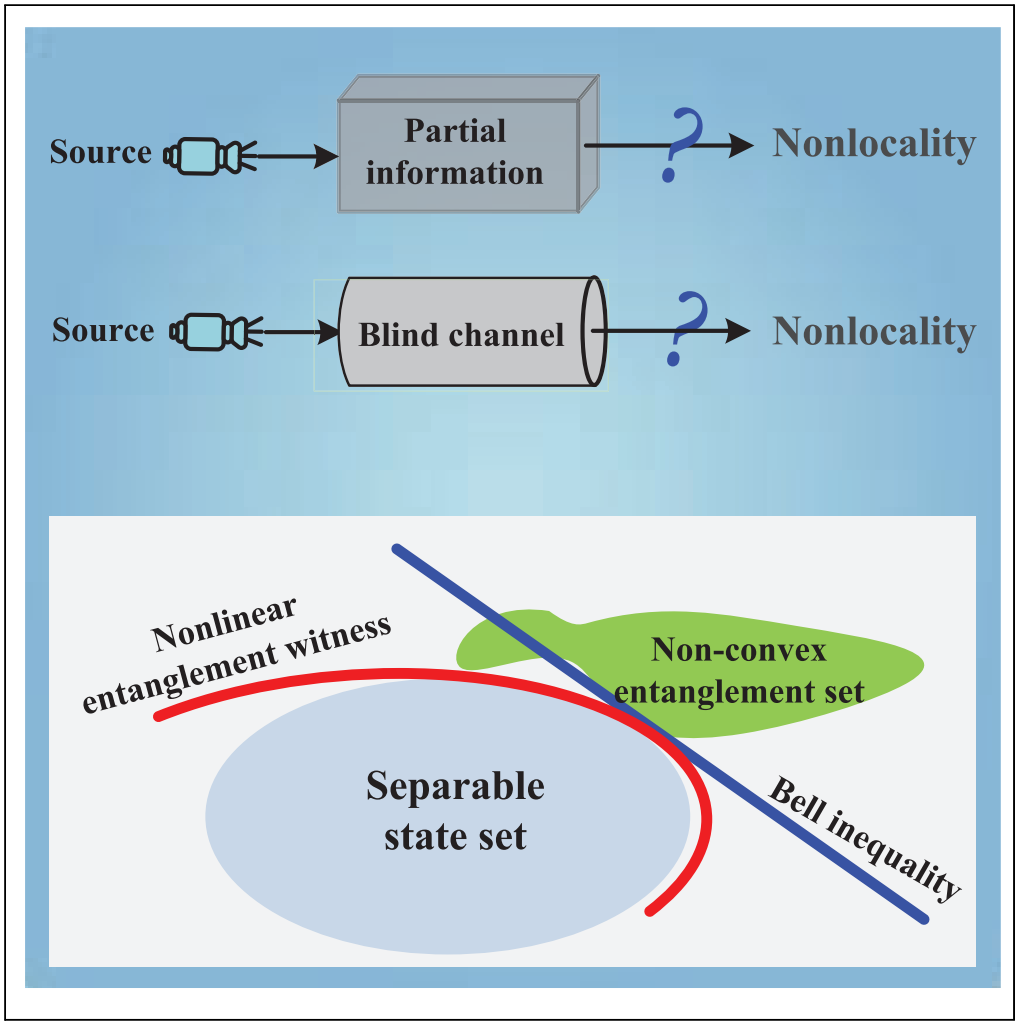
iScience

CellPress
OPEN ACCESS

Article

Blindly verifying partially unknown entanglement



Ming-Xing Luo, Shao-Ming Fei, Jing-Ling Chen

mxluo@swjtu.edu.cn (M.-X.L.)
feishm@cnu.edu.cn (S.-M.F.)
chenjl@nankai.edu.cn (J.-L.C.)

Highlights

A model of entanglement set verification is proposed and analyzed

Nonlinear entanglement witnesses for specific entanglement sets are constructed

Blind quantum verification scheme is built

Luo et al., iScience 25, 103972
March 18, 2022
https://doi.org/10.1016/j.isci.2022.103972

iScience

CellPress
OPEN ACCESS

Article

Blindly verifying partially unknown entanglement

Ming-Xing Luo,[1,5,6,*] Shao-Ming Fei,[2,4,*] and Jing-Ling Chen[3,*]

SUMMARY

Quantum entanglement has shown distinguished features beyond any classical state. Many methods have been presented to verify unknown entanglement with the complete information about the density matrices by quantum state tomography. In this work, we aim to identify unknown entanglement with only partial information of the state space. The witness consists of a generalized Greenberger-Horne-Zeilinger-like paradox expressed by Pauli observables, and a nonlinear entanglement witness expressed by density matrix elements. First, we verify unknown bipartite entanglement and study the robustness of entanglement witnesses against the white noise. Second, we generalize such verification to partially unknown multipartite entangled states, including the Greenberger-Horne-Zeilinger-type and W-type states. Third, we give a quantum-information application related to the quantum zero-knowledge proof. It further provides a useful method in blindly verifying universal quantum computation resources. These results may be interesting in entanglement theories, quantum communication, and quantum networks.

INTRODUCTION

Quantum entanglement cannot be decomposed into a statistical mixture of various product states (Einstein et al., 1935). It is the most surprising nonclassical property of composite quantum systems (Horodecki et al., 2009) that Schrödinger has singled out as "the characteristic trait of quantum mechanics" (Schrödinger, 1935). How to verify a given entanglement has become a fundamental problem in both quantum mechanics and quantum information processing. In 1964, Bell firstly proved that the statistics generated by some proper local quantum measurements on a two-qubit entanglement cannot be generated by any local-hidden variable model (Bell, 1964). The so-called Bell inequality provides an experimental method for verifying the intrinsic nonlocality of entanglement. Subsequently, this method has been extended for various entangled states (Clauser et al., 1969; Gisin, 1991; Greenberger et al., 1989; Brunner et al., 2014; Gühne and Tóth, 2009), except for special mixed states (Werner, 1989). Another method is from the Hahn-Banach Theorem (Lewenstein et al., 2000; Horodecki et al., 2009), which can separate each entanglement from a specific convex set consisting of all the separable states (Horodecki et al., 2009) by exploring the state-dependent witness function. This provides a universal method for witnessing all the entangled states (Horodecki et al., 2009; Amico et al., 2008).

In Bell experiments, such as experimentally observing the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality for a two-qubit state, initially one needs to know the explicit density matrix of the examined quantum state, so as to choose optimal measurements. Otherwise, selecting random measurement settings, he could only observe the probabilistic violations of the CHSH inequality (Laing et al., 2010). So far, the traditional Bell experiments (Bell, 1964; Clauser et al., 1969; Gisin, 1991) and entanglement witnesses (Lewenstein et al., 2000; Horodecki et al., 2009) require essentially the state tomography to learn its density matrix $\rho \in \mathcal{B}(\mathcal{H})$ (Lu et al., 2016), when people come to verify an unknown entangled source, as shown in Figure 1A. This situation seems to rule out the possibility for entanglement verification without complete information of its density matrix. It is interesting to consider that, what happens for an unknown entanglement with partial knowledge?

Specifically, suppose a given source is restricted to be an entanglement ensemble. One possibility is that the device provider gives only its state subspace $\mathcal{S} \subset \mathcal{B}(\mathcal{H})$, but not a specific density matrix. One example is known as an arbitrary bipartite state in the known subspace $\mathcal{S} \subset \mathcal{B}(\mathcal{H})$ spanned by the known basis $\{|00\rangle\langle 00|, |00\rangle\langle 11|, |11\rangle\langle 00|, |11\rangle\langle 11|\}$ (see Figure 1B), but not a specific Einstein-Podolsky-Rosen (EPR) state (Einstein et al., 1935). This can be further regarded as a blind quantum communication model inspired by

[1]CSNMT Int. Coop. Res. Centre (MoST), The School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, P.R. China

[2]School of Mathematical Sciences, Capital Normal University, Beijing 100048, P.R. China

[3]Theoretical Physics Division, Chern Institute of Mathematics, Nankai University, Tianjin 300071, P.R. China

[4]Max-Planck-Institute for Mathematics in the Sciences, Leipzig 04103 Germany

[5]Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, P.R. China

[6]Lead contact

*Correspondence: mxluo@swjtu.edu.cn (M.-X.L.), feishm@cnu.edu.cn (S.-M.F.), chenjl@nankai.edu.cn (J.-L.C.)

https://doi.org/10.1016/j.isci.2022.103972

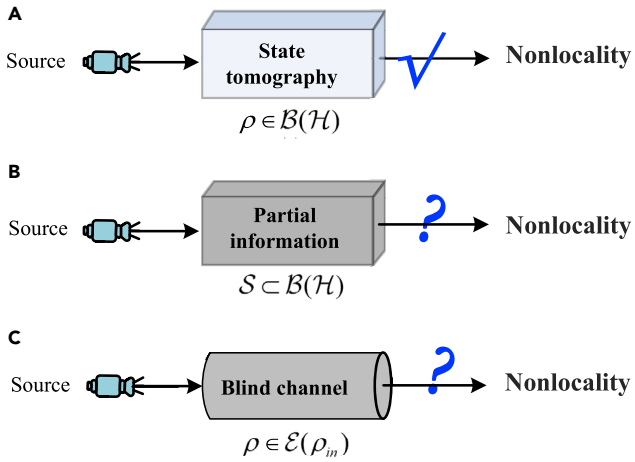


Figure 1. Schematic verification of partially unknown entanglement

(A) Traditional methods. The state tomography is firstly performed to learn the density matrix $\rho \in \mathcal{B}(\mathcal{H})$, which is further used for constructing Bell experiment or entanglement witness. Here, $\mathcal{B}(\mathcal{H})$ denotes the density operator space on Hilbert space $\mathcal{H}$.

(B) Proposed method without the state tomography. The given entanglement is supposed to be in a special subspace $\mathcal{S} \subset \mathcal{B}(\mathcal{H})$ spanned by known basis such as $\{|00\rangle\langle 00|, |00\rangle\langle 11|, |11\rangle\langle 00|, |11\rangle\langle 11|\}$, but without the knowledge of the mixture, that is, the probability in the pure state decomposition of the density matrix.

(C) Entanglement in a blind quantum communication model. A known entanglement ρ_{in} passes through one blind quantum channel $\mathcal{E}(\bullet)$ such as random unitary operations, that is, the output unknown state is given by $\rho = \mathcal{E}(\rho_{in})$.

the blind quantum computation (Broadbent et al., 2009), in which the EPR state passes through a specific blind channel, such as some random unitary operations (see Figure 1C). A natural problem is whether such relaxed assumptions allow verifying entanglement ensembles without the state tomography. This also intrigues an interesting problem of entanglement locking (Horodecki et al., 2005).

The purpose of this paper is to verify unknown entanglement with partial information of the state space. To reach this aim, we shall propose a *nonlinear entanglement witness* (NEW), which consists of a generalized Greenberger-Horne-Zeilinger-like (GHZ-like) paradox expressed by Pauli observables, and a nonlinear inequality expressed by density matrix elements. First, we verify an unknown bipartite entanglement, and also discuss the robustness of entanglement witnesses. Second, we generalize the verification of unknown entanglement to multipartite entangled states, such as the GHZ-type states and the cluster states. Third, we provide a quantum-information application related to the quantum zero-knowledge proof. Our result provides a general method for verifying universal unknown quantum computation resources (Raussendorf and Briegel, 2001). It is also robust against white noises and allows for experiments with recent techniques.

RESULTS

Entanglement ensemble model

A pure finite-dimensional quantum state is represented by a normalized vector $|\varphi\rangle$ in Hilbert space $\mathcal{H}$. An ensemble of pure states $\{|\varphi_i\rangle\}$ is represented by using density matrix $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$ on Hilbert space $\mathcal{H}$, where $\{p_i\}$ is a probability distribution. An bipartite state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is an entanglement (Horodecki et al., 2009) if it cannot be decomposed into the following form

$$\rho_{AB} = \sum_i p_i \varrho_A^{(i)} \otimes \varrho_B^{(i)} \qquad \text{(Equation 1)}$$

where $\varrho_{A(B)}^{(i)}$ are single-particle states and $\{p_i\}$ is a probability distribution.

As for the entanglement ensemble model, in this work, we consider an n-particle state in the density operator space $\mathcal{B}(\otimes_{j=1}^n \mathcal{H}_{A_j})$ associated with the Hilbert space $\otimes_{j=1}^n \mathcal{H}_{A_j}$. The additional information may be learned from the device provider. The traditional entanglement witnesses (Brunner et al., 2014; Gühne and Tóth, 2009; Horodecki et al., 2009) require complete information of its density matrix ρ by using the

state tomography. Here, the given state is distributed to n remote users who have no complete information about the density matrix ρ. For example, for a two-qubit system, its density operator is supposed to be in a special subspace $\mathcal{S}\subset\mathcal{B}(\mathcal{H})$ spanned by the known basis $\{|00\rangle\langle 00|, |00\rangle\langle 11|, |11\rangle\langle 00|, |11\rangle\langle 11|\}$ (see Figure 1B), but without the knowledge of mixture. Thus the main goal here is to separate one entanglement set $\mathcal{S}$ from all the separable states. Interestingly, $\mathcal{S}$ may be not convex and thus rule out the standard construction of linear entanglement witness (Horodecki et al., 2009) or linear Bell inequalities (Brunner et al., 2014). It is also different from self-testing entangled subspaces consisting of all entangled pure states with the state tomography (Baccari et al., 2020). Therefore, how to verify the entanglement set $\mathcal{S}$ will show insights in fundamental problems of entanglement theory.

