Local discrimination of generalized Bell states via commutativity

Mao-Sheng Li,[1] Fei Shi,[2] and Yan-Ling Wang[3,*]
[1]*School of Mathematics, South China University of Technology, Guangzhou 510641, China*
[2]*School of Cyber Security, University of Science and Technology of China, Hefei 230026, China*
[3]*School of Computer Science and Technology, Dongguan University of Technology, Dongguan 523808, China*

(Received 30 November 2021; accepted 21 March 2022; published 30 March 2022)

We study the distinguishability of generalized Bell states under local operations and classical communication. We introduce the concept of a maximally commutative set (MCS), a subset of generalized Pauli matrices whose elements are mutually commutative, and there is no other generalized Pauli matrix that commutes with all the elements of this set. We find that MCS can be considered a detector for the local distinguishability of a set $\mathcal{S}$ of generalized Bell states. In fact, we get an efficient criterion. That is, if the difference set $\Delta\mathcal{S}$ of $\mathcal{S}$ is disjoint with or completely contained in some MCS, then the set $\mathcal{S}$ is locally distinguishable. Furthermore, we give a useful characterization of MCS for arbitrary dimensions, which provides great convenience for detecting the local discrimination of generalized Bell states. Our method can be generalized to more general settings which contain the lattice qudit basis. The results of Fan [Phys. Rev. Lett. **92**, 177905 (2004)], Tian *et al.* [Phys. Rev. A **92**, 042320 (2015)], and a recent work Yuan *et al.* [arXiv:2109.07390] can be deduced as special cases of our result.

DOI: 10.1103/PhysRevA.105.032455

I. INTRODUCTION

Quantum state discrimination is a fundamental task in quantum information processing. The most general task is to identify a quantum state chosen randomly from a known set of states via a positive operator-valued measurement (POVM). It is well known that a set of quantum states can be perfectly distinguished by global measurement if and only if the states of the given set are mutually orthogonal [1]. However, quantum states are usually distributed in composite systems with long distances, so only local operations and classical communication (LOCC) are allowed. In such a setting, a state is chosen from a known orthogonal set of quantum states in a composite systems, and the task is to identify the state under LOCC. If the task can be accomplished perfectly, we say that the set is *locally distinguishable*; otherwise, it is *locally indistinguishable*. If an orthogonal set is locally indistinguishable, we also say that the set presents some kind of nonlocality [2] in the sense that more quantum information could be inferred from global measurement than that from local operations. Any two orthogonal multipartite states are shown to be locally distinguishable [3]. Bennett *et al.* [2] presented the first example of orthogonal product states that are locally indistinguishable, which revealed the phenomenon of quantum nonlocality without entanglement. Results for the local distinguishability of quantum states have been practically applied in quantum cryptography primitives such as data hiding [4,5] and secret sharing [6–8].

For general orthogonal sets of quantum states, it is difficult to give a complete characterization of whether they are locally distinguishable or not. Therefore, most studies (see [2,3,9–56] for an incomplete list) focus on two extreme cases: sets of product states or sets of maximally entangled states. In this paper, we restrict ourselves to the settings of maximally entangled cases.

Bell states are the most famous maximally entangled states, and their local distinguishability has been well understood. In fact, any two Bell states are locally distinguishable, but any three or four are not [10]. Nathanson [17] showed that any three maximally entangled states in $\mathbb{C}^3\otimes\mathbb{C}^3$ can be locally distinguished. Moreover, any $l>d$ maximally entangled states in $\mathbb{C}^d\otimes\mathbb{C}^d$ are known to be locally indistinguishable [17]. Therefore, it is interesting to consider whether a set of maximally entangled states with cardinality $l\leqslant d$ can be locally distinguishable or not. Interestingly, using the fact that applying a local unitary operation does not change the local distinguishability, Fan [16] showed that any l generalized Bell states (GBSs) in $\mathbb{C}^d\otimes\mathbb{C}^d$ are locally distinguishable provided that $(l-1)l\leqslant 2d$ and d is a prime number. Fan's result was extended by Tian *et al.* to the prime-power-dimensional quantum system in [57], where they restricted themselves to the mutually commuting qudit lattice states. Since Fan's result, many works [57–64] have paid attention to the locally distinguishability of GBSs. Ghosh *et al.* [15] found a sufficient condition for a set of GBSs to be one way locally distinguishable. Such a condition was also proven to be necessary by Bandyopadhyay *et al.* [24]. However, the condition itself seems to be difficult to verify for a general set of GBSs. Therefore, it is a very interesting problem to find an easy check sufficient condition for a set of GBSs to be locally distinguishable.

In this work, we introduce the concept of a maximally commutative set (MCS) of GBSs. Using MCSs, we provide

*wangylmath@yahoo.com

a sufficient criterion for a set of GBSs to be one way locally distinguishable. Finally, we characterize the MCS of GBSs, which is crucial for studying the property of distinguishability for the mentioned states.

The rest of this paper is organized as follows. In Sec. II, we introduce the matrix representation of generalized Bell states. Then we give a brief review of some known results of the sufficient conditions of a locally distinguishable set of GBSs. In Sec. III, we present the definition of a maximally commutative set and show that it is useful for judging the local distinguishability. After that, we present some examples of MCSs and study the properties of general MCSs. Finally, we draw a conclusion and present some questions in Sec. IV.

II. REVIEW OF THE LOCAL DISTINGUISHABILITY OF GBSs

Throughout this paper, we use the following notations. Let $d \geqslant 2$ be an integer. $\mathbb{Z}_d$ denotes the ring which is defined over $\{0, 1, \dots, d-1\}$ with the sum operation $+$ [here $i + j$ should be equal to the element $(i + j) \mod d$] and the multiplication operation (computing the usual multiplication first, then taking modulus d). Consider a bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$ with both local dimensions equal to d. Suppose that $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ is the computational basis of a single qudit. Under this computational basis, the standard maximally entangled state in this system can be expressed as $|\Psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$. Generally, any maximally entangled state can be written in the form $|\Psi_U\rangle = (I \otimes U)|\Psi_{00}\rangle$ for some unitary matrix U of dimension d. We often call U the defining unitary matrix of the maximally entangled state $|\Psi_U\rangle$. To define the generalized Bell states, we define the following two operations:

$$X_d = \sum_{i=0}^{d-1} |i + 1 \bmod d\rangle\langle i|, \qquad Z_d = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i|,$$

where $\omega = e^{\frac{2\pi\sqrt{-1}}{d}}$. Then the following d^2 orthogonal maximally entangled states (MES) are called generalized Bell states:

$$\{|\Psi_{m,n}\rangle = \left(I \otimes X_d^m Z_d^n\right)|\Psi_{00}\rangle | m, n \in \mathbb{Z}_d\}. \tag{1}$$

Matrices in $\{X_d^m Z_d^n |\ m, n \in \mathbb{Z}_d\}$ are called the generalized Pauli matrices [16] (GPMs; they are also known as Weyl operators [65,66]). For simplicity, we also use X and Z to represent X_d and Z_d when the dimension is known. Due to the one-to-one correspondence of MESs and their defining unitary matrices, for convenience, we will treat the following three sets equally without distinction:

$$\mathcal{S} := \{|\Psi_{m_i,n_i}\rangle\}_{i=1}^l = \{X^{m_i} Z^{n_i}\}_{i=1}^l = \{(m_i, n_i)\}_{i=1}^l.$$

Our aim in this paper is to provide some sufficient condition such that the set $\mathcal{S}$ is locally distinguishable. Now we give a brief review of some relative results.

