}
\]

where \( j \in \mathbb{Z}_d \) and \( \mathbb{Z}_d \) is the ring of integers modulo \( d \). Our verification protocol is composed of \( 1 + d^{n-1} \) distinct tests based on Pauli measurements. The first test is still the standard test, in which all parties perform \( Z \) measurements, and the test is passed if all the outcomes coincide; the test projector reads

\[
P_0 = \sum_{j=0}^{d-1} (|j\rangle\langle j|)^\otimes n. \tag{10}
\]

For each of the rest tests, party \( k \) \((k = 1, 2, \ldots, n)\) performs \( XZ^{r_k} \) measurement, where \( r_k \in \mathbb{Z}_d \) satisfy the condition \( \sum_k r_k = 0 \) mod \( d \). Denote the outcome of party \( k \) by an integer \( o_k \in \mathbb{Z}_d \) corresponding to the eigenvalue \( \omega^{o_k} \) of \( XZ^{r_k} \). The test is passed if \( \sum_k o_k = 0 \) mod \( d \), so that \( \prod_{k=1}^n X_k Z_k^{r_k} \) has eigenvalue 1. The test projector reads

\[
P_r = \frac{1}{d} \sum_{l=0}^{d-1} \left( \prod_{k=1}^n X_k Z_k^{r_k} \right)^l. \tag{11}
\]

We perform the test \( P_0 \) with probability \( 1/(d + 1) \) and other \( d^{n-1} \) tests with probability \( 1/[(d + 1)d^{n-2}] \) each. The verification operator reads

\[
\Omega_{II} := \frac{1}{d + 1} \left( P_0 + \frac{1}{d^{n-2}} \sum_r P_r \right) = \frac{1 + d|\text{GHZ}_n^d\rangle\langle\text{GHZ}_n^d|}{d + 1}. \tag{12}
\]

The second equality is proved in Appendix A. We have \( \beta(\Omega_{II}) = 1/(d + 1) \), and

\[
\nu(\Omega_{II}) = \frac{d}{d + 1}, \quad N(\Omega_{II}) \approx \frac{d + 1}{d \varepsilon} \ln \delta^{-1}. \tag{13}
\]

Similar to the qubit case, this protocol is optimal among all protocols based on separable measurements. In addition, it is essentially the unique optimal protocol based on Pauli measurements; the number \( 1 + d^{n-1} \) of measurement settings is the smallest possible. Proposition 2 below generalizes Proposition 1 to the qudit case. Its proof is a simple analog of the counterpart for the qubit case and is thus omitted. As in the qubit case, there is some freedom in choosing the Pauli group, and here we focus on the canonical Pauli group generated by operators \( Z \) and \( X \) defined in Eq. (9) for each qudit.

**Proposition 2.** Suppose \( \Omega \) is a verification strategy for \( |\text{GHZ}_n^d\rangle \) that is based on Pauli measurements, where \( d \) is an odd prime. If \( \nu(\Omega) = d/(d + 1) \), then \( \Omega = \Omega_{II} \). In addition, the strategy consists of \( 1 + d^{n-1} \) projective tests: one of them is the standard test \( P_0 \) and is performed with probability \( 1/(d + 1) \), while each of the other tests has the form \( P_r \) in Eq. (11) with \( \sum_{k=1}^n r_k = 0 \) mod \( d \), and is performed with probability \( 1/[(d + 1)d^{n-2}] \).
3.3. Alternative protocols based on 2-designs

When the dimension $d$ is not necessarily a prime, we can still devise optimal protocols for GHZ states by virtue of (weighted complex projective) 2-designs [28, 29, 30]. Let $\{\mathcal{B}_h\}_{h=0}^m$ be $m+1$ bases on the Hilbert space of dimension $d$, where $\mathcal{B}_0$ is the standard basis, and each basis $\mathcal{B}_h$ for $h = 1, 2, \ldots, m$ is composed of $d$ kets of the form

$$\left|\psi_{ht}\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i \theta_{htj}} |j\rangle,$$

where $\theta_{htj} = 2\pi \left[\frac{tj}{d} + \frac{h(j)}{m}\right]$ (14)

for $t = 0, 1, \ldots, d-1$. Let $w_0 = 1/(d+1)$ and $w_h = d/[m(d+1)]$ for $h = 1, 2, \ldots, m$, and let $\{\mathcal{B}_h, w_h\}_{h=0}^m$ be a weighted set of kets with weight $w_h$ for all kets in basis $h$. When $d \geq 3$ and $m \geq \lceil \frac{3}{4}(d-1) \rceil$, the set $\{\mathcal{B}_h, w_h\}_{h=0}^m$ forms a 2-design according to Ref. [30]. Define

$$W := \text{diag} (\mu^0, \mu^1, \ldots, \mu^{d-2}, \mu^{-(d-1)(d-2)/2})$$

with $\mu = e^{2\pi i/m}$ being a primitive $m$th root of unity. Then $\left|\psi_{ht}\right\rangle$ is an eigenstate of $XW^h$ with eigenvalue $\omega^{-t}$, that is,

$$XW^h = \sum_t \omega^{-t} |\psi_{ht}\rangle\langle\psi_{ht}|.$$ (16)

By virtue of the 2-design $\{\mathcal{B}_h, w_h\}_{h=0}^m$ we can construct an optimal protocol using $1 + m^{n-1}$ distinct tests. The first test is still the standard test $P_0$ as given in Eq. (10). For each of the rest tests, party $k$ ($k = 1, \ldots, n$) performs the projective measurement on the basis $\mathcal{B}_{hk}$, where $h_k \in \{1, \ldots, m\}$ and $\sum_k h_k = 0 \mod m$. The outcome of party $k$ is denoted by $o_k$, which corresponds to the ket $\left|\psi_{h_ka_k}\right\rangle$ and the eigenvalue $\omega^{-o_k}$ of $XW^h$. The test is passed if $\sum_k o_k = 0 \mod d$, and the test projector reads

$$P_h = \frac{1}{d} \sum_{t=0}^{d-1} \left( \prod_{k=1}^n X_k W_{hk}^t \right).$$

Note that the target state $\left|\text{GHZ}_n^d\right\rangle$ is stabilized by $\prod_{k=1}^n X_k W_k^{h_k}$ given the assumption $\sum h_k = 0 \mod m$ and so can pass the test with certainty as desired.