Verifying partially unknown bipartite entanglement

Let us consider the simplest case of a two-qubit system on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$. A generalized bipartite entangled pure state shared by Alice and Bob reads

$$|\Phi(\theta)\rangle_{AB} = \cos\theta|00\rangle + \sin\theta|11\rangle, \qquad \text{(Equation 2)}$$

where $\theta\in(0,\pi/2)$, and $|\Phi(\pi/4)\rangle$ is the EPR state (Einstein et al., 1935). We now consider the following scenario: both parties only know the shared state has the following form:

$$\rho_{AB} = E(|\Phi(\theta)\rangle\langle\Phi(\theta)|), \qquad \text{(Equation 3)}$$

where $\mathcal{E}(\bullet)$ is a blind quantum channel defined by $\mathcal{E}(\varrho) = \sum_j p_j(U_j\otimes V_j)\varrho(U_j^\dagger\otimes V_j^\dagger)$, ϱ is the input state, $\{p_j\}$ is an unknown probability distribution, and U_j and V_j are any local phase transformations, e.g., $U_j = e^{i\theta_j}|0\rangle\langle 0| + e^{i\theta_j'}|1\rangle\langle 1|$ *and* $V_j = e^{i\vartheta_j}|0\rangle\langle 0| + e^{i\vartheta_j'}|1\rangle\langle 1|$, with unknown parameters $\theta_j,\theta_j',\vartheta_j,\vartheta_j'\in(0,\pi)$. In general, $\mathcal{E}(\bullet)$ can be defined through some positive-operator-value measurements (POVM), i.e., $\mathcal{E}(\rho) = \sum_i(M_i\otimes 1)\rho(M_i^\dagger\otimes 1)$, with $M_i = \sqrt{q_i}|0\rangle\langle 0| + \sqrt{r_i}|1\rangle\langle 1|$, $\sum_i M_i^\dagger M_i = 1$, and $\sum_i q_i = \sum_i r_i = 1$. The entanglement involved in the state ρ_{AB} is named as *the EPR-type entanglement*. The density matrix ρ_{AB} is rewritten into

$$\rho_{AB} = \rho_{00;00}|00\rangle\langle 00| + \rho_{11;11}|11\rangle\langle 11| + \rho_{00;11}|00\rangle\langle 11| + \rho_{11;00}|11\rangle\langle 00|, \qquad \text{(Equation 4)}$$

where $\rho_{ij;kl}$'s are the matrix elements satisfying $\rho_{00;00}+\rho_{11;11}=1$ and $\rho_{00;11}=\rho_{11;00}^*$. Thus our goal is to verify the entanglement set

$$\mathcal{S}_{epr} := \{\mathcal{E}(|\Phi(\theta)\rangle\langle\Phi(\theta)|), \forall|\Phi(\theta)\rangle, \mathcal{E}(\bullet)\} \qquad \text{(Equation 5)}$$

which is spanned by the known basis $\{|00\rangle\langle 00|, |00\rangle\langle 11|, |11\rangle\langle 00|, |11\rangle\langle 11|\}$ as in Equation (4). Notably, the CHSH inequality (Clauser et al., 1969) is inapplicable because of the unknown parameter θ_i's in Equation (3), which forbids two parties to find suitable observables. Meanwhile, $\mathcal{S}_{epr}$ is not convex. For instance, for the given state $\varrho = |\Phi(\theta)\rangle\langle\Phi(\theta)|$, $U_1 = 1 = |0\rangle\langle 0| + |1\rangle\langle 1|$, and $U_2 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, then one easily has $\rho_{AB} = \frac{1}{2}\sum_{j=1}^{2}(U_j\otimes 1)\varrho\left(U_j^\dagger\otimes 1\right) = \cos^2\theta|00\rangle\langle 00| + \sin^2\theta|11\rangle\langle 11|$, which is a separable state. This fact excludes the well-known method of linear entanglement witnesses (Horodecki et al., 2009).

For solving the problem, we have the following Theorem 1.

Theorem 1. The entanglement set $\mathcal{S}_{epr}$ is verifiable.

Proof.—First, let us present a generalized GHZ-like paradox for quantum entanglement, which is given by

$$\begin{aligned}\langle\sigma_z\otimes\sigma_z\rangle_\rho &= 1,\\ \langle\sigma_z\otimes\sigma_x\rangle_\rho &= 0,\\ \langle\sigma_x\otimes\sigma_z\rangle_\rho &= 0,\\ \langle\sigma_x\otimes\sigma_x\rangle_\rho &\overset{ES}{\neq} 0,\end{aligned} \qquad \text{(Equation 6)}$$

where "ES" represents "entangled states", σ_x and σ_z are Pauli matrices, and $\langle\sigma_j\otimes\sigma_k\rangle_\rho$ is defined by $\langle\sigma_j\otimes\sigma_k\rangle_\rho = Tr[\rho(\sigma_j\otimes\sigma_k)]$. In Equation (6), whose left-hand side contains four operators $\{E_1 = \sigma_z\otimes\sigma_z, E_2 = \sigma_z\otimes\sigma_x, E_3 = \sigma_x\otimes\sigma_z, E_4 = \sigma_x\otimes\sigma_x\}$. For a standard GHZ paradox (Greenberger et al., 1989), the global observableE_i's are required to satisfy a very strict condition: they are mutually commutative, i.e., $[E_j,E_k] = E_jE_k - E_kE_j = 0$ for any $j\neq k$, and moreover the examined entanglement is the common eigenstate of $\{E_1,E_2,E_3,E_4\}$. In Ref. (Wiseman et al., 2007), quantum nonlocality has been classified into three distinct

types: quantum entanglement, EPR steering, and Bell nonlocality. Among which, as quantum entanglement is the weakest type of quantum nonlocality, we develop the paradox (6) without the above strict conditions for witnessing entanglement.

Let us denote the supposedly definite real values of $v_{1,z}$ and $v_{1,x}$ for Alice, and $v_{2,z}$ and $v_{2,x}$ for Bob, with $v_{1,x}, v_{1,z}, v_{2,x}, v_{2,z} \in [1, -1]$ beyond the integers in the standard GHZ paradox (Greenberger et al., 1989). This can be regarded as a restricted hidden variable model. Then similar to the analysis of GHZ paradox, classically we have from Equation (6) that $v_{1,z}v_{2,z} = 1$, $v_{1,z}v_{2,x} = 0$, $v_{1,x}v_{2,z} = 0$, and $v_{1,x}v_{2,x} \neq 0$. But, the product of the first three relations gives $v_{1,z}^2 v_{2,z}^2 v_{1,x}v_{2,x} = v_{1,x}v_{2,x} = 0,$ which conflicts with the fourth relation.

The proof of witnessing entanglement set $\mathcal{S}_{epr}$ depends on the following nonlinear inequality

$$2\sqrt{\rho_{00;11}\rho_{11;00}} + \rho_{00;00} + \rho_{11;11} - 1 \leq 0 \qquad \text{(Equation 7)}$$

Which holds for any biseparable states (see Lemma 1 in Method details). From the inequality (7), ρ in Equation (4) is entangled if and only if $\rho_{00;11} \neq 0,$ in other words, it is separable state if and only if $\rho_{00;11} = \rho_{11;00} = 0$.

Next we come to prove that any separable state would violate one statement in the paradox (6). For any separable state ρ_{bs} without the decomposition in Equation (4), it violates the first statement in the paradox (6). Otherwise, from Equation (6) any ρ_{bs} with $\rho_{00;11} = \rho_{11;00} = 0$ violates the fourth relation in the paradox (6). This has completed the proof. □

The paradox (6) and the nonlinear inequality (7) together have provided a nonlinear entanglement witness to successfully verify the bipartite entangled states in a blind manner. In experiment, the inequality (7) is verified according to the paradox (6). Interestingly, different from the standard linear entanglement witness (Horodecki et al., 2009) for any entanglement derived from the Hahn-Banach Theorem, the inequality (7) implies a nonlinear entanglement witness for verifying the non-convex set $\mathcal{S}_{epr}$ (5). Although the present method is constructive for specific sets, it might intrigue general interests beyond the Hahn-Banach Theorem.

Robustness of entanglement witnesses

The generalized GHZ-like paradox (7) of verifying unknown entangled sources is adaptable against white noise. Consider a bipartite noisy Werner state (Werner, 1989) as

$$\rho_v = v\rho_{AB} + \frac{1-v}{4}1, \qquad \text{(Equation 8)}$$

where ρ_{AB} is given in Equation (4), 1 is the identity operator of rank 4, and $v \in [0, 1]$ is the visibility. From Equations (6) and (7), the entanglement of ρ_v is witnessed if it satisfies the following modified entanglement witness (see Method details)

$$\begin{aligned} &\langle \sigma_z \otimes \sigma_x \rangle_{\rho_v} = 0, \\ &\langle \sigma_x \otimes \sigma_z \rangle_{\rho_v} = 0, \\ &4\langle \sigma_x \otimes \sigma_x \rangle_{\rho_v} + \langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} > 1. \end{aligned} \qquad \text{(Equation 9)}$$

The visibilities of white noise, denoted by v*, are shown in Figure 2. There is an evident gap between two curves, indicating the present entanglement witness is more efficient than the CHSH inequality (Clauser et al., 1969) even with known density matrix.

Verifying partially unknown multipartite entanglement

The stabilizer formalism presents a novel way for describing quantum mechanics by using the concepts from group theory, such as the Pauli group (Dehaene and Moor, 2003). This inspires a way for witnessing partially unknown multipartite entanglement using its stabilizer. Specially, for a given n-partite entanglement ensemble $\{|\Psi(\alpha)\rangle\}$ depending on some parameter $\alpha \in \mathbb{R}$ on Hilbert space $\otimes_{j=1}^{n} \mathcal{H}_{A_j}$, a generalized GHZ-like paradox for quantum entanglement is built as

$$\begin{aligned} &\langle g_j \rangle_{|\Psi(\theta)\rangle} = \pm 1, \ (j = 1, \cdots, N), \\ &\langle w \rangle_{|\Psi(\theta)\rangle} \neq 0, \end{aligned} \qquad \text{(Equation 10)}$$

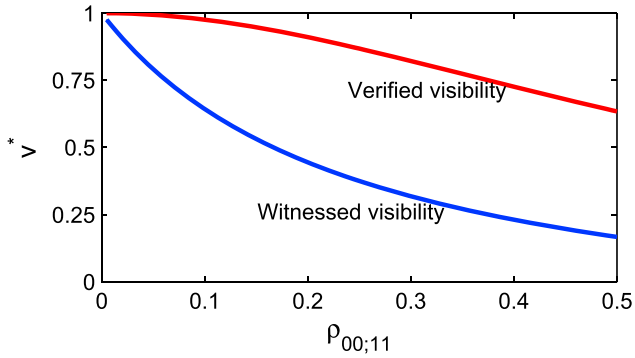


Figure 2. Visibility for white noise

The blue line denotes the critical visibility $v* = 1/(4|\rho_{00;11}| + 1)$ by using the entanglement witness (9) without unknown $\rho_{00;11}$. The red line denotes the visibility given by $v^* = 1/\sqrt{1+4|\rho_{00;11}|^2}$, which is verified by the CHSH inequality (Clauser et al., 1969) with known $\rho_{00;11}$.

where w is an entanglement witness operator (Horodecki et al., 2009), which satisfies $\langle w\rangle_{\rho_{sep}} = 0$ for any bi-separable state ρ_{sep} (Svetlichny, 1987), and $\{g_1, \ldots, g_N\}$ are simultaneous stabilizers of $|\Psi(\alpha)\rangle$'s. Specially, w may be defined by

$$w \in \left\{ \pm|\Psi(\alpha)\rangle\langle\Psi(\alpha)| + \sum_j q_j|\Phi_j\rangle\langle\Phi_j| \right\}, \qquad \text{(Equation 11)}$$

where $\{|\Psi(\alpha)\rangle, |\Phi_j\rangle, \forall j\}$ is an orthogonal basis of specific Hilbert space. The witness operator w may be separable for special q_j's.

One example is an m-partite entanglement given by

$$\rho_{A_1\cdots A_n} = \mathcal{E}(|\Psi(\theta)\rangle\langle\Psi(\theta)|) \qquad \text{(Equation 12)}$$

On Hilbert space $\otimes_{j=1}^n \mathcal{H}_{A_j}$, where $|\Psi(\theta)\rangle$ is a generalized GHZ state (Greenberger et al., 1989) defined by

$$|\Psi(\theta)\rangle_{A_1\cdots A_n} = \cos\theta|0\rangle^{\otimes n} + \sin\theta|1\rangle^{\otimes n} \qquad \text{(Equation 13)}$$

with $\theta \in (0,\pi)$, and $\mathcal{E}(\bullet)$ is a blind quantum channel defined by $\mathcal{E}(\varrho) = \sum p_j(\otimes_{k=1}^n U_j^{(k)})\varrho(\otimes_{k=1}^n U_j^{(k)})^\dagger$, $U_j^{(k)} = e^{i\theta_{jk}}|0\rangle\langle 0| + e^{i\vartheta_{jk}}|1\rangle\langle 1|$ with unknown parameters $\theta_{jk}, \vartheta_{jk} \in (0,\pi)$, and $\{p_j\}$ is unknown probability distribution. This is regarded as *the multipartite GHZ-type entanglement*. A generalized GHZ-like paradox for the entanglement (12) is given by

$$\begin{aligned}
&\langle\sigma_z^{(1)} \otimes \sigma_z^{(n)}\rangle_\rho = 1,\\
&\langle\sigma_z^{(j)} \otimes \sigma_z^{(j+1)}\rangle_\rho = 1,\\
&\langle\sigma_z^{(1)} \otimes \sigma_x^{(n)}\rangle_\rho = 0,\\
&\langle\sigma_z^{(j)} \otimes \sigma_x^{(j+1)}\rangle_\rho = 0,\\
&\langle\sigma_x^{(1)} \otimes \sigma_z^{(n)}\rangle_\rho = 0,\\
&\langle\sigma_x^{(j)} \otimes \sigma_z^{(j+1)}\rangle_\rho = 0,\ (j = 1, \cdots, n-1),\\
&\langle\otimes_{k=1}^n \sigma_x^{(k)}\rangle_\rho \overset{\text{ES}}{\neq} 0,
\end{aligned} \qquad \text{(Equation 14)}$$

where $\sigma_z^{(j)}$ denotes the Pauli matrix σ_z being performed by the j-th party. This paradox reduces to the bipartite paradox (6) when n = 2. For the n-qubit scenarios, denote $\mathcal{S}_{ghz} = \{\mathcal{E}(|\Psi(\theta)\rangle\langle\Psi(\theta)|), \forall|\Psi(\theta)\rangle, \mathcal{E}(\bullet)\}$. We have the following Theorem 2 (see Method details).