Fan [16] noted that if all m_i $(i = 1, \dots, l)$ are distinct, the set $\mathcal{S}$ can be locally distinguished, and those sets with this property are called F type [64]. For each $\alpha \in \mathbb{Z}_d$, we define H_α as the matrix whose jk entry is $w^{-jk-\alpha s_k}/\sqrt{d}$ for $j, k = 1, \dots, d-1$ and $s_k := \sum_{i=k}^{d-1} i$. Then H_α is a unitary matrix, and $H_\alpha \otimes H_\alpha^t$ transfers $|\Psi_{m_i,n_i}\rangle$ to $|\Psi_{\alpha m_i + n_i, -m_i}\rangle$. Fan found that if d is a prime number and $(l-1)l \leqslant 2d$, an α exists such that $H_\alpha \otimes H_\alpha^t$ can transfer $\mathcal{S}$ to a set of F type.

In addition, there is a useful necessary and sufficient condition (see Refs. [15,24] for more details) for one-way local distinguishability of generalized Bell states (in fact, it may be extended to a more general setting whose local unitary operators follow a particular property). $\mathcal{S}$ denotes the defining unitary matrix set if some nontrivial vector $|v\rangle \in \mathbb{C}^d$ exists such that

$$\langle v|U^\dagger V|v\rangle = 0 \tag{2}$$

for all different $U, V \in \mathcal{S}$; then the set of maximally entangled states corresponding to $\mathcal{S}$ is one way distinguishable (hence locally distinguishable) [15,28]. If the set $\mathcal{S}$ is F type, the vector $|v\rangle$ can be chosen as any vector of the computational basis, i.e., $|i\rangle, i \in \mathbb{Z}_d$. We define the set difference $\Delta\mathcal{S}$ of $\mathcal{S} := \{U_i | i = 1, 2, \dots, l\}$ as

$$\Delta\mathcal{S} = \{U_i^\dagger U_j \mid 1 \leqslant i < j \leqslant l\}. \tag{3}$$

Note that

$$(X^{m_i} Z^{n_i})^\dagger X^{m_j} Z^{n_j} = \omega^{-(m_j - m_i)n_i} X^{m_j - m_i} Z^{n_j - n_i}.$$

Up to a phase, we can identify $\Delta\mathcal{S}$ as the set $\{(m_j - m_i, n_j - n_i) | 1 \leqslant i < j \leqslant l\}$. In order to find some nonzero vector $|v\rangle$ such that Eq. (2) is satisfied, the following lemma is important (see also Ref. [67]).

Lemma 1. For two unitary matrices U and V, if they satisfy $UV = zVU$, where z is a complex number, and are not commutative, i.e., $z \neq 1$, then each eigenvector $|v\rangle$ of V satisfies $\langle v|U|v\rangle = 0$. In fact, suppose that $V|v\rangle = \lambda|v\rangle$, where $\bar{\lambda}\lambda = 1$. We also have $\langle v|V^\dagger = \bar{\lambda}\langle v|$. Therefore, $\langle v|U|v\rangle = \langle v|\bar{\lambda}U\lambda|v\rangle = \langle v|V^\dagger UV|v\rangle = z\langle v|U|v\rangle$. Hence, $\langle v|U|v\rangle = 0$ as $z \neq 1$. A pair of unitaries that satisfy the first condition are called Weyl commutative.

Fortunately, any pair of generalized Pauli matrices is Weyl commutative. In fact, for two pairs of (m_i, n_i) and (m_j, n_j) in $\mathbb{Z}_d \times \mathbb{Z}_d$, we always have

$$X^{m_i} Z^{n_i} X^{m_j} Z^{n_j} = \omega^{m_j n_i - m_i n_j} X^{m_j} Z^{n_j} X^{m_i} Z^{n_i}.$$

Moreover, $X^{m_i} Z^{n_i}$ and $X^{m_j} Z^{n_j}$ are commutative if and only if $m_j n_i - m_i n_j \equiv 0 \bmod d$. This condition can be formulated as the determinant equation

$$\begin{vmatrix} m_i & n_i \\ m_j & n_j \end{vmatrix} \equiv 0 \mod d. \tag{4}$$

The pairs (m_i, n_i) and (m_j, n_j) are also called commutative if Eq. (4) is satisfied.

For any set $\mathcal{S}$ of GBSs, if there is a generalized Pauli matrix V which is not commutative for every GPM $U \in \Delta\mathcal{S}$, following Eqs. (2) and (3) and Lemma 1, each eigenvector $|v\rangle$ of V satisfies $\langle v|U|v\rangle = 0$, and therefore, the set $\mathcal{S}$ is locally distinguishable.

Let $m, n \in \mathbb{Z}_d$; $S(m, n)$ denotes the solution set of the following congruence equation:

$$nx - my = 0 \mod d. \tag{5}$$

Therefore, $S(m, n)$ denotes the set of elements in $\mathbb{Z}_d \times \mathbb{Z}_d$ that commute with (m, n). The authors of Ref. [67] defined the set

$$\mathcal{D}(\mathcal{S}) \triangleq (\mathbb{Z}_d \times \mathbb{Z}_d) \setminus \bigcup_{(m,n)\in\Delta\mathcal{S}} S(m, n)$$

which is significant to check whether there is any GPM V that do not commuting with all the elements in $\Delta\mathcal{S}$. By definition, $\mathcal{D}(\mathcal{S})$ denotes the set of all elements in $\mathbb{Z}_d \times \mathbb{Z}_d$ that do not commute with all the elements in $\Delta\mathcal{S}$. Under this definition, they proved the following results.

Theorem 1. Let $\mathcal{S} = \{(m_i, n_i)|4 \leqslant i \leqslant l \leqslant d\}$ be a GBS set in $\mathbb{C}^d \otimes \mathbb{C}^d$; then the set $\mathcal{S}$ is locally distinguishable when any of the following conditions is true (see Ref. [67]).

(1) The discriminant set $\mathcal{D}(\mathcal{S})$ is not empty.

(2) The set $\Delta\mathcal{S}$ is commutative.

(3) The dimension d is a composite number, and for each $(m, n) \in \Delta\mathcal{S}$, m or n is invertible in $\mathbb{Z}_d$.

The nonemptyness of $\mathcal{D}(\mathcal{S})$ implies the local distinguishability of $\mathcal{S}$. Therefore, the set $\mathcal{D}(\mathcal{S})$ can be called a *discriminant set* of $\mathcal{S}$.

III. DETECTOR FOR THE LOCAL DISTINGUISHABILITY OF GBSs

In the first case in Theorem 1, the nonemptyness of the discriminant set $\mathcal{D}(\mathcal{S})$ is equivalent to there being some $(s, t) \in \mathbb{Z}_d \times \mathbb{Z}_d$ such that

$$ms - nt \neq 0 \ \ \forall (m, n) \in \Delta\mathcal{S}.$$

That is, X^sZ^t does not commute with X^mZ^n. Therefore, any nonzero eigenvector $|v\rangle$ of X^sZ^t satisfies

$$\langle v|X^mZ^n|v\rangle = 0,$$

from which one can conclude that the set $\mathcal{S}$ is locally distinguishable. From this point, we can call X^sZ^t a detector of the local discrimination of GBSs. Simply, the ability of the detector X^sZ^t can be defined as the set

$$\mathcal{D}e(X^sZ^t) \triangleq (\mathbb{Z}_d \times \mathbb{Z}_d) \setminus S(s, t). \tag{6}$$

This denotes the set of all elements in $\mathbb{Z}_d \times \mathbb{Z}_d$ that do not commute with (s, t). Then the one-way local distinguishability of $\mathcal{S}$ can be detected by X^sZ^t if and only if $\Delta\mathcal{S} \subseteq \mathcal{D}e(X^sZ^t)$.