We perform the test $P_0$ with probability $1/(d+1)$ and other $m^{n-1}$ tests with probability $d/[(d+1)m^{n-1}]$ each. The verification operator reads

$$\Omega_{\text{III}} := \frac{1}{d+1} \left( P_0 + \frac{d}{m^{n-1}} \sum_h P_h \right) = \frac{1 + d|\text{GHZ}_n^d\rangle\langle\text{GHZ}_n^d|}{d+1}. $$ (18)

The second equality is proved in Appendix A. So this protocol is optimal among all protocols based on separable measurements. Compared with the protocol based on Pauli measurements, this protocol applies to GHZ states of any local dimension, although it requires more measurement settings.
3.4. Efficient certification of GME

A quantum state $\rho$ is genuine multipartite entangled (GME) if its fidelity with the GHZ state $\text{tr}(\rho|\text{GHZ}_n^d\rangle\langle\text{GHZ}_n^d|)$ is larger than $1/d$ [3]. To certify the GME of the qudit GHZ state with significance level $\delta$ using a given verification strategy $\Omega$, the number of tests is determined by Eq. (2) with $\varepsilon = (d - 1)/d$. If, in addition, $\Omega$ is the optimal local strategy with $\nu(\Omega) = d/(d + 1)$, then this number reads

$$N_E = \left\lceil \ln \frac{\delta}{\ln 2 - \ln(d + 1)} \right\rceil.$$  \hspace{1cm} (19)

We have $N_E = 1$ when $d \geq 2\delta^{-1} - 1$, so the GME of the GHZ state can be certified with any given significance level using only one test when the local dimension is sufficiently large, as illustrated in Fig. 1. Although single-copy entanglement detection is known before [22, 31], single-copy detection of GME is still quite surprising, because it is much more difficult to demonstrate GME than just entanglement.

4. Verification of GHZ-like states

4.1. Verification of GHZ-like states with adaptive measurements

Next, consider GHZ-like states

$$|\xi\rangle = \sum_{j=0}^{d-1} \lambda_j |j\rangle^{\otimes n},$$  \hspace{1cm} (20)

where the coefficients $\lambda_j$ have decreasing order $1 \geq \lambda_0 \geq \lambda_1 \geq \cdots \lambda_{d-1} \geq 0$ and satisfy $\sum_{j=0}^{d-1} \lambda_j^2 = 1$. We first show that these states can be verified efficiently using only two
distinct tests constructed from mutually unbiased based (MUB). Recall that two bases \( \{ |\psi_i \rangle \}_{i=0}^{d-1} \) and \( \{ |\varphi_j \rangle \}_{j=0}^{d-1} \) for a Hilbert space of dimension \( d \) are mutually unbiased if they satisfy \( |\langle \psi_i | \varphi_j \rangle |^2 = 1/d \) for all \( i, j \). Let \( \mathcal{B}_0 \) be the standard basis and \( \mathcal{B} = \{ |u_g \rangle \}_{g=0}^{d-1} \) be any basis that is unbiased with \( \mathcal{B}_0 \). A simple example of \( \mathcal{B} \) is the Fourier basis \( \{ \sum_{j=0}^{d-1} \omega^{gj} |j \rangle / \sqrt{d} \}_{g=0}^{d-1} \) with \( \omega = e^{2\pi i/d} \), which happens to be the eigenbasis of the shift operator \( X \) in Eq. (9). The following discussion is independent of the choice of the basis \( \mathcal{B} \) as long as it is unbiased with respect to the standard basis \( \mathcal{B}_0 \).

The first test is the standard test \( P_0 \) in Eq. (10). For the second test, the first \( n-1 \) parties perform projective measurements on the basis \( \mathcal{B} \). If they obtain the outcome \( g = \{ g_1, g_2, \ldots, g_{n-1} \} \), then the normalized reduced state of party \( n \) reads

\[
d^{\frac{n-1}{2}} \left( \bigotimes_{k=1}^{n-1} |u_{g_k} \rangle \right) |\xi \rangle = M |v_g \rangle,
\]

where \( M := \sqrt{d} \text{diag}(\lambda_0, \ldots, \lambda_{d-1}) \) and \( |v_g \rangle := d^{\frac{n-1}{2}} \left( \bigotimes_{k=1}^{n-1} |u_{g_k} \rangle \right) |\text{GHZ}_d \rangle \). It is worth pointing out that \( |v_g \rangle \) has a constant overlap of \( 1/d \) with each element in the basis \( \mathcal{B}_0 \). Then party \( n \) performs the projective measurement \( \{ M |v_g \rangle \langle v_g | \}, \mathbb{1}_1 - M |v_g \rangle \langle v_g | M \} \), where \( \mathbb{1}_1 \) is the identity operator on the Hilbert space of one qudit. The test is passed if party \( n \) obtains the first outcome (corresponding to \( M |v_g \rangle \langle v_g | M \)). The resulting test projector reads

\[
P_1 = \sum_g \left( \prod_{k=1}^{n-1} |u_{g_k} \rangle \langle u_{g_k} | \right) \otimes \left( M |v_g \rangle \langle v_g | M \right).
\]

So we have

\[
\text{tr}(P_0P_1) = \frac{1}{d^{n-1}} \sum_g \sum_{j=0}^{d-1} |\langle j | M |v_g \rangle |^2 = \frac{1}{d^{n-1}} \sum_g \sum_{j=0}^{d-1} \lambda_j^2 = 1,
\]

which implies that the two projectors \( \tilde{P}_0 := P_0 - |\xi \rangle \langle \xi | \) and \( \tilde{P}_1 := P_1 - |\xi \rangle \langle \xi | \) have orthogonal supports.

If we perform the two tests \( P_0 \) and \( P_1 \) with probability \( p \) and \( 1-p \), respectively, then the verification operator reads \( \Omega_{IV} = pP_0 + (1-p)P_1 \), with

\[
\beta(\Omega_{IV}) = \| \tilde{\Omega}_{IV} \| = \max\{p, 1-p\} \geq \frac{1}{2},
\]

where \( \Omega_{IV} = \Omega_{IV} - |\xi \rangle \langle \xi | \). The lower bound is saturated iff \( p = 1/2 \), in which case we have \( \Omega_{IV} = (P_0 + P_1)/2 \). The corresponding spectral gap \( \nu(\Omega_{IV}) \) and the number \( N(\Omega_{IV}) \) of required tests read

\[
\nu(\Omega_{IV}) = \frac{1}{2}, \quad N(\Omega_{IV}) \approx \frac{2}{\varepsilon} \ln \delta^{-1}.
\]

According to Ref. [22], here the spectral gap attains the maximum among all protocols composed of two local projective tests, so the above protocol is the most efficient among all protocols based on two local projective tests.
4.2. Optimal verification of GHZ-like states with one-way LOCC

For a bipartite state $|\zeta\rangle = \sum_{j=0}^{d-1} \lambda_j |jj\rangle$ with the same local dimension and coefficients $\lambda_j$ as $|\xi\rangle$ in Eq. (20), the maximal value of the spectral gap of any verification operator based on one-way LOCC is $1/(1+\lambda_0^2)$ \cite{24,25}. The counterpart for a GHZ-like state cannot be larger. Here we shall demonstrate that this upper bound can be saturated. When $d \geq 3$, our protocol consists of $1 + m^{n-1}$ distinct tests with $m \geq \lceil \frac{3}{4}(d - 1)^2 \rceil$. The first test is the standard test in Eq. (10). For each of the rest tests, the first test is still the standard test $P_0$, where $P_0 := 1^n \otimes (|\zeta\rangle \langle \zeta|)$. The test projector reads

$$P_h' = (1^n \otimes M) P_h (1^n \otimes M),$$

where $P_h$ is the test projector in Eq. (17).