Theorem 2. The entanglement set $\mathcal{S}_{ghz}$ is verifiable

Another example is to verify a W-type entanglement set $\mathcal{S}_w = \{\mathcal{E}(|\Phi\rangle\langle\Phi|), \forall|\Phi\rangle, \mathcal{E}(\bullet)\}$ (see Method details), where $|\Phi\rangle = a_0|001\rangle + a_1|010\rangle + a_2|100\rangle + a_3|111\rangle$ (Dür et al., 2000) on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, a_j are real parameters satisfying $\sum_{j=0}^3 a_j^2 = 1$, and $\mathcal{E}(\bullet)$ is defined in Equation (12).

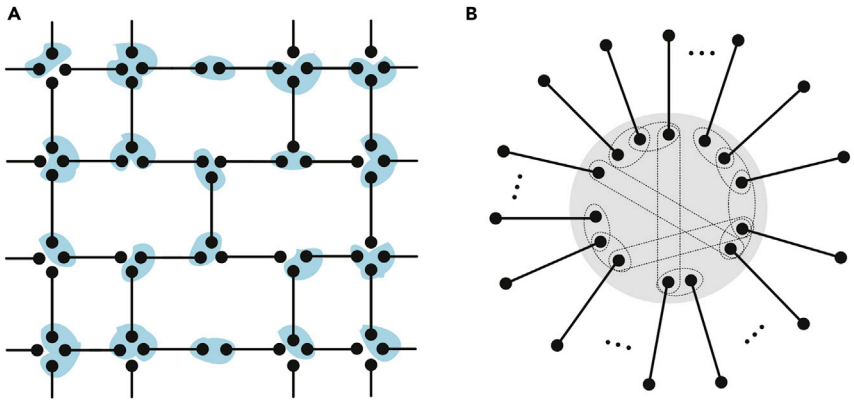


Figure 3. Schematic cluster states generated by quantum networks

(A) A general quantum network consisting of unknown EPR-type sources. Each green area denotes one controlled phase operation on two qubits.

(B) An equivalent star-shaped quantum network.

In the following, let us discuss two applications.

Verifying partially unknown universal computation resources

The one-way quantum computer (Raussendorf and Briegel, 2001) is realized by measuring individual qubits of a highly entangled multiparticle state in a temporal sequence. The involved cluster state provides a universal resource for quantum computation. One easy way to generate cluster states is from quantum networks (den Nest et al., 2006; Wei et al., 2011) by using local two-qubit controlled-phase operations $CP(\theta) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$. Specially, consider a connected quantum network $\mathcal{N}_q$ consisting of $A_1, \cdots, A_n$, where each party shares the entanglement (2) or (13) with others. The connectedness means that for any pair of A_i and A_j there is a chain subnetwork $\mathcal{N}_{ij}$ consisting of $A_i, A_{i_1}, \cdots, A_{i_s}, A_j$ satisfying any adjacent two parties share some entangled states. These multipartite entangled states can be in whole verified by using Bell inequalities (Gühne et al., 2005; Luo, 2021a, 2021b), entanglement witness (Jungnitsch et al., 2011), or GHZ-type paradoxes (Scarani et al., 2005; Tang et al., 2013; Liu et al., 2021). Instead, the goal here is to witness partially unknown cluster states generated by entangled states (2) and (13) under blind channels. Let the set $\mathcal{S}_{cl}$ consist of all cluster states generated from quantum network $\mathcal{N}_q$ in the state $\rho_{\mathcal{G}}$, that is, $\mathcal{S}_{cl} = \{\mathcal{E} \circ \mathcal{C}(\rho_{\mathcal{G}}), \forall \rho_{\mathcal{G}}, \mathcal{E}(\bullet)\}$, where $\mathcal{E}(\bullet)$ is defined in Equation (12), and $\mathcal{C}(\bullet)$ is a blind unitary transformation defined by $\otimes_{j\in\mathcal{G}} CP(\theta_j)$ with unknown $\theta_j \in (0, \pi)$. The set $\mathcal{S}_{cl}$ is unique because $\mathcal{E}(\bullet)$ and $\mathcal{C}(\bullet)$ are commutative. We have the following *Theorem 3* (see Method details).

Theorem 3

The entanglement set $\mathcal{S}_{cl}$ is verifiable.

For the EPR-type state (3) or GHZ-type state (12), the controlling and controlled qubits in the two-qubit operation $CP(\theta) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$ can be swapped. The symmetry allows for reshaping $\mathcal{N}_q$ in Figure 3A into a star-shaped network, as Figure 3B, in which all $CP(\theta)$'s are performed by the center party. The new network is easy for proving the universality of generated entangled states (Wei et al., 2011). Thus Theorem three provides a blind witness of universal quantum computation resources without the state tomography beyond previous results (Gühne et al., 2005; Jungnitsch et al., 2011; Scarani et al., 2005; Tang et al., 2013; Liu et al., 2021).

Zero-knowledge proof of partially unknown quantum entangled source

Classical zero-knowledge proof provides an interesting protocol to prove special hard problems without leaking its information (Goldwasser et al., 1989; Goldreich and Oren, 1994). It is of a cryptographic primitive in secure multiparty computation. The quantum versions take use of entangled states. So far, most results have focused on extensions of classical tasks (Watrous, 2002) or entangled provers (Ito and Vidick, 2012; Ji, 2017; Grilo et al., 2019); however, our proposed method proves a quantum information task, that is, verifying an entanglement (3) (for example) without leaking knowledge of mixture probability distribution

$\{p_j\}$ and parametersθ_j's. One simple protocol is elaborated as following four steps: (i) The prover prepares N copies of EPR-type entanglement (3), i.e., $\otimes_{j=1}^{N}\rho_{A_jB_j}$, and sends the qubit series $B_1,\cdots,B_N$ to the verifier. (ii) The verifier challenges with a random bit series $k_1,\cdots,k_N\in\{0,1\}$. (iii) The prover complies with $a_1,\cdots,a_N\in\{\pm1\}$, where a_j denotes the outcome on qubit A_i by performing Pauli measurement σ_{k_j} with$\sigma_0 := \sigma_x$ and $\sigma_1 := \sigma_z$. (iv) The verifier performs the measurement on qubit B_j with Pauli observable $\sigma_{s_j}\in\{\sigma_x,\sigma_z\}$ under the uniform distribution. The proof is true if all the joint statistics of $\langle\sigma_{k_j}\otimes\sigma_{s_j}\rangle_{\rho_{A_jB_j}}$ satisfy the paradox (6) under the assumptions of ideal Pauli measurement devices. Otherwise, it is false. The verifier can only access the partial particle, which implies a difficult problem for the verifier to complete the task without the help of a prover. The *completeness* is followed from Theorem 1, that is, the prover can convince the verifier's result. A malicious prover, who prepares another entanglement beyond the one in Equation (3) or separable state, cannot convince the verifier's verification because he cannot forage measurement outcomes of challenges before the random measurements $\sigma_{s_1},\cdots,\sigma_{s_N}$. This yields *soundness*. Besides, a malicious verifier can only learn the decomposition (4) of its density matrix, which leaks no useful information of $\{p_j\}$ and parameters θ_j's. This follows the *zero-knowledge*. A more rigid analysis requires formal cryptographic models beyond the scope of this paper. The protocol may be extended for multiparty by using the GHZ-type entanglement (12). Those examples may inspire interesting applications in cryptography.

DISCUSSION

In this paper, we have investigated unknown entangled states with limited information of its state subspace. We proposed a generalized GHZ-like paradox for verifying an entanglement set consisting of unknown bipartite entangled states using only Pauli observables. This allows a blind entanglement verification assisted by a nonlinear entanglement witness in a device-independent manner. We further verified an entanglement set consisting of unknown multipartite entangled states such as multipartite GHZ-type entanglement and cluster states from quantum networks. This provides a useful method for verifying universal quantum computation resources blindly. The present results should be interesting in entanglement theory, Bell theory, and quantum communication.

The well-known Bell theory and entanglement witness are designed for detecting given entanglement. Our method is designed for unknown entanglement without the state tomography. This intrigues a new problem of verifying specific sets consisting of entangled states. It may be regarded as entanglement verification in adversary scenarios where the given entanglement passes through a blind channel of black-box device controlled by adversaries. The present results hold for special sources in generalized EPR states or multipartite GHZ states. It can be extended to high-dimensional EPR-type or GHZ-type entangled states (see Method details). This motivates a general problem for other entangled sources (Dicke, 1954; Luo, 2021a, 2021b) or entangled subspaces (Baccari et al., 2020). Another interesting problem is to find new applications specially in cryptography with specific entanglement sets. In addition, it is unknown what kind of information is necessary for verifying a general set consisting of all entangled states. This might intrigue new entanglement models.

Limitations of the study

This paper is aimed to verify the entangled ensemble. The main limitation of the proposed method is from the simultaneous stabilizers. This requires all the involved states being in a specific subspace. Another is the nonconvexity of the involved subspace, which requires in principle nonlinear entanglement witnesses, or a set of linear witnesses.

STAR★METHODS

Detailed methods are provided in the online version of this paper and include the following:

- KEY RESOURCES TABLE
- RESOURCE AVAILABILITY
  - Lead contact
  - Materials availability
  - Data and code availability
- METHOD DETAILS
  - Proof of Lemma 1
  - Robustness of bipartite entanglement witness

- Proof of Theorem 2
- Witnessing unknown entanglement set S_{ghz}
- Verifying the nonlocality
- Robustness against white noise
- Nonlocality verified by violating the Svetlichny inequality
- Verifying unknown W-type entanglement
- Proof of Theorem 3
- Verifying high-dimensional unknown GHZ-type entanglement
- Bipartite entanglement
- Multipartite entanglement
- Theorem 5

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grants Nos. 62172341, 61303039, 12171044, 12075159, 11875167, and 12075001), Beijing Natural Science Foundation (Grant No. Z190005), Academy for Multidisciplinary Studies, Capital Normal University, Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology (Grant Nos. SIQSE202001, SIQSE202105), and the Academician Innovation Platform of Hainan Province.

AUTHOR CONTRIBUTIONS

M.X. conceived the study. M.X., S.M., and J.L. wrote the manuscript. All authors reviewed and critically revised the manuscript.

DECLARATION OF INTERESTS

The authors declare no competing interests.

Received: December 2, 2021
Revised: February 6, 2022
Accepted: February 17, 2022
Published: March 18, 2022

REFERENCES

Amico, L., Fazio, R., Osterloh, A., and Vedral, V. (2008). Entanglement in many-body systems. Rev. Mod. Phys. *80*, 517–576. https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.80.517.

Baccari, F., Augusiak, R., Supic, I., and Acín, A. (2020). Device-independent certification of genuinely entangled subspaces. Phys. Rev. Lett. *125*, 260507. https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.125.260507.

Bell, J.S. (1964). On the Einstein-Podolsky-Rosen paradox. Phys *1*, 195. https://journals.aps.org/ppf/pdf/10.1103/PhysicsPhysiqueFizika.1.195.

Broadbent, A., Fitzsimons, J., and Kashefi, E. (2009). Universal blind quantum computation. In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer (IEEE Computer society), pp. 517–527.

Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V., and Wehner, S. (2014). Bell nonlocality. Rev. Mod. Phys. *86*, 419. https://link.aps.org/doi/10.1103/RevModPhys.86.419.

Clauser, J.F., Horne, M.A., Shimony, A., and Holt, R.A. (1969). Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. *23*, 880–884. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.23.880.

Dehaene, J., and Moor, B.D. (2003). Normal forms and entanglement measures for multipartite quantum states. Phys. Rev. A. *68*, 042318. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.68.012103.

Dicke, R.H. (1954). Coherence in spontaneous radiation processes. Phys. Rev. *93*, 99–110. https://link.aps.org/doi/10.1103/PhysRev.93.99.

Dür, W., Vidal, G., and Cirac, J.I. (2000). Three qubits can be entangled in two inequivalent ways. Phys. Rev. A. *62*, 062314. https://link.aps.org/doi/10.1103/PhysRevA.62.062314.

Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum mechanical description of physical reality be considered complete? Phys. Rev. *47*, 777–780. https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777.

Gisin, N. (1991). Bell's inequality holds for all non-product states. Phys. Lett. A. *154*, 201. https://www.sciencedirect.com/science/article/abs/pii/037596019190805I.

Goldreich, O., and Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. J. Crypt. *7*, 1–32. https://doi.org/10.1007/BF00195207.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proofs. SIAM J. Comput. *18*, 186–208. https://epubs.siam.org/doi/abs/10.1137/0218012.

Greenberger, D.M., Horne, M.A., and Zeilinger, A. (1989). Going beyond Bell's theorem. In Bell's Theorem, Quantum Theory and Conceptions of the Universe, M. Kafatos, ed. (Kluwer), pp. 69–72.

Grilo, A.B., Slofstra, W., and Yuen, H. (2019). Perfect zero knowledge for quantum multiprover interactive proofs. In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), p. 611.

Gühne, O., and Seevinck, M. (2010). Separability criteria for genuine multiparticle entanglement. New J. Phys. *12*, 053002. https://iopscience.iop.org/article/10.1088/1367-2630/12/5/053002/meta.

Gühne, O., and Tóth, G. (2009). Entanglement detection. Phys. Rep. *474*, 1–75. https://www.sciencedirect.com/science/article/abs/pii/S0370157309000623.

Gühne, O., Tóth, G., Hyllus, P., and Briegel, H.J. (2005). Bell inequalities for graph states. Phys.

Rev. Lett. *95*, 120405. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.95.120405.

Horodecki, K., Horodecki, M., Horodecki, P., and Oppenheim, J. (2005). Locking entanglement with a single qubit. Phys. Rev. Lett. *94*, 200501. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.94.200501.

Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K. (2009). Quantum entanglement. Rev. Mod. Phys. *81*, 865. https://link.aps.org/doi/10.1103/RevModPhys.81.865.

Ito, T., and Vidick, T. (2012). A multi-prover interactive proof for nexp sound against entangled provers. In 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012), pp. 243–252.

Ji, Z. (2017). Compression of quantum multi-prover interactive proofs. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017), pp. 289–302.

