Simple criterion for local distinguishability of generalized Bell states in prime dimension

T. Hashimoto, M. Horibe, and A. Hayashi
Department of Applied Physics, University of Fukui, Fukui 910-8507, Japan

(Received 15 February 2021; accepted 18 May 2021; published 25 May 2021)

Local distinguishability of sets of generalized Bell states (GBSs) is investigated. We first clarify the conditions such that a set of GBSs can be locally transformed to a certain type of GBS set that is easily distinguishable within local operations and one-way classical communication. We then show that if the space dimension d is a prime, these conditions are necessary and sufficient for sets of d GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ to be locally distinguishable. Thus we obtain a simple computable criterion for local distinguishability of sets of d GBSs in prime dimension d.

DOI: 10.1103/PhysRevA.103.052429

I. INTRODUCTION

A set of orthogonal quantum states can be perfectly distinguished, though the laws of quantum mechanics do not allow one to distinguish nonorthogonal quantum states perfectly [1–4]. However, the issue is more involved when the states are shared by several parties and they are allowed to perform only local operations and classical communication (LOCC). Any two bipartite orthogonal states can be distinguished by one-way LOCC [5]. For sets of three orthogonal states, however, some sets require two-way LOCC to distinguish, and some sets are not even locally distinguishable [6,7]. In the space of $\mathbb{C}^d \otimes \mathbb{C}^d$, there are d^2 orthogonal states. However, it is impossible to locally distinguish more than d orthogonal maximally entangled states perfectly in $\mathbb{C}^d \otimes \mathbb{C}^d$ [8–10].

The generalized Bell states (GBSs) are typical examples of orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$, and much attention has been paid to clarifying local distinguishability of sets of GBSs [11–18]. In particular, some sufficient conditions for GBS sets to be one-way LOCC distinguishable or indistinguishable have been discussed in [11,15,18].

In this paper, we present a simple computable criterion for local distinguishability (not limited to be one way) of sets of d GBSs in prime dimension d. In Sec. III, we clarify the conditions such that a set of GBSs can be locally transformed to a certain type of GBS set that can be distinguished by a simple strategy within one-way LOCC. In Sec. IV, if d is a prime, these conditions are shown to be necessary and sufficient for sets of d GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ to be locally distinguishable. Discussion including the case of composite-number dimensions is given in Sec. V.

II. GENERALIZED BELL STATES

Consider bipartite pure states shared by Alice and Bob in space $\mathbb{C}^d \otimes \mathbb{C}^d$. It is convenient to represent a maximally entangled state (MES) by a unitary operator W in $\mathbb{C}^d$ (see, e.g., [8–11]) as

$$|W\rangle^{AB} = \frac{1}{\sqrt{d}} \sum_{a,b=0}^{d-1} W_{ab}\, |a\rangle^A \otimes |b\rangle^B = (W \otimes \mathbf{1})\, |\mathbf{1}\rangle^{AB}, \tag{1}$$

where

$$|\mathbf{1}\rangle^{AB} = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle^A \otimes |a\rangle^B, \tag{2}$$

with $\{|a\rangle\}_{a=0}^{d-1}$ being an orthonormal base of $\mathbb{C}^d$. We note that W denotes both the bipartite state and the unitary operator in this useful notation.

The inner product between two MES states $|W_1\rangle$ and $|W_2\rangle$, expressed in terms of the corresponding operators W_1 and W_2, is given by

$$\langle W_1|W_2\rangle = \frac{1}{d} \operatorname{tr} W_1^\dagger W_2. \tag{3}$$

Suppose Alice and Bob perform some local unitary operations given by A and B, respectively. We find that a MES state $|W\rangle$ is transformed to another MES state $|AWB^T\rangle$ as

$$(A \otimes B)\, |W\rangle = |AWB^T\rangle, \tag{4}$$

where the superscript T represents the transposition with respect to the base $\{|a\rangle\}_{a=0}^{d-1}$.