In fact, we can introduce a stronger detector with the following observation. If a set of detectors $\{X^{s_i}Z^{t_i}\}_{i=1}^n$ is commutative, the detectors can share a common eigenbasis $\{|v_j\rangle\}_{j=1}^d$. Therefore, if

$$\Delta\mathcal{S} \subseteq \bigcup_{i=1}^{n} \mathcal{D}e(X^{s_i}Z^{t_i}),$$

we can also conclude that the set $\mathcal{S}$ is one way distinguishable. Therefore, the more elements the detected set has, the stronger its distinguishability is. This motivates the following definition.

A subset $\{X^{s_i}Z^{t_i}\}_{i=1}^n$ of GBSs is called *maximally commutative* if the elements of the given subset are mutually commutative and there is no other GBS which can commute with all the elements of the set. This can be written as the coordinates $\{(s_i, t_i)\}_{i=1}^n \subseteq \mathbb{Z}_d \times \mathbb{Z}_d$ such that $s_it_j = t_is_j$ for every i, j but there is no other coordinate $(s, t) \in \mathbb{Z}_d \times \mathbb{Z}_d \setminus \{(s_i, t_i)\}_{i=1}^n$ such that $s_jt = t_js$ for every j.

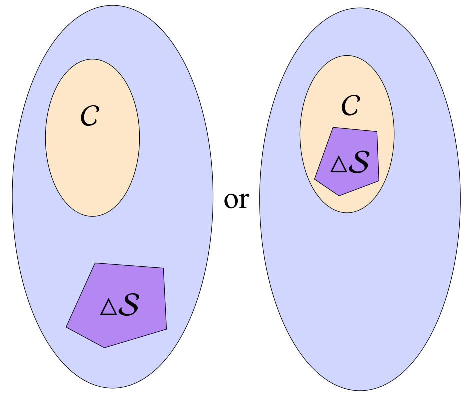

FIG. 1. Here $\mathcal{C}$ represents a maximally commutative set of GBSs, and $\Delta\mathcal{S}$ is the difference set of $\mathcal{S}$. If $\Delta\mathcal{S}$ and the detector $\mathcal{C}$ are in one of the above relations, then the set $\mathcal{S}$ is locally distinguishable.

For any maximally commutative set of GBSs $\mathcal{C} := \{X^{s_i}Z^{t_i}\}_{i=1}^n$, we define a detector as

$$\mathcal{D}e(\mathcal{C}) := \bigcup_{(s,t)\in\mathcal{C}} \mathcal{D}e(X^sZ^t).$$

Therefore, we conclude that if $\Delta\mathcal{S} \subseteq \mathcal{D}e(\mathcal{C})$, the set $\mathcal{S}$ is one way distinguishable. On the other hand, we find that $\mathcal{D}e(\mathcal{C})$ is equal to $\mathcal{P}_d \setminus \mathcal{C}$, where $\mathcal{P}_d := \{X^mZ^n|m, n \in \mathbb{Z}_d\}$. In fact, an element in $\mathcal{P}_d$ but outside $\mathcal{C}$ cannot commute with an element X^sZ^t in $\mathcal{C}$. That is, it belongs to $\mathcal{D}e(X^sZ^t)$. This means that $\mathcal{P}_d \setminus \mathcal{C} \subseteq \mathcal{D}e(\mathcal{C})$. Obviously, $\mathcal{D}e(\mathcal{C}) \subseteq \mathcal{P}_d \setminus \mathcal{C}$. Thus, $\mathcal{D}e(\mathcal{C}) = \mathcal{P}_d \setminus \mathcal{C}$. Therefore, $\Delta\mathcal{S} \subseteq \mathcal{D}e(\mathcal{C})$ if and only if $\Delta\mathcal{S} \cap \mathcal{C} = \emptyset$. Moreover, if $\Delta\mathcal{S} \subseteq \mathcal{C}$, the elements in $\Delta\mathcal{S}$ are mutually commutative. By Theorem 1, the set $\mathcal{S}$ is also locally distinguishable.

Theorem 2. Let $\mathcal{S}$ be a GBS set in $\mathbb{C}^d \otimes \mathbb{C}^d$ and $\mathcal{C}$ be a set of maximally commutative GBSs of dimension d. If $\Delta\mathcal{S} \cap \mathcal{C} = \emptyset$ or $\Delta\mathcal{S} \subseteq \mathcal{C}$, then the set $\mathcal{S}$ is locally distinguishable (see Fig. 1 for an intuitive view of the conditions).

Note that Theorem 2 generalizes Theorem 1. If $\mathcal{D}(\mathcal{S})$ is nonempty (that is, the distinguishability of $\mathcal{S}$ can be detected by the first condition of Theorem 1), then some maximally commutative set $\mathcal{C}$ of GBSs satisfying the condition of Theorem 2 must exist. In fact, the nonemptyness of the discriminant set $\mathcal{D}(\mathcal{S})$ is equivalent to the existence of X^sZ^t that do not commute with every element of $\Delta\mathcal{S}$, but such an X^sZ^t can be extended to be a maximally commutative set $\mathcal{C}$ of GBSs. As the elements in $\mathcal{C}$ all commute with X^sZ^t, $\Delta\mathcal{S} \cap \mathcal{C} = \emptyset$. Moreover, if d is a composite number, $d = pq$, where $p, q \geqslant 2$ are two integers. Clearly, X^p commutes with Z^q; therefore, they can extend to a maximally commutative set of GBSs, say, $\mathcal{C}$. If s or t is invertible in $\mathbb{Z}_d$, we claim that $X^sZ^t \notin \mathcal{C}$. In fact, as $ZX = \omega XZ$, if s is invertible, then $Z^q(X^sZ^t) = \omega^{sq}(X^sZ^t)Z^q \neq (X^sZ^t)Z^q$. If t is invertible, then $(X^sZ^t)X^p = \omega^{tp}X^p(X^sZ^t) \neq X^p(X^sZ^t)$. This also means that $\Delta\mathcal{S} \cap \mathcal{C} = \emptyset$. Therefore, if $\Delta\mathcal{S}$ contains only those elements (one of the two coordinates is invertible in $\mathbb{Z}_d$), then the set $\mathcal{C}$ can detect the one-way distinguishability of $\mathcal{S}$.

Therefore, it is important to find all the maximally commutative sets of GBSs. Now we present some examples in the low-dimensional cases.