Jungnitsch, B., Moroder, T., and Gühne, O. (2011). Entanglement witnesses for graph states: general theory and examples. Phys. Rev. A. *84*, 032310. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.84.032310.

Laing, A., Scarani, V., Rarity, J.G., and O'Brien, J.L. (2010). Reference frame independent quantum key distribution. Phys. Rev. A. *82*, 012304. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.82.012304.

Lewenstein, M., Kraus, B., Cirac, J.I., and Horodecki, P. (2000). Optimization of entanglement witnesses. Phys. Rev. A *62*, 052310. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.62.052310.

Liu, Z.H., Zhou, J., Meng, H.X., Yang, M., Li, Q., Meng, Y., Su, H., Chen, J.L., Sun, K., Xu, J.S., et al. (2021). Experimental test of the Greenberger-Horne-Zeilinger-type paradoxes in and beyond graph states. Npj Quant. Inf. *7*, 66. https://www.nature.com/articles/s41534-021-00397-z.

Lu, D., Xin, T., Yu, N., Ji, Z., Chen, J., Long, G., Baugh, J., Peng, X., Zeng, B., and Laflamme, R. (2016). Tomography is necessary for universal entanglement detection with single-copy observables. Phys. Rev. Lett. *116*, 230501. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.116.230501.

Luo, M.X. (2021a). Fully device-independent model on quantum networks. Preprint at arXiv, 2106.15840. https://arxiv.org/abs/2106.15840.

Luo, M.X. (2021b). New genuinely multipartite entanglement. Adv. Quan. Tech. *4*, 2000123. https://onlinelibrary.wiley.com/doi/10.1002/qute.202000123.

den Nest, M.V., Miyake, A., Dur, W., and Briegel, H.J. (2006). Universal resources for measurement-based quantum computation. Phys. Rev. Lett. *97*, 150504. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.97.150504.

Raussendorf, R., and Briegel, H.J. (2001). A one-way quantum computer. Phys. Rev. Lett. *86*, 5188. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.86.5188.

Scarani, V., Acin, A., Schenck, E., and Aspelmeyer, M. (2005). Nonlocality of cluster states of qubits. Phys. Rev. A. *71*, 042325. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.71.042325.

Schrödinger, E. (1935). Die gegenwärtige situation in der Quantenmechanik. Naturwissenschaften *23*, 807–812. https://link.springer.com/article/10.1007/BF01491891.

Svetlichny, G. (1987). Distinguishing three-body from two-body nonseparability by a Bell-type inequality. Phys. Rev. D *35*, 3066–3069. https://journals.aps.org/prd/abstract/10.1103/PhysRevD.35.3066.

Tang, W., Yu, S., and Oh, C.H. (2013). Greenberger-Horne-Zeilinger paradoxes from qudit graph states. Phys. Rev. Lett. *110*, 100403. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.110.100403.

Vourdas, A. (2004). Quantum systems with finite Hilbert space. Rep. Prog. Phys. *67*, 267. https://iopscience.iop.org/article/10.1088/0034-4885/67/3/R03/meta.

Watrous, J. (2002). Limits on the power of quantum statistical zero-knowledge. In 43rd Symposium on Foundations of Computer Science (FOCS 2002), p. 459.

Wei, T.-C., Affleck, I., and Raussendorf, R. (2011). Affleck-Kennedy-Lieb-Tasaki State on a Honeycomb lattice is a universal quantum computational resource. Phys. Rev. Lett. *106*, 070501. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.106.070501.

Werner, R.F. (1989). Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Phys. Rev. A. *40*, 4277. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.40.4277.

Weyl, H. (2014). The Theory of Groups and Quantum Mechanics (Martino Fine Books), Ch.III.

Wiseman, H.M., Jones, S.J., and Doherty, A.C. (2007). Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. Phys. Rev. Lett. *98*, 140402. http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.98.140402.

STAR★METHODS

KEY RESOURCES TABLE

REAGENT or RESOURCE	SOURCE	IDENTIFIER
Other		
EPR steering	Einstein et al. (1935)	N/A
Entanglement	Horodecki et al. (2009)	N/A
Bell nonlocality	Bell (1964)	N/A
GHZ paradox	Greenberger et al. (1989)	N/A
Entangled subspace	Baccari et al. (2020)	N/A
Entanglement set	This paper	N/A

RESOURCE AVAILABILITY

Lead contact

Further information and requests for resources should be directed to the lead contact Ming-Xing Luo (mxluo@swjtu.edu.cn).

Materials availability

This study did not generate new materials.

Data and code availability

This study has no data and code available.

METHOD DETAILS

Proof of Lemma 1

Lemma 1. For any two-qubit state ρ on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$, the following inequality holds

$$2\sqrt{\rho_{00;11}\rho_{11;00}}+\rho_{00;00}+\rho_{11;11}-1\leq 0, \qquad \text{(Equation 15)}$$

if and only if ρ_{AB} is separable, where $\rho_{ij;ks}$ denote density matrix components of ρ_{AB}, that is, $\rho_{AB}=\sum_{i,j,k,s}\rho_{ij;ks}|ij\rangle\langle ks|$.

Proof. Let us consider an arbitrary separable two-qubit pure state $|\Phi\rangle_{AB}=|\varphi_1\rangle_A|\varphi_2\rangle_B$ on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ with $|\varphi_j\rangle=\cos\theta_j|0\rangle+\sin\theta_j|1\rangle, \theta_j\in(0,\pi), j=1,2$. It follows that $\rho_{00;11}=\cos\theta_1\sin\theta_1\cos\theta_2\sin\theta_2$, and $\rho_{01;01}\rho_{10;10}=(\cos\theta_1\sin\theta_1\cos\theta_2\sin\theta_2)^2$. From the Hermitian symmetry of the density matrix ρ, it implies

$$2\left|\rho_{00;11}\right|=2\sqrt{\rho_{01;01}\rho_{10;10}}\leq\rho_{01;01}+\rho_{10;10}, \qquad \text{(Equation 16)}$$

where the last inequality is due to the Cauchy-Schwarz inequality of $2\sqrt{|xy|}\leq x^2+y^2$.

Consider an arbitrary mixed separable state on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ given by

$$\rho_{AB}=\sum_i p_i|\Phi_i\rangle_{AB}\langle\Phi_i|:=\sum_{j_1,j_2,k_1,k_2}\rho_{j_1j_2;k_1k_2}|j_1j_2\rangle\langle k_1k_2|=\sum_i p_i\sum_{j_1,j_2,k_1,k_2}\rho^{(i)}_{j_1j_2;k_1k_2}|j_1j_2\rangle\langle k_1k_2|, \qquad \text{(Equation 17)}$$

where $|\Phi_i\rangle_{AB}$ are separable pure states defined by $\rho^{(i)}_{j_1j_2;s_1s_2}=|\Phi_i\rangle\langle\Phi_i|$, and$\{p_i\}$ is a probability distribution. From Equation (17) we get

$$\begin{aligned}2\sqrt{\rho_{00;11}\rho_{11;00}}&=2\left|\rho_{00;11}\right|\\&=2\left|\sum_i p_i\rho^{(i)}_{00;11}\right|\\&\leq 2\sum_i p_i\left|\rho^{(i)}_{00;11}\right|\end{aligned} \qquad \text{(Equation 18)}$$

$$\leq\sum_i p_i\left(\rho^{(i)}_{01;01}+\rho^{(i)}_{10;10}\right) \qquad \text{(Equation 19)}$$

$$= \rho_{01;01} + \rho_{10;10} \quad \text{(Equation 20)}$$
$$= 1 - \rho_{00;00} - \rho_{11;11}. \quad \text{(Equation 21)}$$

The inequality (18) is followed from the convexity of function $f(x) = |x|$. The inequality (19) is followed from the inequality (16). The equality (20) is from Equation (17). Equation (21) follows the trace equality of $Tr\rho = 1$. Thus we have successfully proved the inequality (15). □

Robustness of bipartite entanglement witness

Consider a bipartite state with white noise on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is given by

$$\rho_v = v\rho_{AB} + \frac{1-v}{4}1, \quad \text{(Equation 22)}$$

where 1 is the rank-4 identity operator on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and $v \in [0, 1]$. and $v \in [0, 1]$. For the noisy state ρ_v, the density matrix is given by

$$\rho_v = \begin{pmatrix} \frac{1-v}{4} + v\rho_{00;00} & 0 & 0 & v\rho_{00;11} \\ 0 & \frac{1-v}{4} & 0 & 0 \\ 0 & 0 & \frac{1-v}{4} & 0 \\ v\rho_{00;11} & 0 & 0 & \frac{1-v}{4} + v\rho_{11,11} \end{pmatrix},$$

where $\rho_{00;00}$ and $\rho_{11;11}$ satisfies $\rho_{00;00}, \rho_{11;11} \geq 0$ and $\rho_{00;00} + \rho_{11;11} = 1$, and $\rho_{00;11} \geq 0$ (for simplicity, let us take $\rho_{00;11}$ as a real number). From Lemma 1, ρ_v is a bipartite entanglement if v satisfies the following inequality

$$v > \frac{1}{1 + 4\rho_{00;11}}. \quad \text{(Equation 23)}$$

For two observables $\sigma_z \otimes \sigma_x$ and $\sigma_x \otimes \sigma_z$, from Eq. (Robustness of bipartite entanglement witness) it is easy to prove that ρ_v satisfies

$$\langle \sigma_z \otimes \sigma_x \rangle_{\rho_v} = 0, \quad \text{(Equation 24)}$$
$$\langle \sigma_x \otimes \sigma_z \rangle_{\rho_v} = 0. \quad \text{(Equation 25)}$$

Similarly, for two observables $\sigma_z \otimes \sigma_z$ and $\sigma_x \otimes \sigma_x$, from Eq. (Robustness of bipartite entanglement witness) it follows that

$$\langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} = v, \quad \text{(Equation 26)}$$
$$\langle \sigma_x \otimes \sigma_x \rangle_{\rho_v} = 2v\rho_{00;11}. \quad \text{(Equation 27)}$$

So, combining Equations 24–27 and the inequality (23), ρ_v is entangled if it satisfies the following statements as

$$\begin{aligned} &\langle \sigma_z \otimes \sigma_x \rangle_{\rho_v} = 0, \\ &\langle \sigma_x \otimes \sigma_z \rangle_{\rho_v} = 0, \\ &2\langle \sigma_x \otimes \sigma_x \rangle_{\rho_v} + \langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} > 1. \end{aligned} \quad \text{(Equation 28)}$$

This has completed the proof.

Proof of Theorem 2

In this section we prove Theorem 2. The first subsection is for witnessing the unknown entanglement by using present generalized GHZ-type paradox (13) in the main text. The second subsection is for verifying the nonlocality. The third subsection is for the robustness against white noise while the last section is for verifying noisy state using the Svetlichny inequality.

Witnessing unknown entanglement set $\mathcal{S}_{ghz}$

Similar to Lemma 1, we prove the following Lemma.

Lemma 2. For any n-qubit biseparable state ρ on Hilbert space $\otimes_{j=1}^{n} \mathcal{H}_{A_j}$, the following inequality holds

$$2\sqrt{\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n}}+\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}+\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}-1\le 0, \quad \text{(Equation 29)}$$

where $\overrightarrow{0}_n$ and $\overrightarrow{1}_n$ denote respectively n-bit series $0\cdots0$ and $1\cdots1$, and $\rho_{\overrightarrow{i}_n;\overrightarrow{j}_n}$ are density matrix components defined by $\rho_{A_1\cdots A_n}=\sum_{i_1,\cdots,i_n,j_1,\cdots,j_n}\rho_{i_1\cdots i_n;j_1\cdots j_n}|i_1\cdots i_n\rangle\langle j_1\cdots j_n|$.

Proof of Lemma 2. The proof is similar to Lemma 1 and a recent method (Gühne and Seevinck, 2010). Consider an arbitrary biseparable pure state (Svetlichny, 1987) on Hilbert space $\otimes_{j=1}^{n}\mathcal{H}_{A_j}$ given by

$$|\Psi\rangle_{A_1\cdots A_n}=|\psi_1\rangle|\psi_2\rangle \quad \text{(Equation 30)}$$

where $|\psi_1\rangle_{A_1\cdots A_s}=\sum_{j_1,\cdots j_s}\alpha_{j_1\cdots j_s}|j_1\cdots j_s\rangle$ is a s-qubit pure state on Hilbert space $\otimes_{j=1}^{s}\mathcal{H}_{A_j}$ and $|\psi_2\rangle_{A_{s+1}\cdots A_n}=\sum_{j_{s+1},\cdots j_n}\beta_{j_{s+1}\cdots j_n}|j_{s+1}\cdots j_n\rangle$ and $|\psi_2\rangle_{A_{s+1}\cdots A_n}=\sum_{j_{s+1},\cdots j_n}\beta_{j_{s+1}\cdots j_n}|j_{s+1}\cdots j_n\rangle$ is an $n-s$-qubit pure state on Hilbert space $\otimes_{j=s+1}^{n}\mathcal{H}_{A_j}$. It follows that

$$|\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}|=|\alpha_{\overrightarrow{0}_s}\alpha_{\overrightarrow{1}_s}\beta_{\overrightarrow{0}_{n-s}}\beta_{\overrightarrow{1}_{n-s}}|=\sqrt{\rho_{\overrightarrow{0}_s\overrightarrow{1}_{n-s};\overrightarrow{0}_s\overrightarrow{1}_{n-s}}\times\rho_{\overrightarrow{1}_s\overrightarrow{0}_{n-s};\overrightarrow{1}_s\overrightarrow{0}_{n-s}}}. \quad \text{(Equation 31)}$$

This implies that

$$2|\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}|=2\sqrt{\rho_{\overrightarrow{0}_s\overrightarrow{1}_{n-s};\overrightarrow{0}_s\overrightarrow{1}_{n-s}}\rho_{\overrightarrow{1}_s\overrightarrow{0}_{n-s};\overrightarrow{1}_s\overrightarrow{0}_{n-s}}}\le\rho_{\overrightarrow{0}_s\overrightarrow{1}_{n-s};\overrightarrow{0}_s\overrightarrow{1}_{n-s}}+\rho_{\overrightarrow{1}_s\overrightarrow{0}_{n-s};\overrightarrow{1}_s\overrightarrow{0}_{n-s}}\le 1-\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}. \quad \text{(Equation 32)}$$

Here, the inequality (32) is followed from the Cauchy-Schwarz inequality of $2|ab|\le a^2+b^2$, and the inequality (32) has used the inequality of $\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}+\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}+\rho_{\overrightarrow{0}_s\overrightarrow{1}_{n-s};\overrightarrow{0}_s\overrightarrow{1}_{n-s}}+\rho_{\overrightarrow{1}_s\overrightarrow{0}_{n-s};\overrightarrow{1}_s\overrightarrow{0}_{n-s}}\le 1$, $\overrightarrow{0}_m$(or $\overrightarrow{1}_m$) denotes m-bit series $0\cdots0$(or$1\cdots1$).