Suppose we perform the test $P_0$ with probability $p$, and each of the other tests with probability $(1 - p)/m^{n-1}$, then the verification operator reads

$$\Omega_V = p P_0 + (1 - p) \Pi,$$

where

$$\Pi := \frac{1}{m^{n-1}} \sum_h P_h' = |\xi\rangle \langle \xi| + 1^n \otimes (|\zeta\rangle \langle \zeta|) \otimes \rho_n - \sum_{j=0}^{d-1} \lambda_j^2 |jj\rangle \langle jj|^{\otimes n},$$

with $\rho_n := \text{tr}_{1,2,\ldots,n-1} (|\zeta\rangle \langle \zeta|)$ being the reduced state for party $n$. Here the second equality follows from Eqs. (18) and (26). Note that $\Pi = \Pi - |\zeta\rangle \langle \zeta|$ and $P_0 = P_0 - |\zeta\rangle \langle \zeta|$ are orthogonal, we conclude that

$$\beta(\Omega_V) = \|\Omega_V\| = \max\{p, (1 - p)\lambda_0^2\} \geq \frac{\lambda_0^2}{1 + \lambda_0^2}.$$  

(29)

The bound is saturated iff $p = \lambda_0^2/(1 + \lambda_0^2)$, which yields

$$\nu(\Omega_V) = \frac{1}{1 + \lambda_0^2}, \quad N(\Omega_V) \approx \frac{1 + \lambda_0^2}{\varepsilon} \ln \delta^{-1}.$$  

(30)

Therefore, this protocol is optimal among all protocols based on one-way LOCC.

When the dimension $d$ is a prime, the number of distinct tests required for constructing the optimal protocol can be reduced to $1 + d^{n-1}$. Take the qubit case for example. The first test is still the standard test $P_0$. For each of the rest tests, the first $n - 1$ parties perform either $X$ or $Y$ measurements. Then party $n$ performs the projective measurement $\{|v\rangle \langle v|, 1 - |v\rangle \langle v|\}$, where $|v\rangle$ is the normalized reduced state of party $n$ depending on the outcomes of the first $n - 1$ parties. The test is passed if
party $n$ obtains the first outcome (corresponding to $|v\rangle\langle v|$). The test projector has the form

$$P'_{\mathcal{Y}} = (I_1^{\otimes (n-1)} \otimes M) P_{\mathcal{Y}} (I_1^{\otimes (n-1)} \otimes M)$$

(31)

with even $|\mathcal{Y}|$, where $P_{\mathcal{Y}}$ is the test projector in Eq. (6). Then the verification operator reads

$$\Omega'_{V} = p P_{0} + \frac{1-p}{2^{n-1}} \sum_{\mathcal{Y}} P'_{\mathcal{Y}}.$$  

(32)

Again, the maximal spectral gap $\nu(\Omega'_{V}) = 1/(1 + \lambda_0^2)$ can be attained by choosing $p = \lambda_0^2/(1 + \lambda_0^2)$. More details are provided in Appendix C.

4.3. Improved protocol based on more communications

The above protocol for verifying GHZ-like states can be improved further if more communications are allowed. Let $\Omega_k (k = 1, 2, \ldots, n)$ be the strategy defined according to Eq. (27), but with the roles of party $k$ and party $n$ interchanged; that is, the measurement performed by party $k$ depends on the measurement outcomes of other parties. Then we can construct a new strategy by applying $\Omega_1, \Omega_2, \ldots, \Omega_n$ with probability $1/n$ each. The resulting verification operator reads

$$\Omega_{VI} = \frac{1}{n} \sum_{k=1}^{n} \Omega_k = p P_{0} + \frac{1-p}{n} \sum_{k=1}^{n} \Pi_k,$$  

(33)

where $0 \leq p \leq 1$. According to Eq. (28), we have

$$\frac{1}{n} \sum_{k=1}^{n} \Pi_k = |\xi\rangle\langle \xi| + \frac{1}{n} \sum_{k=1}^{n} R_k - \sum_{j=0}^{d-1} \lambda_j^2 |j\rangle\langle j| \otimes I_n,$$  

(34)

where $R_k := I_1^{\otimes (k-1)} \otimes \rho_k \otimes I_1^{\otimes (n-k)}$ and $\rho_k$ is the reduced state of $|\xi\rangle\langle \xi|$ for party $k$. In addition,

$$\beta(\Omega_{VI}) = \max\{p, (1-p)n^{-1}[(n-1)\lambda_0^2 + \lambda_1^2]\}$$  

$$\geq [n + (n-1)\lambda_0^2 + \lambda_1^2]^{-1}[(n-1)\lambda_0^2 + \lambda_1^2].$$  

(35)

The bound is saturated when $p = \frac{(n-1)\lambda_0^2 + \lambda_1^2}{n + (n-1)\lambda_0^2 + \lambda_1^2}$, in which case we have

$$\nu(\Omega_{VI}) = \frac{n}{n + (n-1)\lambda_0^2 + \lambda_1^2} \geq \nu(\Omega_V).$$  

(36)

The strategy $\Omega_{VI}$ is more efficient than $\Omega_V$ except when $\lambda_1 = \lambda_0$, as illustrated in Fig. 2.

5. Adversarial scenario

Finally, we turn to the adversarial scenario in which the quantum state is controlled by a potentially malicious adversary [35, 36]. Efficient state verification in such adversarial
Figure 2. Efficient verification of $n$-qubit GHZ-like states $|\xi\rangle = \cos \theta |0\rangle^\otimes n + \sin \theta |1\rangle^\otimes n$ in the nonadversarial scenario (upper plot) and adversarial scenario (lower plot). Here $N$ is the number of tests required to achieve infidelity $\varepsilon = 0.01$ and significance level $\delta = 0.01$. Note that $N(\Omega_{\text{VI}})$ and $N(\Omega_{\text{IX}})$ are dependent on the qubit number $n$, while $N(\Omega_{\text{IV}})$, $N(\Omega'_{\text{V}})$ and $N(\Omega_{\text{VIII}})$ are not.

scenario is crucial to quantum secret sharing [4, 5] and quantum networks [7]. In this case, we can still verify the target state by virtue of random permutations before applying a strategy $\Omega$ as in the nonadversarial scenario [26, 27]. If there is no restriction on the accessible measurements, then the optimal strategy can be chosen to be homogeneous,

$$\Omega = |\Psi\rangle\langle\Psi| + \beta(\Omega)(1 - |\Psi\rangle\langle\Psi|).$$  \hspace{1cm} (37)