Example 1. There are exactly four classes of maximally commutative sets of GBSs in $\mathbb{C}^3 \otimes \mathbb{C}^3$:

$$\begin{array}{lllll} \mathcal{C}_1 & = & \{(0,0), & (0,1), & (0,2)\}, \\ \mathcal{C}_2 & = & \{(0,0), & (1,0), & (2,0)\}, \\ \mathcal{C}_3 & = & \{(0,0), & (1,1), & (2,2)\}, \\ \mathcal{C}_4 & = & \{(0,0), & (1,2), & (2,1)\}. \end{array}$$

As Theorem 2 provides a sufficient condition for a set to be locally distinguishable, a locally indistinguishable set of GBSs implies the violation of the condition of Theorem 2 immediately. For example, in $\mathbb{C}^3 \otimes \mathbb{C}^3$, the set $\mathcal{S} := \{\mathbb{I}, X, X^2, XZ\}$ is locally indistinguishable as $|\mathcal{S}| = 4 > 3$. The difference set $\Delta\mathcal{S} = \{(1,0), (2,0), (1,1), (0,1), (2,1)\}$. Clearly, $\Delta\mathcal{S} \not\subseteq \mathcal{C}_i$ for all $i = 1, 2, 3, 4$. Moreover, $\Delta\mathcal{S} \cap \mathcal{C}_1 = \{(0,1)\}$, $\Delta\mathcal{S} \cap \mathcal{C}_2 = \{(1,0), (2,0)\}$, $\Delta\mathcal{S} \cap \mathcal{C}_3 = \{(1,1)\}$, and $\Delta\mathcal{S} \cap \mathcal{C}_4 = \{(2,1)\}$, which violate the condition of Theorem 2.

Example 2. There are exactly seven classes of maximally commutative sets of GBSs in $\mathbb{C}^4 \otimes \mathbb{C}^4$:

$$\begin{array}{llllll} \mathcal{C}_1 & = & \{(0,0), & (0,1), & (0,2), & (0,3)\}, \\ \mathcal{C}_2 & = & \{(0,0), & (0,2), & (2,0), & (2,2)\}, \\ \mathcal{C}_3 & = & \{(0,0), & (0,2), & (2,1), & (2,3)\}, \\ \mathcal{C}_4 & = & \{(0,0), & (1,0), & (2,0), & (3,0)\}, \\ \mathcal{C}_5 & = & \{(0,0), & (1,1), & (2,2), & (3,3)\}, \\ \mathcal{C}_6 & = & \{(0,0), & (1,2), & (2,0), & (3,2)\}, \\ \mathcal{C}_7 & = & \{(0,0), & (1,3), & (2,2), & (3,1)\}. \end{array}$$

Example 3. There are exactly 15 classes of maximally commutative sets of GBSs in $\mathbb{C}^8 \otimes \mathbb{C}^8$. Here we do not write out the coordinates (0,0), which belongs to all 15 sets.

$$\begin{array}{lllllllll} \mathcal{C}_1 & = & \{(0,1), & (0,2), & (0,3), & (0,4), & (0,5), & (0,6), & (0,7)\}, \\ \mathcal{C}_2 & = & \{(0,2), & (0,4), & (0,6), & (4,0), & (4,2), & (4,4), & (4,6)\}, \\ \mathcal{C}_3 & = & \{(0,2), & (0,4), & (0,6), & (4,1), & (4,3), & (4,5), & (4,7)\}, \\ \mathcal{C}_4 & = & \{(0,4), & (2,0), & (2,4), & (4,0), & (4,4), & (6,0), & (6,4)\}, \\ \mathcal{C}_5 & = & \{(0,4), & (2,1), & (2,5), & (4,2), & (4,6), & (6,3), & (6,7)\}, \\ \mathcal{C}_6 & = & \{(0,4), & (2,2), & (2,6), & (4,0), & (4,4), & (6,2), & (6,6)\}, \\ \mathcal{C}_7 & = & \{(0,4), & (2,3), & (2,7), & (4,2), & (4,6), & (6,1), & (6,5)\}, \\ \mathcal{C}_8 & = & \{(1,0), & (2,0), & (3,0), & (4,0), & (5,0), & (6,0), & (7,0)\}, \\ \mathcal{C}_9 & = & \{(1,1), & (2,2), & (3,3), & (4,4), & (5,5), & (6,6), & (7,7)\}, \\ \mathcal{C}_{10} & = & \{(1,2), & (2,4), & (3,6), & (4,0), & (5,2), & (6,4), & (7,6)\}, \\ \mathcal{C}_{11} & = & \{(1,3), & (2,6), & (3,1), & (4,4), & (5,7), & (6,2), & (7,5)\}, \\ \mathcal{C}_{12} & = & \{(1,4), & (2,0), & (3,4), & (4,0), & (5,4), & (6,0), & (7,4)\}, \\ \mathcal{C}_{13} & = & \{(1,5), & (2,2), & (3,7), & (4,4), & (5,1), & (6,6), & (7,3)\}, \\ \mathcal{C}_{14} & = & \{(1,6), & (2,4), & (3,2), & (4,0), & (5,6), & (6,4), & (7,2)\}, \\ \mathcal{C}_{15} & = & \{(1,7), & (2,6), & (3,5), & (4,4), & (5,3), & (6,2), & (7,1)\}. \end{array}$$

Using these MCSs, we can show that Theorem 2 is more powerful than Theorem 1 when the dimension $d = 8$. Set

$$\mathcal{S} := \{\mathbb{I}, Z, X, X^2Z^3, X^3Z, X^3Z^2, X^5Z, X^6Z^6\},$$

whose difference set $\Delta\mathcal{S}$ is the set with elements

$$\begin{array}{l} (0,1), (1,0), (2,3), (3,1), (3,2), (5,1), (6,6), (1,7), \\ (2,2), (3,0), (5,0), (6,5), (1,3), (2,1), (4,1), (5,6), \\ (1,6), (3,6), (4,3), (2,0), (3,5), (2,7), (3,4), (1,5). \end{array}$$

We can check that $\mathcal{D}(\mathcal{S}) = \emptyset$, $\Delta\mathcal{S}$ is noncommutative, and neither of the coordinates of (2,0) are invertible in $\mathbb{Z}_8$. Therefore, Theorem 1 fails to detect the distinguishability of this set. However, we find that $\Delta\mathcal{S} \cap \mathcal{C}_2 = \emptyset$. That is, the local distinguishability of $\mathcal{S}$ can be detected by $\mathcal{C}_2$. Moreover, we can check that neither $\Delta\mathcal{S} \cap \mathcal{C}_i = \emptyset$ nor $\Delta\mathcal{S} \subseteq \mathcal{C}_i$ when $i \neq 2$. Therefore, among the 15 classes, $\mathcal{C}_2$ is the only detector that can detect the local distinguishability of $\mathcal{S}$.

More numerical results comparing the power of Theorems 1 and 2 can be seen in the Fig. 2 (we randomly generated N sets of d-dimensional GBSs with cardinality n and found the numbers N_1 and N_2 of sets whose local distinguishability can be detected by Theorems 1 and 2, respectively; the corresponding success rates are defined by N_1/N and N_2/N).

Proposition 1. Let $p \geqslant 2$ be a prime number. Then there are exactly $p + 1$ classes of maximally commutative sets of GBSs in $\mathbb{C}^p \otimes \mathbb{C}^p$.

In fact, these sets are characterized by $(0,1)\mathbb{Z}_p$, $(1,0)\mathbb{Z}_p$, and $(1,i)\mathbb{Z}_p$, $1 \leqslant i \leqslant p-1$, where $(a,b)\mathbb{Z}_p := \{(ai, bi) | i \in \mathbb{Z}_p\}$. With this proposition and Theorem 2, one would deduce Fan's result again. That is, if $\mathcal{S}$ is a set of p-dimensional GBSs with l elements and $l(l-1)/2 \leqslant p$, then $\mathcal{S}$ is locally distinguishable. In fact, in this setting, the number of elements in $\Delta\mathcal{S}$ [which does not contain (0,0)] is less than or equal to $l(l-1)/2$. However, $(0,1)\mathbb{Z}_p \setminus \{(0,0)\}$, $(1,0)\mathbb{Z}_p \setminus \{(0,0)\}$, and $(1,i)\mathbb{Z}_p \setminus \{(0,0)\}$ $(1 \leqslant i \leqslant p-1)$ are $p+1$ classes of mutually disjoint sets. Therefore, some MCS $\mathcal{C}$ must exist such that $\mathcal{C} \cap \Delta\mathcal{S} = \emptyset$.