Similarly, we can prove the inequality (32) for any mixed biseparable state in Equation (30) in terms of each bipartition of $\{A_1,\cdots,A_n\}$. In what follows, consider a biseparable mixed state ρ_{bs} on Hilbert space $\otimes_{j=1}^{n}\mathcal{H}_{A_j}$ as

$$\rho_{bs}=\sum_i p_i|\Psi_i\rangle_{A_1\cdots A_n}\langle\Psi_i|=\sum_{\substack{j_1,\cdots j_n\\k_1,\cdots,k_n}}\rho_{j_1\cdots j_n;k_1\cdots k_n}|j_1\cdots j_n\rangle\langle k_1\cdots k_n|=\sum_i p_i\sum_{\substack{j_1,\cdots j_n\\k_1,\cdots,k_n}}\rho^{(i)}_{j_1\cdots j_n;k_1\cdots k_n}|j_1\cdots j_n\rangle\langle k_1\cdots k_n| \quad \text{(Equation 33)}$$

where $|\Psi_i\rangle$ are biseparable pure states defined in Equation (30) with density matrices $|\Psi_i\rangle_{A_1\cdots A_n}\langle\Psi_i|:=\sum_{j_1,\cdots j_n,k_1,\cdots,k_n}\rho^{(i)}_{j_1\cdots j_n;k_1\cdots k_n}|j_1\cdots j_n\rangle\langle k_1\cdots k_n|$. From the inequality (32), it follows that

$$\begin{aligned}2\sqrt{\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n}}&=2\left|\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\right| \quad \text{(Equation 34)}\\&=2\left|\sum_i p_i\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{1}_n}\right|\\&\le 2\sum_i p_i\left|\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{1}_n}\right|\\&\le\sum_i p_i\left|1-\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho^{(i)}_{\overrightarrow{1}_n;\overrightarrow{1}_n}\right| \quad \text{(Equation 35)}\\&=\sum_i p_i\left(1-\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho^{(i)}_{\overrightarrow{1}_n;\overrightarrow{1}_n}\right) \quad \text{(Equation 36)}\\&=1-\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}. \quad \text{(Equation 37)}\end{aligned}$$

Here, the inequality (34) is followed from the convexity of the function $f(x)=|x|$. The inequality (35) is from the inequality (32). The inequality (36) is obtained from the equality: $\left|1-\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}{}^{(i)}\right|=1-\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n}-\rho^{(i)}_{\overrightarrow{1}_n;\overrightarrow{1}_n}$ because $\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n},\rho^{(i)}_{\overrightarrow{1}_n;\overrightarrow{1}_n}\ge 0$ and $\rho^{(i)}_{\overrightarrow{0}_n;\overrightarrow{0}_n}+\rho^{(i)}_{\overrightarrow{1}_n;\overrightarrow{1}_n}\le 1$. The equality (37) is from Equation (33). This has proved the inequality (29). □

Now, continue to prove Theorem 2. The generalized GHZ-type entangled state reads

$$\rho_{A_1\cdots A_n} = \mathcal{E}(|\Phi(\theta)\rangle\langle\Phi(\theta)|), \quad \text{(Equation 38)}$$

where $|\Phi(\theta)\rangle$ is a generalized GHZ state given by

$$|\Phi(\theta)\rangle_{A_1\cdots A_n} = \cos\theta|0\rangle^{\otimes n} + \sin\theta|1\rangle^{\otimes n}, \quad \text{(Equation 39)}$$

with $\theta\in(0,\frac{\pi}{2})$ and $\mathcal{E}(\bullet)$ is local phase transformation defined by $\mathcal{E}(\rho)=\sum p_j(\otimes_{k=1}^n U_{jk})\rho(\otimes_{k=1}^n U_{jk}^\dagger)$, $U_{jk}=e^{i\theta_{jk}}|0\rangle\langle 0|+e^{i\vartheta_{jk}}|1\rangle\langle 1|$ with unknown parameters $\theta_{jk},\vartheta_{jk}\in(0,\pi)$, and any unknown probability distribution $\{p_j\}$. With these notions, the entanglement set $\mathcal{S}_{ghz}$ is given by

$$\mathcal{S}_{ghz} = \{\rho, \forall|\Phi(\theta)\rangle, \mathcal{E}(\bullet)\} \quad \text{(Equation 40)}$$

The goal is to witness the entanglement set $\mathcal{S}_{ghz}$ by using the generalized GHZ-like paradox (13) in the main text and Lemma 2.

We firstly prove that any entanglement $\rho\in\mathcal{S}_{ghz}$ satisfies the paradox (13). In fact, it is forward to check any entangled state in Equation (38) satisfies the first three equalities of the paradox (14) from the fact that $|\Phi(\theta)\rangle_{A_1\cdots A_n}$ in Equation (39) satisfies these equalities for any $\theta\in(0,\pi)$.

For any state $\rho_{A_1\cdots A_n}\in\mathcal{S}_{ghz}$, it is rewritten into

$$\begin{aligned}\rho_{A_1\cdots A_n} = {} & \rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}\left|\overrightarrow{0}_n\right\rangle\left\langle\overrightarrow{0}_n\right| + \rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\left|\overrightarrow{0}_n\right\rangle\left\langle\overrightarrow{1}_n\right| \\ & + \rho_{\overrightarrow{1}_n;\overrightarrow{0}_n}\left|\overrightarrow{1}_n\right\rangle\left\langle\overrightarrow{0}_n\right| + \rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}\left|\overrightarrow{1}_n\right\rangle\left\langle\overrightarrow{1}_n\right|\end{aligned} \quad \text{(Equation 41)}$$

where $\{\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n},\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}\}$ is a probability distribution, and $\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}=\rho^*_{\overrightarrow{1}_n;\overrightarrow{0}_n}$. From Lemma 2, ρ is an n-partite entanglement in the biseparable model (Svetlichny, 1987) if $\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\neq 0$. Otherwise, ρ is a biseparable state with the following decomposition

$$\rho=\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}\left|\overrightarrow{0}_n\right\rangle\left\langle\overrightarrow{0}_n\right| + \rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}\left|\overrightarrow{1}_n\right\rangle\left\langle\overrightarrow{1}_n\right| = \sum_i p_i(|\Phi(\theta_i)\rangle\langle\Phi(\theta_i)| + |\Phi(\theta_i)^\perp\rangle\langle\Phi(\theta_i)^\perp|) \quad \text{(Equation 42)}$$

where $\{|\Phi(\theta_i)\rangle,|\Phi(\theta_i)^\perp\rangle\}$ are orthogonal states for any θ_i. This further implies that the inequality (29) is sufficient and necessary for witnessing the entanglement set $\mathcal{S}_{ghz}$. Hence, any state in $\mathcal{S}_{ghz}$ is an n-partite entanglement if and only if the paradox (13) holds.

In the following, we prove any biseparable state violates one statement in the paradox (13). In fact, consider an n-qubit biseparable pure state $|\Phi\rangle_{A_1\cdots A_n}=|\varphi\rangle_{A_1\cdots A_k}|\psi\rangle_{A_{k+1}\cdots A_n}$ on Hilbert space $\otimes_{j=1}^n\mathcal{H}_{A_j}$. From all the equalities of the paradox (13), $|\varphi\rangle$ is represented by the state $|0\rangle^{\otimes k}$ or $|1\rangle^{\otimes k}$ while $|\psi\rangle$ is represented by the state $|0\rangle^{\otimes n-k}$ or $|1\rangle^{\otimes n-k}$. $|1\rangle^{\otimes n-k}$ Otherwise, $|\Phi\rangle$ will violate one statement in the paradox (13). Generally, consider a general n-qubit mixed biseparable state ρ_{bs} on Hilbert space $\otimes_{j=1}^n\mathcal{H}_{A_j}$ given by

$$\rho_{bs} = \sum_{jk} p_{jk}\rho_j^{(I)}\otimes\rho_k^{(\bar{I})} \quad \text{(Equation 43)}$$

where $\rho_j^{(I)}$ denote pure states of the systems in the set $I\subset\{A_1,\cdots,A_n\}$, $\rho_k^{(\bar{I})}$ denote pure states of the systems in the complement set $\bar{I}=\{A_1,\cdots,A_n\}-I$, and $\{p_{jk}\}$ is a probability distribution. So, ρ_{bs} can only be a diagonal state given by

$$\rho_{bs} = p_0\left|\overrightarrow{0}_n\right\rangle_{A_1\cdots A_n}\left\langle\overrightarrow{0}_n\right| + p_1\left|\overrightarrow{1}_n\right\rangle_{A_1\cdots A_n}\left\langle\overrightarrow{1}_n\right| \quad \text{(Equation 44)}$$

if all the equalities in the paradox (13) hold. This implies $\langle\sigma_x^{(1)}\otimes\cdots\otimes\sigma_x^{(n)}\rangle_{\rho_{bs}}=0$, that is , ρ_{bs} violates the last inequality of the paradox (13). So, any biseparable state violates either one equality or the last inequality of the paradox (13).

Verifying the nonlocality

We verify the nonlocality by using the generalized GHZ-type paradox (13). Denote the supposedly definite real values of $v_{j,z}$ and $v_{j,x}$ for the j-th party, with $v_{j,x},v_{j,z}\in(1,-1)$ beyond the integers in the standard GHZ paradox (Greenberger et al., 1989), $j=1,\cdots,n$.. Similar to the analysis of the GHZ paradox, classically we have from the first two statements in Equation (13) that

$$v_{j,z} \in \{\pm 1\}, (j = 1, \cdots, n). \quad \text{(Equation 45)}$$

Moreover, combining with the third to sixth statements in Equation (13), we get

$$v_{j,x} = 0, (j = 1, \cdots, n). \quad \text{(Equation 46)}$$

This contradicts to the last relation of $\prod_{j=1}^{n} v_{j,x} \neq 0$ in Equation (13). This completes the proof.

Robustness against white noise

Consider an unknown n-partite entangled state with white noise on Hilbert space $\otimes_{j=1}^{n} \mathcal{H}_{A_j}$ as

$$\varrho_v = v\rho_{A_1 \cdots A_n} + \frac{1-v}{2^n} 1_{2^n} \quad \text{(Equation 47)}$$

where 1_{2^n} is a rank-2^n square identity matrix, ρ is defined in Equation (38), and $v \in [0, 1]$. Its density matrix is given by

$$\begin{aligned} \varrho_v = & \left(\frac{1-v}{2^n} + v\rho_{\overrightarrow{0}_n}\right) \left|\overrightarrow{0}_n\right\rangle\left\langle\overrightarrow{0}_n\right| + \left(\frac{1-v}{2^n} + v\rho_{\overrightarrow{0}_n}\right) \left|\overrightarrow{1}_n\right\rangle\left\langle\overrightarrow{1}_n\right| \\ & + v\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n} \left|\overrightarrow{0}_n\right\rangle\left\langle\overrightarrow{1}_n\right| + v\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n} \left|\overrightarrow{1}_n\right\rangle\left\langle\overrightarrow{0}_n\right| \\ & + \frac{1-v}{2^n} \sum_{\overrightarrow{j} \neq \overrightarrow{0}_n, \overrightarrow{1}_n} \left|\overrightarrow{j}\right\rangle\left\langle\overrightarrow{j}\right| \end{aligned} \quad \text{(Equation 48)}$$

where $\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}$ and $\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}$ satisfies $\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}, \rho_{\overrightarrow{1}_n;\overrightarrow{1}_n} \geq 0$, and , $\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n} + \rho_{\overrightarrow{1}_n;\overrightarrow{1}_n} = 1$, $\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n} \geq 0$ from the definition in Equation (38), $\overrightarrow{j} = j_1 \cdots j_n$ is an n-bit series. From Lemma 2, the noisy state ϱ_v is an n-partite entanglement in the biseparable model (Svetlichny, 1987) if v satisfies the following inequality

$$v > \frac{1}{1 + 4\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}}. \quad \text{(Equation 49)}$$

For $2n$ separable observables $\{\sigma_z^{(1)} \otimes \sigma_x^{(n)}, \sigma_z^{(i)} \otimes \sigma_x^{(i+1)}, \sigma_x^{(1)} \otimes \sigma_z^{(n)}, \sigma_x^{(i)} \otimes \sigma_z^{(i+1)}, i = 1, \cdots, n-1\}$, from Equation (48) it is easy to prove that

$$\langle \sigma_z^{(1)} \otimes \sigma_x^{(n)} \rangle_{\varrho_v} = 0, \quad \text{(Equation 50)}$$
$$\langle \sigma_z^{(i)} \otimes \sigma_x^{(i+1)} \rangle_{\varrho_v} = 0, \quad \text{(Equation 51)}$$
$$\langle \sigma_x^{(1)} \otimes \sigma_z^{(n)} \rangle_{\varrho_v} = 0, \quad \text{(Equation 52)}$$
$$\langle \sigma_x^{(i)} \otimes \sigma_z^{(i+1)} \rangle_{\varrho_v} = 0, \ (i = 1, \cdots, n-1). \quad \text{(Equation 53)}$$