In the high-precision limit $\varepsilon, \delta \to 0$, the minimum number of tests required to verify $|\Psi\rangle$ within infidelity $\varepsilon$ and significance level $\delta$ reads [26, 27] (assuming $\beta(\Omega) > 0$),

$$N \approx [\beta(\Omega)\varepsilon \ln \beta(\Omega)^{-1}]^{-1} \ln \delta^{-1}. $$ \hspace{1cm} (38)

This number is minimized when $\beta(\Omega) = 1/e$, which yields $N \approx e \varepsilon^{-1} \ln \delta^{-1}$. In addition, this number increases monotonically when $\beta(\Omega)$ deviates from the value $1/e$. If $\varepsilon, \delta$ are finite but small, say $\varepsilon, \delta \leq 0.01$, then the choice $\beta(\Omega) = 1/e$ is nearly optimal even if it is not exactly optimal. Besides quantum state verification in the adversarial scenario, the homogeneous strategy in Eq. (37) is useful for fidelity estimation thanks to the equality $\text{tr}(\rho \Omega) = [1 - \beta(\Omega)]|\Psi\rangle\langle\Psi|\rho + \beta(\Omega)$. For this application, a small $\beta(\Omega)$ is preferred to achieve a high precision [27].
Our strategies for verifying qudit GHZ states are homogeneous with \( \beta(\Omega) = 1/(d+1) \), and can be applied to fidelity estimation directly. To construct the optimal verification strategy in the adversarial scenario, it suffices to add the trivial test with a suitable probability. The test operator associated with the trivial test is the identity operator, so all states can pass the test for sure. Let \( p = [(d+1)\beta - 1]/d \); then we have

\[
\Omega_{\text{VII}} := (1 - p) \frac{1 + d |\text{GHZ}_d^n\rangle \langle \text{GHZ}_d^n|}{d+1} + p \mathbb{1} = |\text{GHZ}_d^n\rangle \langle \text{GHZ}_d^n| + \beta(1 - |\text{GHZ}_d^n\rangle \langle \text{GHZ}_d^n|). \tag{39}
\]

Any homogeneous strategy \( \Omega \) with \( 1/(d+1) \leq \beta(\Omega) < 1 \) can be so constructed using local projective measurements. In particular, by choosing \( p = (d+1 - e)/(ed) \), we can construct the homogeneous strategy \( \Omega_{\text{VII}} \) with \( \beta(\Omega_{\text{VII}}) = 1/e \), which is optimal for high-precision verification in the adversarial scenario (the optimal value may be slightly different when \( \varepsilon, \delta \) are finite but small). Similarly, we can construct a homogeneous strategy \( \Omega \) with \( \beta(\Omega) = 2/(d+1) \), with which the GME can be certified in the adversarial scenario using only one test as long as the significance level satisfies \( \delta \geq 4d/(d+1)^2 \), as illustrated in Fig. 1. This claim follows from the same reasoning that leads to Theorem 3 in Ref. [22], although here we are concerned with GME instead of bipartite entanglement.

Next, we devise a homogeneous strategy for verifying GHZ-like states by modifying \( \Omega_{\text{V}} \) in Eq. (27), which requires one-way communication. Let \( \lambda^2_0/(1 + \lambda^2_0) \leq p < 1 \) and replace the test projector \( P_0 \) in Eq. (10) by the following test operator

\[
Q_0 = P_0 + \sum_{j \in \mathcal{B}} \left[ 1 - \left( \frac{1}{p} - 1 \right) \lambda^2_{j_n} \right] |j\rangle \langle j|, \tag{40}
\]

where \( \mathcal{B} \) denotes the subset of \( \mathbb{Z}_d^n \) excluding elements \( j \) that satisfy \( j_1 = j_2 = \cdots = j_n \). Note that \( Q_0 \) can be realized by local projective measurements: All \( n \) parties perform projective measurements on the standard basis; the test is passed with certainty if they obtain the same outcome, while with probability \( 1 - (p^{-1} - 1)\lambda^2_{j_n} \) if they do not obtain the same outcome. Then the verification operator \( \Omega_{\text{V}} \) turns into

\[
\Omega_{\text{VIII}} = pQ_0 + (1 - p)\Pi = |\xi\rangle \langle \xi| + p(1 - |\xi\rangle \langle \xi|), \tag{41}
\]

which is homogeneous with \( \beta(\Omega) = p \). To achieve optimal performance in high-precision verification in the adversarial scenario, we can choose \( p = \max\{e^{-1}, \lambda^2_0/(1 + \lambda^2_0)\} \}. If \( \lambda^2 \leq 1/(e-1) \), then we have \( \beta(\Omega) = 1/e \), so the homogeneous strategy \( \Omega_{\text{VIII}} \) constructed in this way is optimal even among strategies that can access entangling measurements. In general, \( \Omega_{\text{VIII}} \) is optimal among all strategies based on one-way LOCC. Even in the worst case \( \beta(\Omega) = 1/2 \), the number of required tests is only \( 2(\ln \delta^{-1})/\varepsilon \ln 2 \), and the overhead compared with the optimal strategy based on entangling measurements is only about 6%. By contrast, the choice \( p = \lambda^2_0/(1 + \lambda^2_0) \) is optimal for fidelity estimation.

The strategy \( \Omega_{\text{VI}} \) in Eq. (33) can also be turned into a homogeneous strategy. Let
\[ \frac{(n-1)\lambda_0^2 + \lambda_1^2}{n + (n-1)\lambda_0^2 + \lambda_1^2} \leq p < 1 \] and replace the projector \( P_0 \) by the following operator

\[ \tilde{Q}_0 = P_0 + \sum_{j \in \mathcal{S}} \left[ 1 - \frac{1}{n} \left( \frac{1}{p} - 1 \right) \sum_{k=1}^{n} \lambda_{jk}^2 \right] |j\rangle\langle j|, \tag{42} \]

which can be realized by local projective measurements in analogy to \( Q_0 \). The resulting verification operator reads

\[ \Omega_{IX} = p\tilde{Q}_0 + (1 - p) \frac{1}{n} \sum_{k=1}^{n} \Pi_k = |\xi\rangle\langle \xi| + p(1 - |\xi\rangle\langle \xi|), \tag{43} \]

which is homogeneous with \( \beta(\Omega) = p \). For high-precision verification in the adversarial scenario, the optimal choice of \( p \) is

\[ p = \max \left\{ e^{-1} ; \frac{(n-1)\lambda_0^2 + \lambda_1^2}{n + (n-1)\lambda_0^2 + \lambda_1^2} \right\}. \]

The resulting strategy \( \Omega_{IX} \) is optimal if \( (n-1)\lambda_0^2 + \lambda_1^2 \leq n/(e - 1) \), in which case we have \( \beta(\Omega) = 1/e \). For fidelity estimation, the alternative choice \( \frac{(n-1)\lambda_0^2 + \lambda_1^2}{n + (n-1)\lambda_0^2 + \lambda_1^2} \) is optimal.