Lemma 2. Each maximally commutative set of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ must have cardinality less than or equal to d.

This can be obtained by observing that a commutative set of unitary matrices can be simultaneously diagonalized and the elements of GBSs are mutually orthogonal. Moreover, one could easily verify the following lemma.

Lemma 3. Let $\mathcal{C}$ be a maximally commutative set of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$. If (i, j) belongs to $\mathcal{C}$, so does (ik, jk), where $k \in \mathbb{Z}_d$, i.e., $(i, j)\mathbb{Z}_d \subseteq \mathcal{C}$. Moreover, if both (i_1, j_1) and (i_2, j_2) belong to $\mathcal{C}$, so does $(i_1 + i_2, j_1 + j_2)$.

From this lemma, one can conclude that each maximally commutative set $\mathcal{C}$ can be written in the forms

$$\mathcal{C} = \bigcup_{k=1}^{n}(i_k, j_k)\mathbb{Z}_d, \quad \mathcal{C} = \sum_{k=1}^{n}(i_k, j_k)\mathbb{Z}_d. \tag{7}$$

Here $A + B := \{a + b|\ a \in A, b \in B\}$, where A and B are subsets of a group.

We find that the numbers of MCSs of GBSs are related to an interesting function (which is known as the σ function) in number theory. This function actually denotes the sum of all divisors of a positive integer. For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$, and $\sigma(16) = 1 + 2 + 4 + 8 + 16 = 31$. Generally, let $d = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$; then

$$\sigma(d) = \prod_{k=1}^{l}\left(1 + p_k + \cdots + p_k^{n_k}\right).$$

Theorem 3. Structure characterization of MCSs. Let $d \geqslant 3$ be an integer. For each pair (i, j) in $\mathbb{Z}_d \times \mathbb{Z}_d$, where $i \neq 0$, we define the following set:

$$\mathcal{C}_{i,j} := \{(x, y) \in \mathbb{Z}_d \times \mathbb{Z}_d | \begin{vmatrix} i & j \\ x & y \end{vmatrix} \equiv 0 \mod d, x \in i\mathbb{Z}_d\}.$$

Then $\mathcal{C}_{i,j}$ is a MCS of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ with exactly d elements. Moreover, if we define $\mathcal{C}_{0,0} := \{(0, y)|y \in \mathbb{Z}_d\}$, then every MCS of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ must be one of $\mathcal{C}_{i,j}$ with $i \neq 0$ or $\mathcal{C}_{0,0}$. There are exactly $\sigma(d)$ classes of MCSs $\mathcal{S}_{\mathrm{MC},d}$ which can be listed as follows:

$$\mathcal{S}_{\mathrm{MC},d} := \{\mathcal{C}_{i,j}|d = ik, \quad 0 \leqslant j \leqslant k - 1\} \cup \{\mathcal{C}_{0,0}\}.$$

Proof. First, we show that the cardinality of each $\mathcal{C}_{i,j}$ is equal to d. We denote by d_i the greatest common divisor of i and d. Then the set $i\mathbb{Z}_d := \{ij \in \mathbb{Z}_d \mid j \in \mathbb{Z}_d\}$ has exactly d/d_i elements. More exactly,

$$i\mathbb{Z}_d = \{ik|\ k = 0, 1, \ldots, \frac{d}{d_i} - 1\}.$$

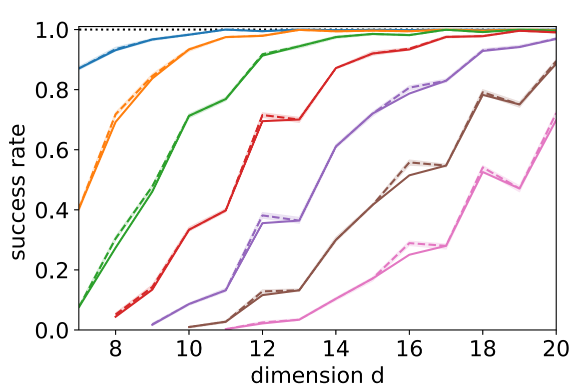

FIG. 2. For $n = 5, 6, 7, 8, 9, 10, 11$, we randomly generate $N = 100\,000$ sets of GBSs whose cardinalities are all n for $d = 7$–20, respectively. The solid lines represent the success rates of Theorem 1, and the dashed lines represent the success rates of Theorem 2. The lines from top to bottom represent sets with cardinality from 5 to 11, respectively. Here the starting point of each curve with respect to n has dimension $d \geqslant n$.

For each $x = ik$ ($k = 0, 1, \ldots, \frac{d}{d_i} - 1$), there are exactly d_i solutions of $y \in \mathbb{Z}_d$ that satisfy

$$\begin{vmatrix} i & j \\ x & y \end{vmatrix} \equiv 0 \mod d. \tag{8}$$

In fact, Eq. (8) is equivalent to $i(y - kj) \equiv 0 \mod d$, whose solutions can be expressed analytically as $y = kj + \frac{d}{d_i}l$, where $l = 0, 1, \ldots, d_i - 1$. Therefore, the set $\mathcal{C}_{i,j}$ can be expressed as

$$\left\{\left(ik, kj + \frac{d}{d_i}l\right)\middle|\ k = 0, 1, \ldots, \frac{d}{d_i}; l = 0, 1, \ldots, d_i - 1\right\}.$$

One can check that for two different pairs of (k_1, l_1) and (k_2, l_2) with the above conditions, the coordinates $(ik_1, k_1 j + \frac{d}{d_i}l_1) \neq (ik_2, k_2 j + \frac{d}{d_i}l_2)$. Therefore, the cardinality of $\mathcal{C}_{i,j}$ is equal to d.

Now we show that the elements in $\mathcal{C}_{i,j}$ are mutually commutative. In fact, for any two solutions $(ik_1, k_1 j + \frac{d}{d_i}l_1)$ and $(ik_2, k_2 j + \frac{d}{d_i}l_2)$, we have

$$\begin{vmatrix} ik_1 & k_1 j + \frac{d}{d_i}l_1 \\ ik_2 & k_2 j + \frac{d}{d_i}l_2 \end{vmatrix} = \frac{i}{d_i}(k_1 l_2 - k_2 l_1)d, \tag{9}$$

which is always equal to $0 \mod d$ as d_i divides i.

Therefore, each $\mathcal{C}_{i,j}$ is a commutative set of GBSs with cardinality d. By Lemma 2, each $\mathcal{C}_{i,j}$ must also be maximal.