Generalized Bell states (GBSs) belong to a special class of MESs, where the unitary operator W is given by

$$W_{m,n} = X^m Z^n \; (m, n = 0, 1, \ldots, d-1). \tag{5}$$

Here, X and Z are generalized Pauli operators defined as

$$X = \sum_{a=0}^{d-1} |a+1\rangle \langle a|, \tag{6}$$

$$Z = \sum_{a=0}^{d-1} \omega_d^a\, |a\rangle \langle a|, \tag{7}$$

where we employ the periodic convention for the base states; that is, $|d+a\rangle = |a\rangle$, and ω_d is a dth primitive root of unity, $\omega_d = e^{2\pi i/d}$. It is readily checked that the unitary operators X and Z satisfy the following relations:

$$X^d = Z^d = \mathbf{1},\ ZX = \omega_d XZ. \tag{8}$$

We can also see that the set of d^2 unitaries $\{W_{m,n}\}_{m,n=0}^{d-1}$ in Eq. (5) is an orthonormal base in the operator space of $\mathbb{C}^d$,

$$\mathrm{tr}\, W_{m,n}^\dagger W_{m',n'} = d\delta_{mm'}\delta_{nn'}. \tag{9}$$

This together with Eq. (3) implies that d^2 GBSs $\{|W_{m,n}\rangle\}_{m,n=0}^{d-1}$ form an orthonormal base in $\mathbb{C}^d \otimes \mathbb{C}^d$, and therefore they are perfectly distinguishable by global measurements in the total space $\mathbb{C}^d \otimes \mathbb{C}^d$. However, it is known that Alice and Bob cannot distinguish more than d MESs in $d \times d$ dimensions, if they are restricted to employ local operations and classical communication (LOCC) [8–10].

Suppose we are given a set of ℓ GBSs $\mathcal{W} = \{|W_{m_i,n_i}\rangle\}_{i=1}^{\ell}$ with $\ell \leqslant d$. To specify a GBS set, we will use the following notations interchangeably:

$$\mathcal{W} = \{|W_{m_i,n_i}\rangle\}_{i=1}^{\ell} = \{W_{m_i,n_i}\}_{i=1}^{\ell} = \{(m_i,n_i)\}_{i=1}^{\ell}. \tag{10}$$

Our concern in this paper is what the conditions are for the set $\mathcal{W}$ to be distinguishable by LOCC.

Fan [11] noted that there is a special class of GBS sets for which one can easily find the way to distinguish the states with one-way LOCC. This is when all $m_i (i = 1, 2, \dots, \ell)$ are distinct, and GBS sets with this property will be called F-type sets in this paper. Assume the set $\mathcal{W}$ is F type. The states in the set are explicitly given by

$$|W_{m_i,n_i}\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} \omega_d^{n_i a} |a+m_i\rangle |a\rangle \ \ (i = 1, \dots, \ell). \tag{11}$$

Suppose Alice and Bob locally perform the projective measurement in the base $\{|a\rangle\}_{a=0}^{d-1}$ and compare their outcomes. Then they obtain m_i, thereby identifying i since all m_i are distinct.

III. LOCAL UNITARY TRANSFORMATIONS AND F-EQUIVALENT SET

Suppose a GBS set $\mathcal{W} = \{(m_i,n_i)\}_{i=1}^{\ell}$ is transformed to another set $\mathcal{W}' = \{(m_i',n_i')\}_{i=1}^{\ell}$ by some local unitary transformations,

$$\begin{aligned} U \otimes V\, |X^{m_i}Z^{n_i}\rangle &= |UX^{m_i}Z^{n_i}V^T\rangle \\ &\sim |X^{m_i'}Z^{n_i'}\rangle \ \ (i = 1, \dots, \ell), \end{aligned} \tag{12}$$

where the symbol "$\sim$" means equality up to a global phase. It is clear that local distinguishability is invariant under local unitary transformations. If a set $\mathcal{W}$ can be transformed to a F-type set $\mathcal{W}'$ (defined in the preceding section), the set $\mathcal{W}$ is also distinguishable by one-way LOCC [11].