6. Conclusion

We proposed optimal protocols for verifying GHZ states based on local projective measurements. Only Pauli measurements are required when the local dimension is a prime. These protocols are also surprisingly efficient for estimating the fidelity and certifying the GME. In particular, they enable the certification of the GME with any given significance level using only one test when the local dimension is sufficiently large. Such a high efficiency has never been achieved or even anticipated before. Our results indicate that it is easier to certify GME than thought previously. We hope that these results will be demonstrated in experiments in the near future. Moreover, our protocols can be generalized to verify GHZ-like states and can be applied to the adversarial scenario, while retaining a high efficiency. Our study provides an efficient tool for evaluating the qualities of GHZ states prepared in the lab. Meanwhile, it offers valuable insights on the verification, fidelity estimation, and entanglement certification of multipartite quantum states. In the future it would be desirable to generalize our results to other important multipartite quantum states.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant No. 11875110).
Appendix A. Proofs of Equations (7), (12) and (18)

Proof of Eq. (7). The sum of all $P_\mathcal{Y}$ with $\mathcal{Y} \subset \{1, 2, \ldots, n\}$ of even cardinalities can be expressed as

\[
\sum_\mathcal{Y} P_\mathcal{Y} = 2^{n-2} \mathbb{1} + \frac{1}{2} \sum_{l=0}^{[n/2]} (-1)^l \sum_j P_j \{Y^{\otimes 2l} \otimes X^{\otimes (n-2l)}\}
\]

\[
= 2^{n-2} \mathbb{1} + \frac{1}{4} [(X+iY)^{\otimes n} + (X-iY)^{\otimes n}]
\]

\[
= 2^{n-2} \mathbb{1} + \frac{1}{4} [(1 + |0\rangle\langle 1|)^{\otimes n} + (|1\rangle\langle 0|)^{\otimes n}], \tag{A.1}
\]

where $\sum_j P_j \{Y^{\otimes 2l} \otimes X^{\otimes (n-2l)}\}$ denotes the sum over $\left(\begin{array}{c} n \\ 2l \end{array}\right)$ distinct permutations of $Y^{\otimes 2l} \otimes X^{\otimes (n-2l)}$. This equation implies the second equality in Eq. (7). \hfill \square

Proof of Eq. (12). The sum of all $P_r$ with $\sum_k r_k = 0 \mod d$ can be expressed as

\[
\sum_r P_r = d^{n-2} \mathbb{1} + \frac{1}{d} \sum_{l=1}^{d-1} \sum_r \prod_{k=1}^{n} (X_k Z_k)^l
\]

\[
= d^{n-2} \mathbb{1} + \frac{1}{d^2} \sum_{l=1}^{d-1} \sum_{s=0}^{d-1} \sum_{r=0}^{d-1} \omega^{-sr} (XZ)^l
\]

\[
= d^{n-2} \mathbb{1} + \frac{1}{d^2} \sum_{l=1}^{d-1} \sum_{j=0}^{d-1} (d |j+l\rangle \langle j|)^{\otimes n}
\]

\[
= d^{n-2} \mathbb{1} + \sum_{j' \neq j} (|j'\rangle \langle j|)^{\otimes n}, \tag{A.2}
\]

which implies Eq. (12). Here the first equality is meaningful when $d$ is odd, in which case $(X_k Z_k)^d = \mathbb{1}_1$. The third equality follows from the following fact: For $s = 0, 1, \ldots, d-1$ and $l = 1, 2, \ldots, d-1$, we have

\[
\sum_{r=0}^{d-1} \omega^{-sr} (XZ)^l = X^l \sum_{r=0}^{d-1} \omega^r [l(l-1)/2 - s] Z^r
\]

\[
= \sum_{j=0}^{d-1} |j+l\rangle \langle j| \left( \sum_{r=0}^{d-1} \omega^r [l(l-1)/2 + jl - s] \right). \tag{A.3}
\]

The last term in the parentheses vanishes except when $l(l-1)/2 + jl - s = 0 \mod d$, in which case it equals $d$. If $d$ is an odd prime and $l \neq 0$, then the equation $l(l-1)/2 + jl - s = 0 \mod d$ for each $s$ has a unique solution for $j \in \mathbb{Z}_d$, and the map from $s$ to the solution $j$ is one to one, so the third equality in Eq. (A.2) holds.

To clarify why the above proof does not work when $d$ is an odd number that is not a prime, suppose $l$ is a divisor of $d$. Then the equation $l(l-1)/2 + jl - s = 0 \mod d$ has multiple solutions when $s$ is a multiple of $l$, while it has no solution otherwise. Therefore, the third equality in Eq. (A.2) does not hold in this case. That is why we
assume that $d$ is an odd prime in order to construct the optimal protocol based on Pauli measurements.

\textbf{Proof of Eq. (15).} The sum of all $P_h$ with $\sum_k h_k = 0 \mod m$ can be expressed as

\[
\sum_h P_h = \frac{m^{n-1}}{d} \mathbf{1} + \frac{1}{d} \sum_{h} \prod_{k=1}^{n} (X_k W_k^{h_k})^l
\]

\[
= \frac{m^{n-1}}{d} \mathbf{1} + \frac{1}{d} \sum_{l=1}^{d-1} \sum_{s=1}^{m} \left[ \sum_{h=1}^{m} \mu^{-sh} (XW^h)^l \right] \otimes \otimes
\]

\[
= \frac{m^{n-1}}{d} \mathbf{1} + \frac{1}{d} \sum_{l=1}^{d-1} \sum_{j=0}^{d-1} (m|j+l\rangle\langle j|) \otimes \otimes
\]

\[
= \frac{m^{n-1}}{d} \mathbf{1} + \sum_{j' \neq j} (|j'\rangle\langle j|) \otimes \otimes, \tag{A.4}
\]

which implies Eq. (15). Here the third equality follows from the following fact: For each $l = 1, 2, \ldots, d-1$ and $s = 1, 2, \ldots, m$, we have

\[
f(s, l) := \sum_{h=1}^{m} \mu^{-sh}(XW^h)^l = \sum_{h=1}^{m} \mu^{-sh} \sum_{t=0}^{d-1} \omega^{-tl}|\psi_{ht}\rangle\langle \psi_{ht}|
\]

\[
= \frac{1}{d} \sum_{j,j'=0}^{d-1} (|j'\rangle\langle j|) \left( \sum_{h=1}^{m} \mu^{h(j'-j)(j'+j-1)/2-s} \right) \left( \sum_{t=0}^{d-1} \omega^{t(j'-j-l)} \right)
\]

\[
= \sum_{j=0}^{d-1} (|j+l\rangle\langle j|) \left( \sum_{h=1}^{m} \mu^{h[g(j,l)-s]} \right), \tag{A.5}
\]

where $g(j, l) := (\hat{j} - j)(\hat{j} + j - 1)/2$ with

\[
\hat{j} := \begin{cases} j + l & j + l \leq d - 1, \\ j + l - d & j + l \geq d. \end{cases} \tag{A.6}
\]