Next, we show that for every MCS $\mathcal{C}$, it must be one of $\mathcal{C}_{i,j}$ with $i \neq 0$ or $\mathcal{C}_{0,0}$. For any maximally commutative set $\mathcal{C}$ of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$, from Eq. (7), $(x_k, y_k) \in \mathcal{C}$ ($k = 1, \ldots, n$) exist such that

$$\mathcal{C} = \sum_{k=1}^{n}(x_k, y_k)\mathbb{Z}_d.$$

If all x_k are equal to zero, one must conclude that $\mathcal{C} = \mathcal{C}_{0,0}$. If not, let i denote the greatest common divisor of $x_1, x_2, \ldots, x_n$ and d, which is not equal to zero in this case. There exist $r_k \in \mathbb{Z}_d$ such that $i = \sum_{k=1}^{n} r_k x_k$ (following Ref. [68], Theorem 1.4, we have $i = R_0 d + \sum_{k=1}^{n} R_k x_k$, $R_i \in \mathbb{Z}$, then taking modulus d). We define $j = \sum_{k=1}^{n} r_k y_k$. By Lemma 3, we have $(i, j) \in \mathcal{C}$. Both (x_k, y_k) and (i, j) are in $\mathcal{C}$. By the definition of i, for each k, the element $x_k \in i\mathbb{Z}_d$. As both (x_k, y_k) and (i, j) are in $\mathcal{C}$, we have $iy_k - jx_k \equiv 0 \mod d$. Therefore, by the definition of $\mathcal{C}_{i,j}$, for each k, the element $(x_k, y_k) \in \mathcal{C}_{i,j}$. From Lemma 3 again, we have $\mathcal{C} \subseteq \mathcal{C}_{i,j}$. However, both sets are maximally commutative sets of GBSs. Therefore, $\mathcal{C}$ must equal $\mathcal{C}_{i,j}$.

In the following, we show that each $\mathcal{C}_{x,y}$ ($x \neq 0$) belongs to one of $\mathcal{S}_{\mathrm{MC},d}$. We denote by d_x the greatest common divisor of x and d (we might assume $x = c_x d_x$, where $c_x \in \mathbb{Z}$). So $d_x = qx + rd$ for some integers q, r. A unique $j \in \{0, 1, \ldots, k_x - 1\}$ (where $k_x d_x = d$) exists such that

$$qy - j \in k_x\mathbb{Z}_d.$$

That is, $qy - j = k_x l_x$ for some $l_x \in \mathbb{Z}_d$. For this j, we have the following equation:

$$\begin{vmatrix} d_x & j \\ x & y \end{vmatrix} = \begin{vmatrix} d_x & qy - k_x l_x \\ x & y \end{vmatrix} = (d_x - qx)y + l_x k_x x,$$

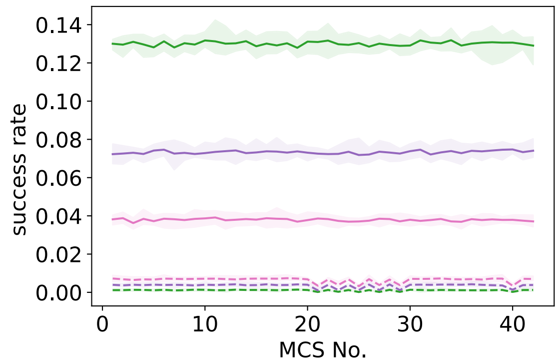

FIG. 3. We consider the cases $d = 20$ and $n = 9, 10$, or 11 (which correspond to green, purple, and pink curves, respectively). We randomly generate 100 000 sets (which are separated into 10 equal classes) of GBSs whose cardinalities are all $n = 9, 10, 11$, respectively. Each solid curve shows the success rates for the $\sigma(20) = 42$ classes of MCSs. The dashed lines represent the success rates for the 42 classes of MCSs such that the local distinguishability of the samples can be detected by only one class of the MCS itself.

which is equal $(ry + l_x c_x)d \equiv 0$ under $\mod d$. By definition, $x \in d_x\mathbb{Z}_d$. Therefore, we have $(x, y) \in \mathcal{C}_{d_x,j}$. As the elements in $\mathcal{C}_{d_x,j}$ all commute with each other, for any $(x_1, y_1) \in \mathcal{C}_{d_x,j}$, we have

$$\begin{vmatrix} x & y \\ x_1 & y_1 \end{vmatrix} \equiv 0 \mod d.$$

Note that for $d_x\mathbb{Z}_d = x\mathbb{Z}_d$, we have $x_1 \in x\mathbb{Z}_d$. Therefore, $\mathcal{C}_{d_x,j} \subseteq \mathcal{C}_{x,y}$. By the maximality, we must have $\mathcal{C}_{x,y} = \mathcal{C}_{d_x,j}$. Therefore, we conclude that every $\mathcal{C}_{x,y}$ must be one of the elements in $\mathcal{S}_{\mathrm{MC},d}$

On the other hand, we need to show that the sets in $\mathcal{S}_{\mathrm{MC},d}$ are mutually different. Clearly, $\mathcal{C}_{0,0}$ is different from all the other sets. Let $\mathcal{C}_{i_1,j_1}$ and $\mathcal{C}_{i_2,j_2}$ be any two members of $\mathcal{S}_{\mathrm{MC},d}$ where $(i_1, j_1) \neq (i_2, j_2)$ and i_1, i_2 are nonzero. As $d = i_1k_1$, if $i_1 = i_2$, we have $i_1 j_2 - i_2 j_1 = i_1(j_2 - j_1)$, which lies between $-(d-1)$ and $d-1$ but is not equal to zero. Hence, the pairs (i_1, j_1) and (i_2, j_2) do not commute. Therefore, $\mathcal{C}_{i_1,j_1} \neq \mathcal{C}_{i_2,j_2}$. If $i_1 \neq i_2$, we can assume that $i_1 < i_2$ without loss of generality. As both i_1 and i_2 are divisors of d, we can check that $i_1 \notin i_2\mathbb{Z}_d$. Therefore, by definition, $(i_1, j_1) \notin \mathcal{C}_{i_2,j_2}$. Hence, we also have $\mathcal{C}_{i_1,j_1} \neq \mathcal{C}_{i_2,j_2}$.

Each divisor i $(1 \leqslant i < d)$ of d contributes to d/i classes of MCSs to $\mathcal{S}_{\mathrm{MC},d}$. Therefore,

$$|\mathcal{S}_{\mathrm{MC},d}| = 1 + \sum_{i|d,1\leqslant i<d} d/i = \sum_{i|d} d/i = \sigma(d).$$

This completes the proof.

From the above theorem, we know that there are $\sigma(d)$ classes of MCSs of d-dimensional GBSs. Among these MCSs, are there any differences in their abilities to detect the local distinguishability of sets of GBSs? Is there any redundant MCS (whose ability is strictly weaker than some other MCS) in detecting the local discrimination of generalized Bell sets? We present some numerical results for these two questions.

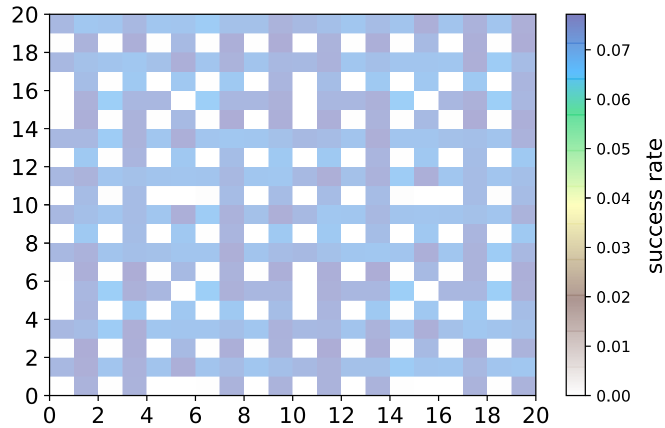

FIG. 4. We consider the case with $d = 20$ and $n = 10$. This plot shows the success rates for each detector [see Eq. (6)] indicated by the coordinates $(i, j) \in \mathbb{Z}_{20} \times \mathbb{Z}_{20}$. We randomly generate 100 000 sets of GBSs whose cardinalities are all $n = 10$.