Similarly, for $n+1$ observables $\sigma_z^{(1)} \otimes \sigma_z^{(n)}, \sigma_z^{(i)} \otimes \sigma_z^{(i+1)}, (i = 1, \cdots, n-1)$ and $\sigma_x^{(1)} \otimes \cdots \otimes \sigma_x^{(n)}$. from Equation (48) it follows that

$$\langle \sigma_z^{(1)} \otimes \sigma_z^{(n)} \rangle_{\varrho_v} = v, \quad \text{(Equation 54)}$$
$$\langle \sigma_z^{(i)} \otimes \sigma_z^{(i+1)} \rangle_{\varrho_v} = v, \quad \text{(Equation 55)}$$
$$\langle \sigma_x \otimes \sigma_x \rangle_{\varrho_v} = 2v\varrho_{00;11}. \quad \text{(Equation 56)}$$

So, from Equations 50–56 and the inequality (49), ϱ_v is n-partite entangled (Svetlichny, 1987) if it satisfies the following statements

$$\begin{aligned} & \langle \sigma_z^{(1)} \otimes \sigma_x^{(n)} \rangle_{\varrho_v} = 0, \\ & \langle \sigma_z^{(i)} \otimes \sigma_x^{(i+1)} \rangle_{\varrho_v} = 0, \\ & \langle \sigma_x^{(1)} \otimes \sigma_z^{(n)} \rangle_{\varrho_v} = 0, \\ & \langle \sigma_x^{(i)} \otimes \sigma_z^{(i+1)} \rangle_{\varrho_v} = 0, \ (i = 1, \cdots, n-1), \\ & \langle \sigma_z^{(i)} \otimes \sigma_z^{(j)} \rangle_{\varrho_v} + 2\langle \sigma_x^{(1)} \otimes \cdots \otimes \sigma_x^{(n)} \rangle_{\varrho_v} > 1 \end{aligned} \quad \text{(Equation 57)}$$

for any $(i, j) \in \{(1, n), (1, 2), \cdots, (n-1, n)\}$. This has completed the proof. □

Nonlocality verified by violating the Svetlichny inequality

Another method for verifying the multipartite nonlocality of noisy state is using the Svetlichny inequality (Svetlichny, 1987) with the known density matrix. Take a tripartite GHZ-type state in Equation (48) as an example. For simplicity, we can restrict measurement along directions lying in the x-y plane of Pauli sphere,

so that two observables A_i and A_i' of the i-th party are specified by the azimuthal angles φ_i and φ_i', respectively, for $i = 1, 2, 3..$ For the noisy state in Equation (47) with $n = 3$, it follows that

$$\begin{aligned}
\langle A_1A_2A_3\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1+\varphi_2+\varphi_3),\\
\langle A_1A_2A_3'\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1+\varphi_2+\varphi_3'),\\
\langle A_1A_2'A_3\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1+\varphi_2'+\varphi_3),\\
\langle A_1A_2'A_3'\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1+\varphi_2'+\varphi_3'),\\
\langle A_1'A_2A_3\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1'+\varphi_2+\varphi_3),\\
\langle A_1'A_2A_3'\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1'+\varphi_2+\varphi_3'),\\
\langle A_1'A_2'A_3\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1'+\varphi_2'+\varphi_3),\\
\langle A_1'A_2'A_3'\rangle_{\varrho_v} &= 2v\rho_{000;111}\cos(\varphi_1'+\varphi_2'+\varphi_3').
\end{aligned} \tag{Equation 58}$$

From Equation (58), we get

$$\begin{aligned}
|SV|_{\varrho_v} &= \langle A_1A_2A_3\rangle + \langle A_1A_2A_3'\rangle\\
&\quad + \langle A_1A_2'A_3\rangle + \langle A_1'A_2A_3\rangle\\
&\quad - \langle A_1'A_2'A_3'\rangle - \langle A_1'A_2'A_3\rangle\\
&\quad - \langle A_1'A_2A\rangle_3 - \langle A_1A_2'A_3'\rangle\\
&= 8\sqrt{2}v\rho_{000;111},
\end{aligned} \tag{Equation 59}$$

where $\varphi_1+\varphi_2+\varphi_3 = \frac{3\pi}{4}$ and $\varphi_i' = \varphi_i + \frac{\pi}{2}$. The noise visibility is given by

$$1 \geq v^* > \frac{1}{2\sqrt{2}\rho_{000;111}} \tag{Equation 60}$$

for a known state ϱ_v, as shown in Figure 4. It should be interesting to explore other Bell-type inequalities with greater noise visibility.

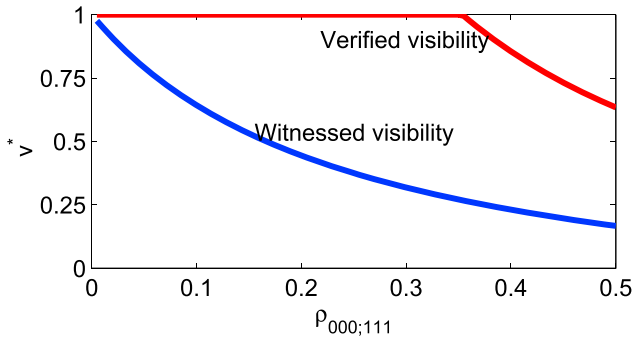


Figure 4. (Color online) Visibility of white noise for ϱ_v in Equation (47)

Here, n = 3. The blue line denotes the witnessed visibility given in Equation (49) with unknown density matrix. The red line denotes the verified visibility given in Equation (60) by using the Svetlichny inequality (Svetlichny, 1987) with known density matrix.

Verifying unknown W-type entanglement

Our goal here is for verifying unknown W-type entanglement. Consider a three-qubit system W-type entangled state (Dür et al., 2000) on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ given by

$$\begin{aligned}
|\Phi\rangle_{ABC} &= a_0|001\rangle + a_1|010\rangle\\
&\quad + a_2|100\rangle + a_3|111\rangle,
\end{aligned} \tag{Equation 61}$$

where a_j's are real parameters satisfying $\sum_{j=0}^{3} a_j^2 = 1..$ Suppose $|\Phi\rangle_{ABC}$ is shared by three parties, Alice, Bob, and Charlie who only know the shared state being the following form:

$$\rho_{ABC} = \mathcal{E}(|\Phi\rangle\langle\Phi|), \tag{Equation 62}$$

where $\mathcal{E}(\bullet)$ is a local channel defined by

$$\mathcal{E}(\varrho) = \sum_j p_j (U_j \otimes V_j \otimes Y_j)\varrho\left(U_j^\dagger \otimes V_j^\dagger \otimes Y_j^\dagger\right), \tag{Equation 63}$$

according to local unknown phase rotations U_i, V_j and Y_j defined in Equation (11) (in the main text), and $\{p_j\}$ is an unknown probability distribution. The entanglement involved in the state ρ_{ABC} is named as *the W-type entanglement*.

Under the local channel $\mathcal{E}(\bullet)$, the density matrix ρ_{ABC} in Equation (62) can be rewritten into the following form

$$\rho_{ABC} = \sum_{j_1+j_2+j_3=1,3} \rho_{j_1j_2j_3;j_1j_2j_3} |j_1j_2j_3\rangle\langle j_1j_2j_3| \quad \text{(Equation 64)}$$

where $\rho_{j_1j_2j_3;k_1k_2k_3}$'s satisfy that $\{\rho_{j_1j_2j_3;j_1j_2j_3}\}$ being a probability distribution and $\rho_{j_1j_2j_3;k_1k_2k_3} = \rho^*_{k_1k_2k_3;j_1j_2j_3}$. Our goal in what follows is to verify the entanglement set

$$\mathcal{S}_w := \{\mathcal{E}(|\Phi\rangle\langle\Phi|), \forall |\Phi\rangle, \mathcal{E}(\bullet)\} \quad \text{(Equation 65)}$$

which is spanned by the basis $\{|j_1j_2j_3\rangle\langle k_1k_2k_3|, \forall j_1+j_2+j_3 = 1,3; k_1+k_2+k_3 = 1,3\}$.

The entanglement set $\mathcal{S}_w$ is not convex because the separable state $\rho_{ABC} = \sum_{j=0}^{d-1} \rho_{j_1j_2j_3;j_1j_2j_3} |j_1j_2j_3\rangle\langle j_1j_2j_3|$ has the decomposition in Equation (64). This rules out the linear entanglement witnesses (Horodecki et al., 2009). Similar to Theorem 2, we have the following Theorem 2′.

Theorem 2′. The entanglement set $\mathcal{S}_w$ is verifiable if

$$\begin{aligned}&\sqrt{\rho_{001;111}\rho_{111;000}} + \sqrt{\rho_{010;100}\rho_{111;000}}\\ &+\sqrt{\rho_{001;010}\rho_{111;000}} + \sqrt{\rho_{100;111}\rho_{111;000}} > \frac{1}{4}.\end{aligned} \quad \text{(Equation 66)}$$

Proof. Similar to the generalized GHZ-like paradox (13) in the main text, we present a paradox for W states $\rho \in \mathcal{S}_w$ as

$$\begin{aligned}&\langle\sigma_z\otimes\sigma_z\otimes\sigma_z\rangle_\rho = -1,\\ &\langle\sigma_x\otimes\sigma_z\otimes\sigma_z\rangle_\rho = 0,\\ &\langle\sigma_z\otimes\sigma_x\otimes\sigma_z\rangle_\rho = 0,\\ &\langle\sigma_z\otimes\sigma_z\otimes\sigma_x\rangle_\rho = 0,\\ &\langle\sigma_x^{(1)}\otimes\sigma_x^{(2)}\rangle_\rho \overset{\text{ES}}{\neq} 0,\\ &\langle\sigma_x^{(1)}\otimes\sigma_x^{(3)}\rangle_\rho \overset{\text{ES}}{\neq} 0.\end{aligned} \quad \text{(Equation 67)}$$

The proof of the nonlocality with definite real values of both parties is similar to its for Theorem 2. Specially, denote the supposedly definite real values of $v_{1,z}$ and $v_{1,x}$ for Alice, $v_{2,z}$ and $v_{2,x}$ for Bob, and $v_{3,z}$ and $v_{3,x}$ for Charlie, with $v_{j,x}, v_{j,z} \in (1,-1)$. From the first statement in Equation (67) we have $v_{1,z}v_{2,z}v_{3,z} = 1$ while implies $v_{j,z} \neq 0$.. Combined with the second to fourth statements in Equation (67), it follows that $v_{j,x} = 0$ for any j. This conflicts with the last relation.

Next, we prove any biseparable state would violate one statement in the paradox (67). For any biseparable state ρ_{bs} on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, it violates the first statement in the paradox (67) if it does not has the decomposition (64). Otherwise, ρ_{bs} has the decomposition (64). From Equation (67), we have

$$\begin{aligned}&\langle\sigma_z\otimes\sigma_z\otimes\sigma_z\rangle_{\rho_{bs}} = -1,\\ &\langle\sigma_x\otimes\sigma_z\otimes\sigma_z\rangle_{\rho_{bs}} = 0,\\ &\langle\sigma_z\otimes\sigma_x\otimes\sigma_z\rangle_{\rho_{bs}} = 0,\\ &\langle\sigma_z\otimes\sigma_z\otimes\sigma_x\rangle_{\rho_{bs}} = 0,\\ &\langle\sigma_x^{(1)}\otimes\sigma_x^{(2)}\rangle_{\rho_{bs}} = 2\sqrt{\rho_{001;111}\rho_{111;001}} + 2\sqrt{\rho_{010;100}\rho_{100;010}}\\ &\langle\sigma_x^{(1)}\otimes\sigma_x^{(3)}\rangle_{\rho_{bs}} = 2\sqrt{\rho_{001;100}\rho_{100;001}} + 2\sqrt{\rho_{010;111}\rho_{111;010}}.\end{aligned} \quad \text{(Equation 68)}$$

It will violate the inequality (66), that is, for any bisparable state we have

$$\begin{aligned}&\sqrt{\rho_{001;111}\rho_{111;001}} + \sqrt{\rho_{010;100}\rho_{100;010}}\\ &+\sqrt{\rho_{001;010}\rho_{010;001}} + \sqrt{\rho_{100;111}\rho_{111;100}} \leq \frac{1}{2}\end{aligned} \quad \text{(Equation 69)}$$

Hence, this has completed the proof.

Now, before ending the proof we prove the inequality (69). Consider an arbitrary biseparable pure state on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C$ as

$$|\Phi\rangle_{ABC} = |\varphi_1\rangle_A|\varphi_2\rangle_{BC} \quad \text{(Equation 70)}$$

where $|\varphi\rangle_i = a_0|0\rangle + a_1|1\rangle$and $|\varphi_2\rangle = \sum_{i,j=0,1} b_{ij}|ij\rangle$, with$\sum_{j=0}^{1} a_j^2 = \sum_{i,j=0}^{1} b_{ij}^2 = 1$ and $|\varphi_2\rangle = \sum_{i,j=0,1} b_{ij}|ij\rangle$, with $\sum_{j=0}^{1} a_j^2 = \sum_{i,j=0}^{1} b_{ij}^2 = 1$. Similar to proof of Lemma 2, we can prove that

$$2\sqrt{\rho_{001;111}\rho_{111;001}} \le \rho_{011;011} + \rho_{101;101}, \quad \text{(Equation 71)}$$
$$2\sqrt{\rho_{010;100}\rho_{100;010}} \le \rho_{000;000} + \rho_{110;110}. \quad \text{(Equation 72)}$$

Moreover, from the positive semidefinite density matrix ρ, all the principal minors are positive semidefinite. Combining with the Cauchy-Schmidt inequality, we get

$$\begin{aligned} 2\sqrt{\rho_{001;010}\rho_{010;001}} &\le \sqrt{\rho_{001;001}\rho_{010;010}} \\ &\le \rho_{001;001} + \rho_{010;010}, \end{aligned} \quad \text{(Equation 73)}$$

and

$$\begin{aligned} 2\sqrt{\rho_{100;111}\rho_{111;100}} &\le \sqrt{\rho_{100;100}\rho_{111;111}} \\ &\le \rho_{100;100} + \rho_{111;111}. \end{aligned} \quad \text{(Equation 74)}$$

From the inequalities (71)-(74), we get

$$\sqrt{\rho_{001;111}\rho_{111;001}} + \sqrt{\rho_{010;100}\rho_{100;010}} + \sqrt{\rho_{001;010}\rho_{010;001}} + \sqrt{\rho_{100;111}\rho_{111;100}} \le \sum_{j_1,j_2,j_3=0,1} \rho_{j_1j_2j_3;j_1j_2j_3} = 1 \quad \text{(Equation 75)}$$

For other two biseparable states, we can similarly prove the inequality (75). Moreover, for any mixed biseparable states $\rho_{bs} = \sum_i p_i|\Phi_i\rangle\langle\Phi_i|$ with product states $|\Phi_i\rangle$, from the concavity of function $f(x) = \sqrt{x}$ it follows that

$$\begin{aligned} &\sqrt{\rho_{001;111}\rho_{111;001}} + \sqrt{\rho_{010;100}\rho_{100;010}} \\ &+ \sqrt{\rho_{001;010}\rho_{010;001}} + \sqrt{\rho_{100;111}\rho_{111;100}} \\ &\le \sum_j p_j \sqrt{\rho^{(j)}_{001;111}\rho^{(j)}_{111;001}} + \sum_j p_j \sqrt{\rho^{(j)}_{010;100}\rho^{(j)}_{100;010}} \\ &+ \sum_j p_j \sqrt{\rho^{(j)}_{001;010}\rho^{(j)}_{010;001}} + \sum_j p_j \sqrt{\rho^{(j)}_{100;111}\rho^{(j)}_{111;100}} \\ &\le 1 \end{aligned} \quad \text{(Equation 76)}$$

from the inequality (75), where $\rho^{(i)}_{j_1j_2j_3;k_1k_2k_3}$ are density matrix elements defined by $|\Phi_i\rangle\langle\Phi_i| = \sum_{j_1,j_2,j_3,k_1,k_2,k_3} \rho^{(i)}_{j_1j_2j_3;k_1k_2k_3}|j_1j_2j_3\rangle\langle k_1k_2k_3|$. This has proved the inequality (66).