Let us determine the most general form of local unitary operations that transform all GBS states to other GBS states, that is,

$$UX^mZ^nV^T \sim X^{m'}Z^{n'}\ (m,n = 0, \dots, d-1). \tag{13}$$

A GBS set $\mathcal{W}$ is called F equivalent if $\mathcal{W}$ can be transformed to a F-type set by this local unitary operation. By setting $m = n = 0$ in Eq. (13), we have

$$UV^T \sim X^{\mu_0}Z^{\nu_0}, \tag{14}$$

for some integers $0 \leqslant \mu_0, \nu_0 \leqslant d-1$. This implies

$$UX^mZ^nU^\dagger \sim X^{m''}Z^{n''}, \tag{15}$$

for some m'', n'', since

$$\begin{aligned} UX^mZ^nU^\dagger &= UX^mZ^nV^T(UV^T)^{-1} \\ &= X^{m'}Z^{n'}(X^{\mu_0}Z^{\nu_0})^{-1} \sim X^{m'-\mu_0}Z^{n'-\nu_0}. \end{aligned}$$

Some specific types of unitary operators U with this property have been used to study the F equivalence of GBS sets [11,18]. In this paper, we will employ more general unitary operators by establishing the necessary and sufficient conditions for the existence of unitary U with the property of Eq. (15).

First assume that Eq. (15) holds for some unitary U. Setting $m = 1, n = 0$ or $m = 0, n = 1$, we obtain

$$\begin{cases} X' &\equiv UXU^\dagger \sim X^\alpha Z^\gamma, \\ Z' &\equiv UZU^\dagger \sim X^\beta Z^\delta, \end{cases} \tag{16}$$

for some integers $0 \leqslant \alpha, \beta, \gamma, \delta \leqslant d-1$. It is clear that the relations given by Eq. (8) persist under a unitary transformation, implying $X'^d = Z'^d = \mathbf{1}$ and $Z'X' = \omega_d X'Z'$. From the latter relation, we find that $\alpha, \beta, \gamma, \delta$ should satisfy

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv 1 \pmod{d}. \tag{17}$$

Conversely, assume that integers $0 \leqslant \alpha, \beta, \gamma, \delta \leqslant d-1$ satisfy the relation (17), and define

$$\begin{cases} X' &\sim X^\alpha Z^\gamma, \\ Z' &\sim X^\beta Z^\delta. \end{cases} \tag{18}$$

We have the relation $Z'X' = \omega_d X'Z'$ and, furthermore, we can evidently choose global phase factors of X', Z' such that $X'^d = Z'^d = \mathbf{1}$ since $(X^\alpha Z^\gamma)^d \sim (X^\beta Z^\delta)^d \sim \mathbf{1}$. We can show that the set of operators $\{X', Z'\}$ is unitary equivalent to $\{X, Z\}$; that is, there exists a unitary operator such that $X' = UXU^\dagger$, $Z' = UZU^\dagger$. This can be seen in the following way: Let us take an eigenstate $|\psi_0\rangle$ of Z' with an eigenvalue being a dth root of unity, $\omega_d^{k_0}$. Using the relation $Z'X' = \omega_d X'Z'$ repeatedly, we find that $|\psi_k\rangle \equiv X'^k |\psi_0\rangle$ is an eigenstate of Z' with eigenvalue $\omega_d^{k_0+k}$. Now it is clear that the relations $X' = UXU^\dagger$, $Z' = UZU^\dagger$ hold if we take $U = \sum_{k=0}^{d-1} |\psi_{k-k_0}\rangle \langle k|$.