The three solid lines in Fig. 3 imply that the success rates of all MCSs are almost equal to each other [one should compare this with the detectors defined in Eq. (6); see Fig. 4]. The three dashed lines imply that each class of MCSs is irredundant in the sense that for each MCS $\mathcal{C}$, some set $\mathcal{S}$ exists whose local distinguishability can be detected only by $\mathcal{C}$ and not by other MCSs.

IV. CONCLUSION AND DISCUSSION

In this paper, we studied the problem of local distinguishability of generalized Bell states. First, we provided a review of some important methods for detecting the local distinguishability of GBSs. Motivated by a recent method derived by Yuan *et al.* [67], we introduced the concept of a maximally commutative set of GBSs. Surprisingly, we found that each MCS is useful for detecting the local distinguishability of GBSs. More exactly, given a set $\mathcal{S}$ of GBSs, if some MCS $\mathcal{C}$ exists such that the difference set $\Delta\mathcal{S}$ of $\mathcal{S}$ is disjoint with or contained in $\mathcal{C}$, then the set $\mathcal{S}$ can be one way distinguishable. This method is stronger than that in Ref. [67], and it motivates us to find all the MCSs of a given dimension. Indeed, we presented a complete structure characterization of MCSs in Theorem 3.

However, a MCS gives a sufficient condition only for local distinguishability, and it is not necessary. It would be interesting to derive an easy to check condition for the local distinguishability of GBSs which is both sufficient and necessary. In addition, it would be interesting to check whether Fan's results can be extended to systems without the assumption about the dimension of local systems. A weaker form is as follows: given any integer l, does some D (which depends on l) exist such that if $d \geqslant D$, then any l GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ are locally distinguishable? As far as we known, this problem has been solved only for the case $l = 3$. We conjecture that this holds for all other cases. It is well known that at most d maximally entangled states can be locally distinguished. Therefore, it would be interesting to find all the one-way locally distinguishable sets of GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ with cardinality d.

Note that our method here can be generalized to any maximally entangled basis whose defining unitary matrices $\mathcal{B}$ satisfy the following: for any $U, V \in \mathcal{B}$ some $W \in \mathcal{B}$ exists such that $U^\dagger V \propto W$. The lattice qudit basis [57] is such an example. From their proof, any locally distinguishable set of lattice qudit bases that can be detected in Ref. [57] can always be detected by a MCS of lattice qudit bases. Therefore, our method can also be seen as a generalization of the one in [57]. Therefore, it would also be interesting to give a complete characterization of the MCS of lattice qudit bases and study its application to local discrimination. Finally, it would be interesting to provide some operational significance of the MCSs introduced in our work.

ACKNOWLEDGMENTS

The authors are grateful for the anonymous referee's suggestions to improve the quality of this paper. M.-S.L. and Y.-L.W. were supported by the National Natural Science Foundation of China under Grants No. 12005092, No. 11901084, and No. 61773119, the China Postdoctoral Science Foundation (Grant No. 2020M681996), and the Research Startup Funds of DGUT (Grant No. GC300501-103). F.S. was supported by the NSFC under Grants No. 11771419 and No.12171452, the Anhui Initiative in Quantum Information Technologies under Grant No. AHY150200, and the National Key Research and Development Program of China under Grant No. 2020YFA0713100.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2004).

[2] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Phys. Rev. A **59**, 1070 (1999).

[3] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States, Phys. Rev. Lett. **85**, 4972 (2000).

[4] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding Bits in Bell States, Phys. Rev. Lett. **86**, 5807 (2001).

[5] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).

[6] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).

[7] R. Rahaman and M. G. Parker, Quantum scheme for secret sharing based on local distinguishability, Phys. Rev. A **91**, 022330 (2015).

[8] J. Wang, L. Li, H. Peng, and Y. Yang, Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states, Phys. Rev. A **95**, 022320 (2017).

[9] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible Product Bases and Bound Entanglement, Phys. Rev. Lett. **82**, 5385 (1999).

[10] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, Distinguishability of Bell states, Phys. Rev. Lett. **87**, 277902 (2001).

[11] J. Walgate and L. Hardy, Nonlocality, Asymmetry, and Distinguishing Bipartite States, Phys. Rev. Lett. **89**, 147901 (2002).

[12] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local Indistinguishability: More Nonlocality with Less Entanglement, Phys. Rev. Lett. **90**, 047902 (2003).

[13] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible product bases, uncompletable product bases and bound entanglement, Commun. Math. Phys. **238**, 379 (2003).

[14] S. De Rinaldis, Distinguishability of complete and unextendible product bases, Phys. Rev. A **70**, 022309 (2004).

[15] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Distinguishability of maximally entangled states, Phys. Rev. A **70**, 022304 (2004).

[16] H. Fan, Distinguishability and Indistinguishability by Local Operations and Classical Communication, Phys. Rev. Lett. **92**, 177905 (2004).

[17] M. Nathanson, Distinguishing bipartite orthogonal states by LOCC: Best and worst cases, J. Math. Phys. **46**, 062103 (2005).

[18] J. Watrous, Bipartite Subspaces Having no Bases Distinguishable by Local Operations and Classical Communication, Phys. Rev. Lett. **95**, 080505 (2005).

[19] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Bounds on Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication, Phys. Rev. Lett. **96**, 040501 (2006).

[20] J. Niset and N. J. Cerf, Multipartite nonlocality without entanglement in many dimensions, Phys. Rev. A **74**, 052103 (2006).

[21] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Distinguishing Arbitrary Multipartite Basis Unambiguously Using Local Operations and Classical Communication, Phys. Rev. Lett. **98**, 230502 (2007).

[22] Y. Feng and Y.-Y. Shi, Characterizing locally indistinguishable orthogonal product states, IEEE Trans. Inf. Theory **55**, 2799 (2009).

[23] R. Y. Duan, Y. Feng, Y. Xin, and M. S. Ying, Distinguishability of quantum states by separable operations, IEEE Trans. Inf. Theory **55**, 1320 (2009).

[24] S. Bandyopadhyay, S. Ghosh, and G. Kar, LOCC distinguishability of unilaterally transformable quantum states, New J. Phys. **13**, 123013 (2011).

[25] S. Bandyopadhyay, More Nonlocality with Less Purity, Phys. Rev. Lett. **106**, 210402 (2011).

[26] N. Yu, R. Duan, and M. Ying, Four Locally Indistinguishable Ququad-Ququad Orthogonal Maximally Entangled States, Phys. Rev. Lett. **109**, 020506 (2012).

[27] A. Cosentino, Positive partial transpose indistinguishable states via semidefinite programming, Phys. Rev. A **87**, 012321 (2013).

[28] M. Nathanson, Three maximally entangled states can require two-way local operations and classical communication for local discrimination, Phys. Rev. A **88**, 062316 (2013).

[29] M.-S. Li, Y.-L. Wang, S.-M. Fei, and Z.-J. Zheng, d locally indistinguishable maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$, Phys. Rev. A **91**, 042318 (2015).

[30] S. X. Yu and C. H. Oh, Detecting the local indistinguishability of maximally entangled states, arXiv:1502.01274.