Proof of Theorem 3

Consider an n-partite quantum network $\mathcal{N}_q$ shared by n parties $A_1, \cdots, A_n$. The total state of $\mathcal{N}_q$ is given by

$$\rho_{\mathcal{G}} = \otimes_{j=1}^{m_1}\rho_j \otimes_{k=1}^{m_2}\varrho_k \quad \text{(Equation 77)}$$

where ρ_j are generalized EPR entangled states defined in Equation (1) in the main text and ϱ_k are multipartite GHZ entangled states defined in Equation (12) in the main text. Denote the triple $(A_j, \theta_j, (k_j, s_j))$ as the specification of a local controlled-phase

$$CP(\theta_j) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta_j}|11\rangle\langle 11| \quad \text{(Equation 78)}$$

performed by A_j on two qubits from entangled states ρ_{k_j} and ρ_{s_j}. Let $\mathcal{G} = \{(A_j, \theta_j, (k_j, s_j)), \forall j\}$ be the set of all specifications for generating a cluster state.

Define cluster-type entanglement set $\mathcal{S}_{cl}$ as

$$\mathcal{S}_{cl} = \{\mathcal{E}\circ\mathcal{C}(\rho_{\mathcal{G}}), \forall\rho_{\mathcal{G}}, \mathcal{E}(\bullet), \mathcal{C}(\bullet)\} \quad \text{(Equation 79)}$$

where $\mathcal{E}(\bullet)$ is a blind quantum channel consisting of local phase rotations on each qubit, e.g., $\mathcal{E}(\rho) = \otimes_{j=1}^{m_1}\mathcal{E}_j(\rho_j)\otimes_{k=1}^{m_2}\widehat{\mathcal{E}}_k(\varrho_k)$with $\mathcal{E}_j(\bullet)$ defined in Equation (2) (in the main text) and $\widehat{\mathcal{E}}_j(\bullet)$ defined in Equation (11)

(in the main text), $\mathcal{C}(\bullet)$ is a blind unitary transformation defined by $\otimes_{j\in\mathcal{G}}CP(\theta_j)$ with unknown $\theta_j\in(0,\pi)$. The definition in Equation (79) is reasonable because $\mathcal{E}(\bullet)$ and $\mathcal{C}(\bullet)$ are communicative. The main goal in what follows is to verify $\mathcal{S}_{cl}$.

We firstly prove two lemmas.

Lemma 3. Consider any unknown m-partite entanglement $\rho_{A_1\cdots A_m}$ in Equation (11) shared by n parties $A_1,\cdots,A_m$. Then any two parties A_i and A_j can share one unknown bipartite entanglement in Equation (2) assisted by other's local operations and classical communication (LOCC).

Proof of Lemma 3. Consider any unknown multipartite GHZ-type $\rho_{A_1\cdots A_m}$ given in Equation (11). For any two parties A_i and A_j, suppose other parties perform local projection measurement under the basis $\left\{|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)\right\}$ and send out measurement outcomes $a_k, k\in\{1,\cdots,n\}-\{i,j\}$. The resultant conditional on outcomes a_k's is given by

$$\rho_{A_iA_j}=\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}|00\rangle\langle 00|+\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}|11\rangle\langle 11|+(-1)^{\sum_k a_k}\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}|00\rangle\langle 11|+(-1)^{\sum_k a_k}\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n}|11\rangle\langle 00| \tag{Equation 80}$$

which can be locally transformed into

$$\begin{aligned}\rho_{A_iA_j}=&\rho_{\overrightarrow{0}_n;\overrightarrow{0}_n}|00\rangle\langle 00|+\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}|00\rangle\langle 11|\\&+\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n}|11\rangle\langle 00|+\rho_{\overrightarrow{1}_n;\overrightarrow{1}_n}|11\rangle\langle 11|\end{aligned} \tag{Equation 81}$$

after one party performs a local rotation $|0\rangle\langle 0|+(-1)^{\sum_k a_k}|1\rangle\langle 1|$ on its shared qubit. From Lemmas 1 and 2, $\rho_{A_iA_j}$ is an entanglement in Equation (2) if and only if $\rho_{A_1\cdots A_n}$ is an entanglement (i.e., $\rho_{\overrightarrow{1}_n;\overrightarrow{0}_n},\rho_{\overrightarrow{0}_n;\overrightarrow{1}_n}\neq 0$). This has completed the proof.

Lemma 4. Consider a chain quantum network consisting of any two unknown entangled states ρ_{AB} and ρ_{CD} in Equation (2), where Alice has qubit A, Bob has two qubits B and C while Charlie has qubit D. Then Alice and Charlie can share one unknown entanglement in Equation (2) assisted by Bob's LOCC.

Proof of Lemma 4. Consider a chain quantum network consisting of any two unknown states $\rho_{AB}=\sum_{i,j,k,s}\rho_{ij,ks}|ij\rangle\langle ks|$ and $\rho'_{CD}=\sum_{i,j,k,s}\rho'_{ij,ks}|ij\rangle\langle ks|$ in Equation (2). Suppose Charlie performs joint measurement on two qubits B and C under the Bell basis $\left\{|\varphi_\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi_\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)\right\}$. It follows the resultant as

$$\rho_{AD}=\frac{1}{\rho_{00;00}\rho'_{00;00}+\rho_{11;11}\rho'_{11;11}}\left(\rho_{00;00}\rho'_{00;00}|00\rangle\langle 00|\pm\rho_{00;11}\rho'_{00;11}|00\rangle\langle 11|\pm\rho_{11;00}\rho'_{11;00}|11\rangle\langle 00|+\rho_{11;11}\rho'_{11;11}|11\rangle\langle 11|\right) \tag{Equation 82}$$

for the measurement outcomes $|\varphi_\pm\rangle$. Both above states can be locally transformed into

$$\rho_{AD}=\frac{1}{\rho_{00;00}\rho'_{00;00}+\rho_{11;11}\rho'_{11;11}}\left(\rho_{00;00}\rho'_{00;00}|00\rangle\langle 00|+\rho_{00;11}\rho'_{00;11}|00\rangle\langle 11|+\rho_{11;00}\rho'_{11;00}|11\rangle\langle 00|+\rho_{11;11}\rho'_{11;11}|11\rangle\langle 11|\right) \tag{Equation 83}$$

after one party performs a local rotation σ_z on its shared qubit for the measurement outcome $|\varphi_-\rangle$. Similarly, for the measurement outcomes $|\psi_\pm\rangle$., the resultant is given by

$$\rho_{AD}=\frac{1}{\rho_{11;11}\rho'_{00;00}+\rho_{00;00}\rho'_{11;11}}\left(\rho_{11;11}\rho'_{00;00}\left||01\rangle\rangle\langle\langle 01|\right|\pm\rho_{00;11}\rho'_{11;00}|01\rangle\langle 10|\pm\rho_{11;00}\rho'_{00;11}|10\rangle\langle 01|+\rho_{00;00}\rho'_{11;11}|10\rangle\langle 10|\right) \tag{Equation 84}$$

which can be locally transformed into

$$\rho_{AD}=\frac{1}{\rho_{11;11}\rho'_{00;00}+\rho_{00;00}\rho'_{11;11}}\left(\rho_{11;11}\rho'_{00;00}|01\rangle\langle 01|+\rho_{00;11}\rho'_{11;00}|01\rangle\langle 10|+\rho_{11;00}\rho'_{00;11}|10\rangle\langle 01|+\rho_{00;00}\rho'_{11;11}|10\rangle\langle 10|\right) \tag{Equation 85}$$

with a local phase shift conditional on measurement outcome. So, from Lemmas 1 and 2, both states in Equations (83) and (85) are entangled states in Equation (2) if and only if ρ_{AB} and ρ'_{CD} are entangled $\left(\text{i.e., } \rho_{00;11}, \rho_{11;00}, \rho'_{00;11}, \rho'_{11;00} \neq 0\right)$. This has completed the proof. □

Proof of Theorem 3. Note $\mathcal{C}(\bullet)$ does not change the entanglement of the joint state $\mathcal{E}(\rho_{\mathcal{G}})$ because it consists of all the local unitary operations. From the equality of $\mathcal{C}\circ\mathcal{E}(\rho_{\mathcal{G}}) = \mathcal{E}\circ\mathcal{C}(\rho_{\mathcal{G}})$, it is sufficient to verify all the states $\mathcal{E}(\rho_{\mathcal{G}})$. Moreover, from the assumption of connectedness the joint state $\rho_{\mathcal{G}}$ is entangled in the biseparable model (Svetlichny, 1987) if the associated quantum network $\mathcal{N}_q$ is connected. This can be verified by using the recent method (Luo, 2021a, 2021b) combined with Lemmas 3 and 4, that is, each pair can share one bipartite entangled state with the help of other parties' local measurements and classical communication. From Equation (79), it only needs to verify all the entangled states $\mathcal{E}_j(\rho_j)$ and $\widehat{\mathcal{E}}_k(\varrho_k)$.

The main idea is to combine the paradoxes (5) and (13) in the main text. Specially, for a given N-partite cluster state $\varrho_{A_1\cdots A_N} \in \mathcal{S}_{cl}$ on Hilbert space $\otimes_{j=1}^{N}\mathcal{H}_{A_j}$, it satisfies the following statements as

$$\langle \sigma_z^{(i)} \otimes \sigma_z^{(j)} \rangle_{\varrho} = 1, (A_i, A_j) \in \{\rho_s, \forall s\} \cup \{\tau_t, \forall t\} \quad \text{(Equation 86)}$$

$$\langle \sigma_z^{(i)} \otimes \sigma_x^{(j)} \rangle_{\varrho} = 0, (A_i, A_j) \in \{\rho_s, \forall s\} \cup \{\tau_t, \forall t\} \quad \text{(Equation 87)}$$

$$\langle \sigma_x^{(i)} \otimes \sigma_z^{(j)} \rangle_{\varrho} = 0, (A_i, A_j) \in \{\rho_s, \forall s\} \cup \{\tau_t, \forall t\} \quad \text{(Equation 88)}$$

$$\langle \sigma_x^{(i)} \otimes \sigma_x^{(j)} \rangle_{\varrho} \overset{\text{ES}}{\neq}, (A_i, A_j) \in \{\rho_s, \forall s\} \quad \text{(Equation 89)}$$

$$\langle \otimes_{A_i \in \varrho_j} \sigma_x^{(i)} \rangle_{\varrho} \overset{\text{ES}}{\neq} 0, \tau_j \in \{\tau_t, \forall t\} \quad \text{(Equation 90)}$$

where the statement for $(A_i, A_j) \in \{\rho_s, \forall s\} \cup \{\tau_t, \forall t\}$ in Equations 86–88 means both qubits A_i and A_j belong to one EPR-type entanglement (2) or one GHZ-type entanglement (12). The statement for $(A_i, A_j) \in \{\rho_s, \forall s\}$ in Equation (89) means both qubits A_i and A_j belong to one EPR-type entanglement (2). The statement of $\tau_j \in \{\tau_t, \forall t\}$ in Equation (90) means all the qubits τ_j belong to one multipartite GHZ-type entanglement (12).

Similar to the paradoxes (5) and (13), Equations 86–90 are used for verifying the entanglement for single EPR-type entanglement or GHZ-type entanglement in the cluster state ϱ. This completes the *proof.* □

Verifying high-dimensional unknown GHZ-type entanglement

Our goal in this section is to extend Theorems 1 and 2 for verifying high-dimensional unknown GHZ-type entanglement. Consider a d-dimensional Hilbert space $\mathcal{H}$ with computation basis $\{|0\rangle, \cdots, |d-1\rangle\}$, where $d \geq 2$.. Denote $\omega = \exp(2\pi i/d)$ as the root of unity, that is, $\omega^d = 1$ and $\omega \neq 1$.. Define Σ_1 be the shift operator (Weyl, 2014, Ch.III) (similar to Pauli operator σ_x) given by

$$\Sigma_1 = \sum_{j=0}^{d-1} |j+1 \mod d\rangle\langle j| \quad \text{(Equation 91)}$$

and Σ_1 be the clock operator (similar to Pauli operator σ_z) matrix given by

$$\Sigma_3 = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j| \quad \text{(Equation 92)}$$

It is easy to check that

$$(\Sigma_1)^{d-1} = (\Sigma_3)^d = 1 \quad \text{(Equation 93)}$$

with the identity operator 1 on $\mathcal{H}$. Both operators Σ_1 and Σ_3 are fundamental operations for quantum dynamics in high-dimensional spaces (Vourdas, 2004).