The last term in the parentheses in Eq. (A.5) vanishes except when $g(j, l) - s = 0 \mod m$, in which case it equals $m$. Given $l \in \{1, 2, \ldots, d-1\}$, note that each $j \in \{0, 1, \ldots, d-1\}$ is a solution of the equation $g(j, l) - s = 0 \mod m$ for a unique $s \in \mathbb{Z}_m$. If, in addition, $m \geq \lfloor \frac{d}{2}(d-1)^2 \rfloor$, then the equation $g(j, l) - s = 0 \mod m$ for each $l$ and $s$ has at most one solution for $j \in \mathbb{Z}_d$, which implies that the third equality in Eq. (A.4) holds. To prove this claim, let $g_m(j, l) := [g(j, l) \mod m]$; then $g_m(0, l), g_m(1, l), \ldots, g_m(d-1, l)$ are not equal to each other, as explained as follows; cf. Proposition 4.3 in Ref. [30].

For a given $l \in \{1, 2, \ldots, d-1\}$, the function $g(j, l)$ is monotonically increasing in $j$ when $j \in \{0, \ldots, d-l-1\}$, but monotonically decreasing in $j$ when $j \in \{d-l, \ldots, d-1\}$. \hfill $\square$
In addition we have

\[ 0 \leq l(2d - l - 3)/2 < m, \quad j = 0, \ldots, d - l - 1, \]

(A.7)

\[ -m < (l - d)(d + l - 3)/2 \leq g(j, l) \leq (l - d)(d - l - 1)/2 \leq 0, \quad j = d - l, \ldots, d - 1, \]

(A.8)

\[ l(2d - l - 3)/2 < (l - d)(d + l - 3)/2 + m. \]

(A.9)

Therefore, the two number sets \( \{g_m(j, l)\}_{j=0}^{d-l-1} \) and \( \{g_m(j, l)\}_{j=d-l}^{d-1} \) have no intersection; moreover, all the numbers \( g_m(0, l), g_m(1, l), \ldots, g_m(d-1, l) \) are distinct.

The second equality in Eq. (A.5) follows from the fact that

\[
XW^h = \sum_t \omega^{-t} |\psi_{ht}\rangle \langle \psi_{ht}| \quad \text{for } h = 1, \ldots, m.
\]

To see this, note that

\[
\sum_{t=0}^{d-1} \omega^{-t} |\psi_{ht}\rangle \langle \psi_{ht}| = \frac{1}{d} \sum_{j,j'=0}^{d-1} (|j'\rangle \langle j|) \left( e^{i\pi h (j'-j)(j'+j-1)/m} \sum_{t=0}^{d-1} \omega^{t(j'-j-1)} \right)
\]

\[
= \sum_{j=0}^{d-1} (|\tilde{j}\rangle \langle j|) \left( e^{i\pi h (\tilde{j}-j)(\tilde{j}+j-1)/m} \right)
\]

\[
= \mu^{-h(d-1)(d-2)/2} (|0\rangle \langle d-1|) + \sum_{j=0}^{d-2} \mu^{hj} (|j+1\rangle \langle j|)
\]

\[
= XW^h,
\]

(A.10)

where \( \tilde{j} \) is equal to \( \hat{j} \) in Eq. (A.6) with \( l = 1 \). This observation completes the proof. \( \square \)

Appendix B. Proof of Proposition 1

Proof. To start with, we assume that the strategy \( \Omega \) consists of \( 1 + 2^{n-1} \) tests, that is, \( P_0 \) and \( P_\mathcal{Y} \) with even \( |\mathcal{Y}| \). In other words, \( \Omega \) can be expressed as

\[
\Omega = p_0 P_0 + \sum_{\mathcal{Y}} p_\mathcal{Y} P_\mathcal{Y}, \quad p_0, p_\mathcal{Y} \geq 0, \quad p_0 + \sum_{\mathcal{Y}} p_\mathcal{Y} = 1.
\]

(B.1)

Then \( p_0 \leq \beta(\Omega) = 1/3 \) due to the assumption \( \nu(\Omega) = 2/3 \). Accordingly,

\[
\text{tr}(\Omega) = 2p_0 + 2^{n-1} \sum_{\mathcal{Y}} p_\mathcal{Y} = 2p_0 + 2^{n-1}(1 - p_0) \geq \frac{2^n + 2}{3},
\]

(B.2)

where the inequality is saturated iff \( p_0 = 1/3 \). In addition,

\[
\beta(\Omega) \geq \frac{\text{tr}(\Omega) - 1}{2^n - 1} \geq \frac{2^n - 1}{3(2^n - 1)} = \frac{1}{3}.
\]

(B.3)

The first inequality is saturated iff \( \Omega \) is homogeneous, which means all eigenvalues of \( \Omega \) are equal except for the largest one. The second inequality is saturated iff the inequality
in Eq. (B.2) is saturated, which means \( p_0 = 1/3 \). If \( \nu(\Omega) = 2/3 \), that is, \( \beta(\Omega) = 1/3 \), then both inequalities are saturated, so that

\[
\Omega = \frac{1}{3} (1 + 2|\text{GHZ}_n^2\rangle\langle\text{GHZ}_n^2|) = \Omega_1 = \frac{1}{3} \left( P_0 + \frac{1}{2n-2} \sum_{\mathcal{Y}} P_{\mathcal{Y}} \right).
\]

Moreover, the decomposition in the right hand side is unique because the \( 2^{n-1} + 1 \) projectors \( P_0 \) and \( P_{\mathcal{Y}} \) with even \( |\mathcal{Y}| \) are linearly independent in the operator space.