[31] M.-S. Li, S.-M. Fei, Z.-X. Xiong, and Y.-L. Wang, Twist-teleportation-based local discrimination of maximally entangled states, Sci. China Phys. Mech. Astron. **63**, 280312 (2020).

[32] S. Bandyopadhyay and M. Nathanson, Tight bounds on the distinguishability of quantum states under separable measurements, Phys. Rev. A **88**, 052313 (2013).

[33] A. Cosentino and V. Russo, Small sets of locally indistinguishable orthogonal maximally entangled states, Quantum Inf. Comput. **14**, 1098 (2014).

[34] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, Limitations on separable measurements by convex optimization, IEEE Trans. Inf. Theory, **61**, 3593 (2015).

[35] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, A framework for bounding nonlocality of state discrimination, Commun. Math. Phys. **323**, 1121 (2013).

[36] Y.-H. Yang, F. Gao, G.-J. Tian, T.-Q. Cao, and Q.-Y. Wen, Local distinguishability of orthogonal quantum states in a $2 \otimes 2 \otimes 2$ system, Phys. Rev. A **88**, 024301 (2013).

[37] Z.-C. Zhang, F. Gao, G.-J. Tian, T.-Q. Cao, and Q.-Y. Wen, Nonlocality of orthogonal product basis quantum states, Phys. Rev. A **90**, 022313 (2014).

[38] Z.-C. Zhang, F. Gao, S.-J. Qin, Y.-H. Yang, and Q.-Y. Wen, Nonlocality of orthogonal product states, Phys. Rev. A **92**, 012332 (2015).

[39] Y.-L. Wang, M.-S. Li, Z.-J. Zheng, and S.-M. Fei, Nonlocality of orthogonal product-basis quantum states, Phys. Rev. A **92**, 032313 (2015).

[40] G.-B. Xu, Q.-Y. Wen, S.-J. Qin, Y.-H. Yang, and F. Gao, Quantum nonlocality of multipartite orthogonal product states, Phys. Rev. A **93**, 032341 (2016).

[41] Z.-C. Zhang, F. Gao, Y. Cao, S.-J. Qin, and Q.-Y. Wen, Local indistinguishability of orthogonal product states, Phys. Rev. A **93**, 012314 (2016).

[42] X. Zhang, X. Tan, J. Weng, and Y. Li, LOCC indistinguishable orthogonal product quantum states, Sci. Rep. **6**, 28864 (2016).

[43] Y.-L. Wang, M.-S. Li, Z.-J. Zheng, and S.-M. Fei, The local indistinguishability of multipartite product states, Quantum Inf. Process. **16**, 5 (2017).

[44] Z.-C. Zhang, K.-J. Zhang, F. Gao, Q.-Y. Wen, and C. H. Oh, Construction of nonlocal multipartite quantum states, Phys. Rev. A **95**, 052344 (2017).

[45] S. Halder, Several nonlocal sets of multipartite pure orthogonal product states, Phys. Rev. A **98**, 022303 (2018).

[46] M.-S. Li and Y.-L. Wang, Alternative method for deriving nonlocal multipartite product states, Phys. Rev. A **98**, 052352 (2018).

[47] D.-H. Jiang and G.-B. Xu, Nonlocal sets of orthogonal product states in arbitrary multipartite quantum system, Phys. Rev. A **102**, 032211 (2020).

[48] S. Halder and C. Srivastava, Locally distinguishing quantum states with limited classical communication, Phys. Rev. A **101**, 052313 (2020).

[49] S. Halder and R. Sengupta, Distinguishability classes, resource sharing, and bound entanglement distribution, Phys. Rev. A **101**, 012311 (2020).

[50] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Strong Quantum Nonlocality without Entanglement, Phys. Rev. Lett. **122**, 040403 (2019).

[51] Z.-C. Zhang and X. Zhang, Strong quantum nonlocality in multipartite quantum systems, Phys. Rev. A **99**, 062108 (2019).

[52] F. Shi, M. Hu, L. Chen, and X. Zhang, Strong quantum nonlocality with entanglement, Phys. Rev. A **102**, 042202 (2020).

[53] P. Yuan, G. J. Tian, and X. M. Sun, Strong quantum nonlocality without entanglement in multipartite quantum systems, Phys. Rev. A **102**, 042228 (2020).

[54] Y.-L. Wang, M.-S. Li, and M.-H. Yung, Graph-connectivity-based strong quantum nonlocality with genuine entanglement, Phys. Rev. A **104**, 012424 (2021).

[55] M. Banik, T. Guha, M. Alimuddin, G. Kar, S. Halder, and S. S. Bhattacharya, Multicopy Adaptive Local Discrimination: Strongest Possible Two-Qubit Nonlocal Bases, Phys. Rev. Lett. **126**, 210505 (2021).

[56] D. Ha and Y. Kwon, Quantum nonlocality without entanglement: Explicit dependence on prior probabilities of nonorthogonal mirror-symmetric states, npj Quantum Inf. **7**, 81 (2021).

[57] G.-J. Tian, S.-X. Yu, F. Gao, Q.-Y. Wen, and C. H. Oh, Local discrimination of qudit lattice states via commutativity, Phys. Rev. A **92**, 042320 (2015).

[58] G.-J. Tian, S.-X. Yu, F. Gao, Q.-Y. Wen, and C. H. Oh, Local discrimination of four or more maximally entangled states, Phys. Rev. A **91**, 052314 (2015).

[59] G.-J. Tian, S.-X. Yu, F. Gao, and Q.-Y. Wen, Classification of locally distinguishable and indistinguishable sets of maximally entangled states, Phys. Rev. A **94**, 052315 (2016).

[60] T. Singal, R. Rahaman, S. Ghosh, and G. Kar, Necessary condition for local distinguishability of maximally entangled states: Beyond orthogonality preservation, Phys. Rev. A **96**, 042314 (2017).

[61] Y.-L. Wang, M.-S. Li, S.-M. Fei, and Z.-J. Zheng, The local distinguishability of any three generalized Bell states, Quantum Inf. Process. **16**, 126 (2017).

[62] J. T. Yuan, Y. H. Yang, and C. H. Wang, Constructions of locally distinguishable sets of maximally entangled states which require two-way LOCC, J. Phys. A **53**, 505304 (2020).

[63] Y. H. Yang, G. F. Mu, J. T. Yuan, and C. H. Wang, Distinguishability of generalized Bell states in arbitrary dimension system via one-way local operations and classical communication, Quantum Inf. Process. **20**, 52 (2021).

[64] T. Hashimoto, M. Horibe, and A. Hayashi, Simple criterion for local distinguishability of generalized Bell states in prime dimension, Phys. Rev. A **103**, 052429 (2021).

[65] B. Baumgartner, B. C. Hiesmayr, and H. Narnhofer, State space for two qutrits has a phase space structure in its core, Phys. Rev. A **74**, 032327 (2006).

[66] R. A. Bertlmann and P. Krammer, Bloch vectors for qudits, J. Phys. A **41**, 235303 (2008).

[67] J.-T. Yuan, Y.-H. Yang, and C.-H. Wang, Necessary and sufficient conditions for local discrimination of generalized Bell states: Finding out all locally indistinguishable sets of generalized Bell states, arXiv:2109.07390.

[68] M. B. Nathanson, *Elementary Methods in Number Theory*, Graduate Texts in Mathematics Vol. 195 (Springer, New York, 2000).