Bipartite entanglement

Consider a two-qudit system $|\Phi\rangle_{AB}$ on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are both d-dimensional spaces. A bipartite entangled pure state shared by Alice and Bob is given by

$$|\Phi\rangle_{AB} = \sum_{j=0}^{d-1} \alpha_j |jj\rangle, \quad \text{(Equation 94)}$$

where α_j are real parameters satisfying $\sum_{j=0}^{d-1}\alpha_j^2 = 1$. Suppose that both parties only know the shared state has the following form:

$$\rho_{AB} = \mathcal{E}(|\Phi\rangle\langle\Phi|), \tag{Equation 95}$$

where $\mathcal{E}(\bullet)$ is a blind quantum channel defined by

$$\mathcal{E}(\varrho) = \sum_j p_j (U_j \otimes V_j)\varrho\left(U_j^\dagger \otimes V_j^\dagger\right), \tag{Equation 96}$$

with local phase transformations U_j and V_j given respectively by

$$\begin{aligned} U_j &= \sum_{k=0}^{d-1} e^{i\theta_{kj}}|k\rangle\langle k|, \\ V_j &= \sum_{k=0}^{d-1} e^{i\vartheta_{kj}}|k\rangle\langle k|, \end{aligned} \tag{Equation 97}$$

with unknown parameters $\theta_{kj}, \vartheta_{kj} \in (0,\pi)$, and $\{p_j\}$ is an unknown probability distribution. In general, $\mathcal{E}(\bullet)$ can be defined through semi-positive definite operators M_j's as

$$\mathcal{E}(\varrho) = \sum_j (M_j \otimes N_j)\varrho\left(M_j^\dagger \otimes N_j^\dagger\right) \tag{Equation 98}$$

where M_j and N_j are Kraus operators defined respectively by $M_j = \sum_s \sqrt{q_{js}}|s\rangle\langle s|$, $N_j = \sum_t \sqrt{r_{jt}}|t\rangle\langle t|$ which satisfy $\sum_j M_j^\dagger M_j = \sum_j N_j^\dagger N_j = 1$, $\{q_{js}, \forall s\}$ and $\{r_{jt}, \forall t\}$ are unknown probability distributions. Under the blind channel $\mathcal{E}(\bullet)$, the density matrix ρ_{AB} in Equation (95) can be rewritten into the following form

$$\rho_{AB} = \sum_{j=0}^{d-1} \rho_{jj;jj}|jj\rangle\langle jj| + \sum_{j \neq k} \rho_{jj;kk}|jj\rangle\langle kk|, \tag{Equation 99}$$

where $\rho_{ij;kl}$'s are the density matrix elements satisfying $\{\rho_{jj;jj}\}$ is a probability distribution and $\rho_{jj;kk} = \rho_{kk;jj}^*$. Our goal in what follows is to verify the entanglement set

$$\mathcal{S}_2 := \{\mathcal{E}(|\Phi\rangle\langle\Phi|), \forall |\Phi\rangle, \mathcal{E}(\bullet)\} \tag{Equation 100}$$

which is spanned by the basis $\{|jj\rangle\langle kk|, \forall j,k\}$.

It is easy to prove that $\mathcal{S}_2$ is not convex because the separable state $\rho_{AB} = \sum_{j=0}^{d-1} \rho_{jj;jj}|jj\rangle\langle jj|$ has the decomposition in Equation (99). This rules out the linear entanglement witnesses (Horodecki et al., 2009). Similar to Theorem 1, we have the following Theorem.

Theorem 4. The entanglement set $\mathcal{S}_2$ is verifiable.

Proof. Similar to the generalized GHZ-like paradox (5) in the main text, we present a paradox for high-dimensional quantum entanglement by using Σ_1 in Equation (91) and Σ_3 in Equation (92) as

$$\begin{aligned} &\langle \Sigma_3^k \otimes \Sigma_3^{d-k}\rangle_\rho = 1, (k = 1, \cdots, d-2) \\ &\langle \Sigma_3 \otimes \Sigma_1\rangle_\rho = 0, \\ &\langle \Sigma_1 \otimes \Sigma_3\rangle_\rho = 0, \\ &\langle \Sigma_1 \otimes \Sigma_1\rangle_\rho \overset{\text{ES}}{\neq} 0. \end{aligned} \tag{Equation 101}$$

This can be proved by a forward evaluation. The proof of the nonlocality with definite real values of both parties is similar to its for Theorem 1.

The proof for witnessing the entanglement set $\mathcal{S}_2$ depends on the following nonlinear inequality

$$2\sum_{0 \le j \neq k \le d-1} \sqrt{\rho_{jk;jk}\rho_{kj;kj}} + \sum_{j=0}^{d-1} \rho_{jj;jj} - 1 \le 0 \tag{Equation 102}$$

for any bipartite separable state. The proof will be presented in the later. From the inequality (102), ρ in Equation (99) is entangled for $\rho_{jj;kk}\neq 0$ for any two integers $j\neq k$, in other words, it is separable state if and only if $\rho_{jj;kk}=0$ for any integers j and k with $j\neq k$.

Next we come to prove that any separable state would violate one statement in the paradox (101). For any separable state ρ_s, it violates the first statement in the paradox (101) if it does not has the decomposition in Equation (99). Otherwise, ρ_s has the decomposition in Equation (99). From Equation (101), we have

$$\begin{aligned}&\langle\Sigma_3^k\otimes\Sigma_3^{d-k}\rangle_\rho=\sum_{j=0}^{d-1}\rho_{jj;jj}=1,\\&\langle\Sigma_3\otimes\Sigma_1\rangle_\rho=0,\\&\langle\Sigma_1\otimes\Sigma_3\rangle_\rho=0,\\&\langle\Sigma_1\otimes\Sigma_1\rangle_\rho=\sum_{j=0}^{d-1}\rho_{jj;j+1\ j+1}+\sum_{j=0}^{d-1}\rho_{j+1\ j+1;jj}.\end{aligned}\qquad\text{(Equation 103)}$$

It means that $\rho_{jj;kk}=0$ for any integers j and k with $j\neq k$. This violates the fourth statement in the paradox (101). Hence, this has completed the proof if we can prove the inequality (102).

Proof of the inequality (102). Similar to Lemma 1, consider an arbitrary separable two-qudit pure state on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ as

$$|\Phi\rangle=|\varphi_1\rangle|\varphi_2\rangle\qquad\text{(Equation 104)}$$

With $|\varphi_i\rangle=\sum_{j=0}^{d-1}a_{i,j}|j\rangle$ and $\sum_{j=0}^{d-1}a_j^2=1$, $i=1,2$. It follows that

$$\begin{aligned}\left|\rho_{jj;j+1\ j+1}\right|&=\left|a_{1,j}a_{2,j}a_{1,j+1}a_{2,j+1}\right|\\&=\sqrt{\rho_{j\ j+1;j\ j+1}\rho_{j+1\ j;j+1\ j}}.\end{aligned}\qquad\text{(Equation 105)}$$

This implies that

$$2\left|\rho_{jj;j+1\ j+1}\right|\leq\rho_{j\ j+1;j\ j+1}+\rho_{j+1\ j;j+1\ j},\qquad\text{(Equation 106)}$$

due to the Cauchy-Schwarz inequality of $2\sqrt{|xy|}\leq x^2+y^2$.

Consider an arbitrary mixed separable state on Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ as

$$\rho=\sum_i p_i|\Phi_i\rangle\langle\Phi_i|:=\sum_{j_1,j_2,k_1,k_2}\rho_{j_1j_2;k_1k_2}|j_1j_2\rangle\langle k_1k_2|=\sum_i p_i\sum_{j_1,j_2,k_1,k_2}\rho^{(i)}_{j_1j_2;k_1k_2}|j_1j_2\rangle\langle k_1k_2|\qquad\text{(Equation 107)}$$

with separable pure states $|\Phi_i\rangle$'s, where $\{p_i\}$ is a probability distribution, and $\rho^{(i)}_{j_1j_2;k_1k_2}=|\Phi_i\rangle\langle\Phi_i|$. Similar to the inequalities (18)-(20), from Equation (106) we get

$$2\left|\rho_{jj;j+1\ j+1}\right|=2\left|\sum_i p_i\rho^{(i)}_{jj;j+1\ j+1}\right|\leq\rho_{j\ j+1;j\ j+1}+\rho_{j+1\ j;j+1\ j}\qquad\text{(Equation 108)}$$

Similarly, we can prove that

$$2\left|\rho_{jk;jk}\right|\leq\rho_{jk;jk}+\rho_{kj;kj},j\neq k\qquad\text{(Equation 109)}$$

So, from the inequality (109) we have

$$2\sum_{0\leq j\neq k\leq d-1}\sqrt{\rho_{jk;jk}\rho_{kj;kj}}=2\sum_{0\leq j\neq k\leq d-1}\left|\rho_{jk;jk}\right|\leq\sum_{0\leq j\neq k\leq d-1}\left(\rho_{jk;jk}+\rho_{kj;kj}\right)=1-\sum_{j=0}^{d-1}\rho_{jj;jj}\qquad\text{(Equation 110)}$$

This has completed the proof.

Multipartite entanglement

Consider an n-qudit system $|\Psi\rangle_{A_1\cdots A_n}$ on Hilbert space $\otimes_{j=1}^n\mathcal{H}_{A_j}$, where $\mathcal{H}_{A_j}$'s are all d-dimensional spaces. A generalized n-partite entangled pure state shared by $A_1,\cdots,A_n$ is given by

$$|\Psi\rangle_{A_1\cdots j_n} = \sum_{j=0}^{d-1} \alpha_j |j,\cdots,j\rangle, \tag{Equation 111}$$

where α_j's are real parameters satisfying $\sum_{j=0}^{d-1}\alpha_j^2 = 1$. Suppose that all the parties only know the shared state has the following form:

$$\rho_{A_1\cdots A_n} = \mathcal{E}(|\Psi\rangle\langle\Psi|), \tag{Equation 112}$$

where $\mathcal{E}(\bullet)$ is a blind quantum channel defined similar to Equation (96) by using unknown local phase transformations for each party. Under the blind channel $\mathcal{E}(\bullet)$, the density matrix $\rho_{A_1\cdots A_n}$ in Equation (111) can be rewritten into the following form

$$\rho_{A_1\cdots A_n} = \sum_{j=0}^{d-1} \rho_{\overrightarrow{j}_n;\overrightarrow{j}_n} \left|\overrightarrow{j}_n\right\rangle\left\langle\overrightarrow{j}_n\right| + \sum_{j\neq k} \rho_{\overrightarrow{j}_n;\overrightarrow{k}_n} \left|\overrightarrow{j}_n\right\rangle\left\langle\overrightarrow{k}_n\right|, \tag{Equation 113}$$

where $\overrightarrow{j}_n$ denotes n number of j, i.e., $\overrightarrow{j}_n = j\cdots j$, $\rho_{\overrightarrow{j}_n;\overrightarrow{k}_n}$ are the density matrix elements satisfying $\sum_{j=0}^{d-1}\rho_{\overrightarrow{j}_n;\overrightarrow{j}_n} = 1$ ($\{\rho_{\overrightarrow{j}_n;\overrightarrow{j}_n}\}$ is a probability distribution) and $\rho_{\overrightarrow{j}_n;\overrightarrow{k}_n} = \rho^*_{\overrightarrow{k}_n;\overrightarrow{j}_n}$. Our goal in what follows is to verify the entanglement set

$$\mathcal{S}_n := \{\mathcal{E}(|\Psi\rangle\langle\Psi|), \forall|\Psi\rangle, \mathcal{E}(\bullet)\} \tag{Equation 114}$$

which is spanned by the basis $\{\left|\overrightarrow{j}_n\right\rangle\left\langle\overrightarrow{j}_n\right|, \left|\overrightarrow{j}_n\right\rangle\left\langle\overrightarrow{j}_n\right|, \forall j,k\}$.

Similar to Theorem 2, we have the following Theorem 5.

Theorem 5

The entanglement set $\mathcal{S}_n$ is verifiable.

The proof of Theorem 5 is based on two facts. One is from the generalized GHZ-like paradox given by

$$\begin{aligned}
&\langle\left(\Sigma_3^{(1)}\right)^k \otimes \left(\Sigma_3^{(n)}\right)^{d-k}\rangle = 1,\ (k=1,\cdots,d-1),\\
&\langle\left(\Sigma_3^{(j)}\right)^k \otimes \left(\Sigma_3^{(j+1)}\right)^{d-k}\rangle = 1,\\
&\langle\Sigma_3^{(1)}\otimes\Sigma_1^{(n)}\rangle = 0,\\
&\langle\Sigma_3^{(j)}\otimes\Sigma_1^{(j+1)}\rangle = 0,\\
&\langle\Sigma_1^{(1)}\otimes\Sigma_3^{(n)}\rangle = 0,\\
&\langle\Sigma_1^{(j)}\otimes\Sigma_3^{(j+1)}\rangle = 0,\ (j=1,\cdots,n-1),\\
&\langle\Sigma_1^{(1)}\otimes\cdots\otimes\Sigma_1^{(n)}\rangle \overset{ES}{\neq} 0,
\end{aligned} \tag{Equation 115}$$

for all the entangled states in $\mathcal{S}_n$, while it will be violated by any biseparable state. Here, $\Sigma_i^{(j)}$ denotes the local observable Σ_i performed by A_j. The paradox (115) can be proved similar to its for the paradox (13). The other is from the nonlinear inequality given by

$$2\sum_{0\leq i\neq k\leq d-1}\sqrt{\rho_{\overrightarrow{j}_n;\overrightarrow{k}_n}\rho_{\overrightarrow{k}_n;\overrightarrow{j}_n}} + \sum_{j=0}^{d-1}\rho_{\overrightarrow{j}_n;\overrightarrow{j}_n} \leq 1, \tag{Equation 116}$$

which holds for any biseparable state. This can be proved similar to Lemma 2 and the inequality (102), where $\overrightarrow{j} = j_1\cdots j_n$ and $\overrightarrow{k} = k_1\cdots k_n, j_1,\cdots,j_n,k_1,\cdots,k_n \in \{0,\cdots,d-1\}$.