Next, we turn to the general situation. Suppose on the contrary that the strategy \( \Omega \) involves test operators \( Q_1, Q_2, \ldots, Q_r \) that are different from those appearing in Eq. (B.4). According to Lemma 1 below, each \( Q_s \) satisfies either \( Q_s > P_0 \) or \( Q_s > P_{\mathcal{Y}_s} \) for some \( \mathcal{Y}_s \in \{1, 2, \ldots, n\} \) with even cardinality. Let \( \Omega' \) be a variant of \( \Omega \) obtained by replacing \( Q_s \) with \( P_0 \) when \( Q_s > P_0 \) or with \( P_{\mathcal{Y}_s} \) when \( Q_s > P_{\mathcal{Y}_s} \). Then

\[
\beta(\Omega) = \|\Omega\| \geq \|\Omega'\| = \beta(\Omega') \geq \frac{1}{3};
\]

where \( \Omega = \Omega - |\text{GHZ}_n^2\rangle\langle\text{GHZ}_n^2| \) and \( \Omega' = \Omega' - |\text{GHZ}_n^2\rangle\langle\text{GHZ}_n^2| \). If \( \beta(\Omega) = 1/3 \) (that is, \( \nu(\Omega) = 2/3 \)), then the two inequalities are saturated. So \( \Omega' \) is homogeneous according to Eq. (B.4); that is, \( \Omega' \) is proportional to the projector \( \mathbb{1} - |\text{GHZ}_n^2\rangle\langle\text{GHZ}_n^2| \). In this case, the first inequality can be saturated only if \( \Omega = \Omega' \) or, equivalently, \( \Omega = \Omega' \). Therefore, the strategy \( \Omega \) consists of only the test projectors \( P_0 \) and \( P_{\mathcal{Y}} \) with even \( |\mathcal{Y}| \). In addition, the test projector \( P_0 \) can be realized only when all parties perform \( Z \) measurements; the test projector \( P_{\mathcal{Y}} \) can be realized only when all parties in the set \( \mathcal{Y} \) perform \( Y \) measurements, and the other parties perform \( X \) measurements. This observation completes the proof of Proposition 1. \( \square \)

**Lemma 1.** Suppose \( Q \) is any test operator for the GHZ state \( |\text{GHZ}_n^2\rangle \) that is based on some Pauli measurement. If at least one party performs \( Z \) measurement, then \( Q \geq P_0 \). If parties in the set \( \mathcal{Y} \) perform \( Y \) measurements and other parties perform \( X \) measurements, then \( Q \geq P_{\mathcal{Y}} \) when \( |\mathcal{Y}| \) is even and \( Q = 1 \) when \( |\mathcal{Y}| \) is odd.

The bound \( Q \geq P_0 \) can be saturated only when all parties perform \( Z \) measurements. The bound \( Q \geq P_{\mathcal{Y}} \) can be saturated only when all parties in the set \( \mathcal{Y} \) perform \( Y \) measurements, and the other parties perform \( X \) measurements.

**Proof of Lemma 1.** By assumption, the GHZ state \( |\text{GHZ}_n^2\rangle \) can always pass the test specified by the test operator \( Q \), which means \( |\text{GHZ}_n^2\rangle\langle\text{GHZ}_n^2| \leq Q \leq 1 \). Denote by \( \mathcal{X}, \mathcal{Y}, \mathcal{Z} \) the sets of parties that perform \( X, Y, Z \) measurements, respectively, and let \( a = |\mathcal{X}|, b = |\mathcal{Y}|, c = |\mathcal{Z}| \). Let \( |\pm XY\rangle \) be the eigenstates of \( X \) (\( Y \)) with eigenvalues \( \pm 1 \). Due to the permutation symmetry of the state \( |\text{GHZ}_n^2\rangle \) and the projector \( P_0 \), we can assume without loss of generality that \( \mathcal{X} \) consists of the first \( a \) parties, while \( \mathcal{Y} \) consists of the last \( c \) parties.

If at least one party performs \( Z \) measurement, then \( c \geq 1 \) by assumption. When \( a + b + c = n \), note that \( |\pm X\rangle^{\otimes a} \otimes |\pm Y\rangle^{\otimes b} \otimes |0\rangle^{\otimes c} \) has nonzero overlap with \( |\text{GHZ}_n^2\rangle \); the
same is true for all kets of the form
$$|\phi_z\rangle := (Z^z \otimes 1^c_1) (|+\rangle^{a} \otimes |+\rangle^{b} \otimes |0\rangle^{c})$$,
$$z = (z_1, z_2, \ldots, z_{a+b}) \in \{0, 1\}^{a+b}, \quad (B.6)$$
$$|\varphi_z\rangle := (Z^z \otimes 1^c_1) (|+\rangle^{a} \otimes |+\rangle^{b} \otimes |1\rangle^{c})$$,
$$z = (z_1, z_2, \ldots, z_{a+b}) \in \{0, 1\}^{a+b}, \quad (B.7)$$

where
$$Z^z := \prod_{k=1}^{a+b} Z_k^{z_k}. \quad (B.8)$$

Therefore,
$$Q \geq \sum_{z \in \{0,1\}^{a+b}} \langle \phi_z | \phi_z \rangle + |\varphi_z | \langle \varphi_z | \rangle = 1_{1}^{a+b} \otimes [\langle |0\rangle^{c} |0\rangle^{c} + \langle |1\rangle^{c} |1\rangle^{c}] \geq P_0, \quad (B.9)$$
where $1_{1}$ is the identity operator on the Hilbert space of one qubit. Equation (B.9) shows that $X$ and $Y$ measurements are redundant when some party performs $Z$ measurement.

Next, suppose all parties perform either $X$ or $Y$ measurements; that is, $c = 0$ and $a + b = n$. Let
$$|\phi_z\rangle := Z^z (|+\rangle^{a} \otimes |+\rangle^{b})$$,
$$z = (z_1, z_2, \ldots, z_n) \in \{0, 1\}^n. \quad (B.10)$$

Then
$$|\langle \text{GHZ}_{n}^2 | \phi_z \rangle|^2 = \frac{1}{2n+1} |1 + i^b (-1)^{|z|}|^2,$$  
$$(B.11)$$

where $|z|$ denotes the Hamming weight of $z$, that is, the number of bits equal to 1. If $b = |\mathcal{Y}|$ is odd, then the overlap in Eq. (B.11) is nonzero for all $z \in \{0, 1\}^n$. Therefore $Q = 1$ since, otherwise, the GHZ state cannot pass the test with certainty. If $b = |\mathcal{Y}| = 2t$ is even, then
$$|\langle \text{GHZ}_{n}^2 | \phi_z \rangle|^2 = \frac{1}{2n+1} |1 + (-1)^{|z|+t}|^2,$$  
$$(B.12)$$

so the overlap is nonzero iff $|z| = t \mod 2$. Therefore,
$$Q \geq \sum_{z \in \{0,1\}^n, |z|=t \mod 2} |\phi_z \rangle \langle \phi_z | = P_{\mathcal{Y}}. \quad (B.13)$$

The above analysis also shows that $Q = 1$ if the Pauli measurement is incomplete and no party performs $Z$ measurement.