Thus we establish the following lemma:

Lemma 1. There exists a unitary operator U such that

$$\begin{cases} UXU^\dagger \sim X^\alpha Z^\gamma, \\ UZU^\dagger \sim X^\beta Z^\delta, \end{cases} \tag{19}$$

if and only if integers $0 \leqslant \alpha, \beta, \gamma, \delta \leqslant d-1$ satisfy

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv 1 \pmod{d}. \tag{20}$$

All 2×2 matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with integer entries satisfying $0 \leqslant \alpha, \beta, \gamma, \delta \leqslant d-1$ and the condition given by Eq. (20) form a group under matrix multiplication modulo d. This group is denoted by $Sp(d)$. We note that U is not unique for a given element of $Sp(d)$. It depends on global phase factors that are not specified in Eq. (19). The phase of U itself is not determined either since the unitary transformations of Eq. (19) are independent of a phase change, $U \to e^{i\theta}U$. For discussions on explicit forms of U corresponding to a given element of $Sp(d)$, see Ref. [19], where a Euclidean type of algorithm to construct U is presented.

Using $UX^mZ^nV^T = UX^mZ^nU^\dagger(UV^T)$ together with Eqs. (14) and (19), we conclude that operator X^mZ^n transforms under local transformations as

$$UX^mZ^nV^T \sim X^{m'}Z^{n'}, \tag{21}$$

where

$$\begin{pmatrix} m' \\ n' \end{pmatrix} \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} + \begin{pmatrix} \mu_0 \\ \nu_0 \end{pmatrix} \pmod d. \tag{22}$$

Now it is easy to write the conditions for a GBS set $\mathcal{W} = \{(m_i, n_i)\}_{i=1}^{\ell}$ to be F equivalent. The conditions are that

$$m_i' = m_i\alpha + n_i\beta + \mu_0 \ (i = 1, \dots, \ell) \tag{23}$$

are all distinct modulo d for some $Sp(d)$ matrix $(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix})$ and an integer $0 \leqslant \mu_0 \leqslant d-1$.

It is clear that the integer μ_0 can be omitted in the above conditions. As for α and β, it is assumed that they are the elements of some $Sp(d)$ matrix $(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix})$. However, these constraints can be lifted; that is, α and β are any integers. This can be seen in the following way: Suppose that $m_i\alpha + n_i\beta$ are all distinct modulo d for some integers α and β. It is clear that $m_i\alpha_1 + n_i\beta_1$ are also all distinct modulo d, where $\alpha_1 \equiv \alpha, \beta_1 \equiv \beta \pmod d$ and $0 \leqslant \alpha_1, \beta_1 \leqslant d-1$. Write $\alpha_1 = c\alpha_2, \beta_1 = c\beta_2$ with $c = \gcd(\alpha_1, \beta_1)$. Note that $\gcd(\alpha_2, \beta_2) = 1$. Then we find that $m_i\alpha_2 + n_i\beta_2$ are all distinct modulo d and there are some integers $0 \leqslant \gamma_2, \delta_2 \leqslant d-1$ such that $\alpha_2\delta_2 - \beta_2\gamma_2 \equiv 1 \pmod d$.

Thus we arrive at the following theorem:

Theorem 1. A set of ℓ GBSs $\mathcal{W}$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ is F equivalent and therefore one-way LOCC distinguishable if and only if

$$m_i\alpha + n_i\beta \ (i = 1, \dots, \ell) \tag{24}$$

are all distinct modulo d for some integers α and β.

Theorem 1 gives a sufficient condition for a GBS set $\mathcal{W}$ to be distinguishable by one-way LOCC. We show that the same condition can be derived from a different point of view. Ghosh *et al.* showed that a GBS set $\mathcal{W}$ is one-way LOCC distinguishable if and only if there is some state $|\phi\rangle$ such that $\{X^{m_i}Z^{n_i}|\phi\rangle\}_i^{\ell}$ are pairwise orthogonal [8]. This orthogonality is expressed as

$$\langle\phi|X^{m_i-m_j}Z^{n_i-n_j}|\phi\rangle = 0, \ i \neq j. \tag{25}$$

We show that in some cases, the state $|\phi\rangle$ satisfying this equation can easily be found. To do so, we will employ a general property of two unitary operators. Let V and V' be unitary, and assume that $VV' = \lambda V'V$ with $\lambda \neq 1$. For any eigenstate $|\phi\rangle$ of V, we find

$$\langle\phi|V'|\phi\rangle = \lambda\,\langle\phi|V^\dagger V'V|\phi\rangle = \lambda\,\langle\phi|V'|\phi\rangle\,. \tag{26}$$

From this, it follows that $\langle\phi|V'|\phi\rangle = 0$ since $\lambda \neq 1$.