Finally, it is worth pointing out that Proposition 2 can be proved using a similar reasoning as presented above. Lemma 1 featuring in the proof of Proposition 1 is replaced by the following lemma, which applies to the qudit case, assuming that $d$ is an odd prime. Its proof is a simple analog of the counterpart for the qubit case and is thus omitted.
Lemma 2. Suppose $Q$ is any test operator for the GHZ state $|\text{GHZ}_n^d\rangle$ that is based on some Pauli measurement, where $d$ is an odd prime. If at least one party performs $Z$ measurement, then $Q \geq P_0$. If party $k$ performs $XZ^{r_k}$ measurement for $k = 1, 2, \ldots, n$, then $Q = 1$ when $\sum_{k=1}^n r_k \neq 0 \bmod d$ and $Q \geq P_r$ when $\sum_{k=1}^n r_k = 0 \bmod d$, where $P_r$ is defined in Eq. (11).

Appendix C. Alternative optimal strategy for verifying GHZ-like states

In the main text we proposed an optimal strategy for verifying GHZ-like states $|\xi\rangle = \sum_{j=0}^{d-1} \lambda_j |j\rangle^{\otimes n}$ using one-way LOCC, which requires only $1 + 2^{n-1}$ distinct tests when $d = 2$ and $1 + m^{n-1}$ distinct tests with $m \geq \lceil \frac{3}{4}(d - 1)^2 \rceil$ when $d \geq 3$. Here we propose an alternative optimal protocol using much fewer measurement settings, assuming that the local dimension is an odd prime. In addition, for each test, all parties except for one of them can perform Pauli measurements as in the case of qubits. The underlying idea is similar to the construction of $\Omega_V$ in the main text. Let

$$P_r' = (\mathbb{1}_1^{\otimes (n-1)} \otimes M) P_r (\mathbb{1}_1^{\otimes (n-1)} \otimes M),$$

where $P_r$ is the projector given in Eq. (11), and $M := \sqrt{d} \text{diag}(\lambda_0, \ldots, \lambda_{d-1})$. Recall that

$$\frac{1}{d^{n-1}} \sum_r P_r = \frac{1}{d} \left[ 1 + \sum_{j \neq j'} (|j'\rangle \langle j|)^{\otimes n} \right], \quad d \text{ is odd prime.}$$

So we have

$$\frac{1}{d^{n-1}} \sum_r P_r' = (\mathbb{1}_1^{\otimes (n-1)} \otimes M) \left( \frac{1}{d^{n-1}} \sum_r P_r \right) (\mathbb{1}_1^{\otimes (n-1)} \otimes M)$$

$$= |\xi\rangle \langle \xi| + \mathbb{1}_1^{\otimes (n-1)} \otimes \rho_n - \sum_{j=0}^{d-1} \lambda_j^2 (|j\rangle \langle j|)^{\otimes n},$$

where $\rho_n := \text{tr}_{1,2,\ldots,n-1}(|\xi\rangle \langle \xi|)$ is the reduced state for party $n$. Therefore, $1 + d^{n-1}$ distinct tests are sufficient for constructing a strategy that is equivalent to $\Omega_V$ in the main text when $d$ is an odd prime. To be concrete, the strategy has the form

$$\Omega'_V = pP_0 + \frac{1-p}{d^{n-1}} \sum_r P_r',$$

and we have

$$\beta(\Omega'_V) = \beta(\Omega_V) = \max \{ p, (1-p)\lambda_0^2 \} \geq \frac{\lambda_0^2}{1 + \lambda_0^2}.$$
References

[1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in: *Bell’s Theorem, Quantum Theory, and Conceptions of the universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 69-72.

[2] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Bell’s theorem without inequalities. *Am. J. Phys.* **58**, 1131 (1990).

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

[4] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**, 042301 (2001).

[5] Y.-A. Chen et al. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95**, 200502 (2005).

[6] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **430**, 54 (2004).

[7] W. McCutcheon et al. Experimental verification of multipartite entanglement in quantum networks. *Nature Photon.* **7**, 13251 (2016).

[8] V. Scarani and N. Gisin, Spectral decomposition of Bell’s operators for qubits. *J. Phys. A: Math. Gen.* **34**, 6043 (2001).

[9] C. Zhang, Y.-F. Huang, Z. Wang, B.-H. Liu, C.-F. Li, and G.-C. Guo, Experimental Greenberger-Horne-Zeilinger-Type Six-Photon Quantum Nonlocality. *Phys. Rev. Lett.* **115**, 260402 (2015).

[10] X.-L. Wang et al. Experimental ten-photon entanglement. *Phys. Rev. Lett.* **117**, 210502 (2016).

[11] C. Song et al. 10-Qubit Entanglement and Parallel Logic Operations with a Superconducting Circuit. *Phys. Rev. Lett.* **119**, 180511 (2017).

[12] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, Experimental Greenberger-Horne-Zeilinger entanglement beyond qubits. *Nature Photon.* **12**, 759 (2018).

[13] Y. Ji, J. Bian, X. Chen, J. Li, X. Nie, H. Zhou, and X. Peng, Experimental preparation of Greenberger-Horne-Zeilinger states in an Ising spin model by partially suppressing the nonadiabatic transitions. *Phys. Rev. A* **99**, 032323 (2019).

[14] K. J. Resch, P. Walther, and A. Zeilinger, Full Characterization of a Three-Photon Greenberger-Horne-Zeilinger State Using Quantum State Tomography. *Phys. Rev. Lett.* **94**, 070402 (2005).

[15] D. Cruz et al. Efficient quantum algorithms for GHZ and W states, and implementation on the IBM quantum computer. *Adv. Quantum Technol.* **2**, 1900015 (2019).

[16] H. Häffner et al. Scalable multiparticle entanglement of trapped ions. *Nature* **438**, 643 (2005).

[17] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing. *J. Phys. A: Math. Gen.* **39**, 14427 (2006).

[18] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).

[19] H. Zhu and M. Hayashi, Efficient verification of hypergraph states. (2018), arXiv:1806.05565.

[20] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient verification of Dicke states. (2019), arXiv:1904.01979.

[21] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. *New J. Phys.* **11**, 043028 (2009).

[22] H. Zhu and M. Hayashi, Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).

[23] Z. Li, Y.-G Han, and H. Zhu, Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).

[24] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).

[25] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states. (2019), arXiv:1901.09856.
[26] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario. (2019), arXiv:1909.01900.

[27] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario. (2019), arXiv:1909.01943.

[28] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements. J. Math. Phys. 45, 2171 (2004).

[29] A. J. Scott, Tight informationally complete quantum measurements. J. Phys. A: Math. Gen. 39, 13507 (2006).

[30] A. Roy and A. J. Scott, Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. J. Math. Phys. 48, 072110 (2007).

[31] A. Dimić and B. Dakić, Single-copy entanglement detection. npj Quantum Inf. 4, 11 (2018).

[32] I. D. Ivanović, Geometrical description of quantal state determination. J. Phys. A: Math. Gen. 14, 3241 (1981).

[33] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements. Ann. Phys. 191, 363 (1989).

[34] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases. Int. J. Quantum Inf. 08, 535 (2010).

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

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