Now let V be $X^{-\beta}Z^{\alpha}$ with some integers α, β and suppose that V does not commute with $V' = X^{m_i-m_j}Z^{n_i-n_j}$ for every $i \neq j$. This noncommutability can be expressed as the following conditions:

$$(m_i - m_j)\alpha + (n_i - n_j)\beta \neq 0 \pmod d, \ i \neq j, \tag{27}$$

which is equivalent to the conditions in Theorem 1. Taking $|\phi\rangle$ to be an eigenstate V, we obtain Eq. (25), which shows that the set $\mathcal{W}$ is one-way LOCC distinguishable.

IV. NECESSARY AND SUFFICIENT CONDITION FOR LOCAL DISTINGUISHABILITY IN THE CASE OF PRIME $\ell = d$

Theorem 1 in the preceding section gives a sufficient condition for a GBS set $\mathcal{W} = \{|W_{m_i,n_i}\rangle\}_{i=1}^{\ell}$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ to be distinguishable by one-way LOCC for arbitrary ℓ and d. In this section, we consider the case where d is a prime number and $\ell = d$. Then it will be shown that the condition given in Theorem 1 is also necessary for one-way LOCC distinguishability; F equivalence is equivalent to one-way LOCC distinguishability. Furthermore, we will see that the restriction to one-way LOCC can be removed by using a lemma given by Yu and Oh [20].

Let us assume that a set of d GBSs $\mathcal{W} = \{|W_{m_i,n_i}\rangle\}_{i=1}^{d}$ is one-way LOCC distinguishable and show that the set $\mathcal{W}$ is then F equivalent. According to Ghosh *et al.*, there is a normalized state $|\phi\rangle$ such that

$$\langle\phi|W_{m_i,n_i}^\dagger W_{m_j,n_j}|\phi\rangle = \delta_{ij} \ (i, j = 1, \dots, d), \tag{28}$$

which implies

$$\sum_{i=1}^{d} W_{m_i,n_i}\,|\phi\rangle\,\langle\phi|\,W_{m_i,n_i}^\dagger = \mathbf{1}. \tag{29}$$

For $|\phi\rangle\,\langle\phi|$ on the left-hand side, we substitute its expanded form in terms of the complete operator set $\{W_{m,n}\}_{m,n=0}^{d-1}$,

$$|\phi\rangle\,\langle\phi| = \frac{1}{d}\sum_{m,n=0}^{d-1}\langle\phi|W_{m,n}^\dagger|\phi\rangle\,W_{m,n}. \tag{30}$$

We obtain

$$\sum_{m,n=0}^{d-1}\langle\phi|W_{m,n}^\dagger|\phi\rangle\,\kappa_{mn}W_{m,n} = \mathbf{1}, \tag{31}$$

where κ_{mn} is defined as

$$\kappa_{mn} = \frac{1}{d}\sum_{i=1}^{d}\omega_d^{n_im-m_in}. \tag{32}$$

Note that Eq. (31) is the expansion form of the identity $\mathbf{1}$ in terms of $W_{m,n}$. When $(m, n) \neq (0, 0)$, the coefficients $\langle\phi|W_{m,n}^\dagger|\phi\rangle\,\kappa_{mn}$ should vanish. Evidently there are some $(m, n) \neq (0, 0)$ such that $\langle\phi|W_{m,n}^\dagger|\phi\rangle \neq 0$, which requires $\kappa_{mn} = 0$.

Here we employ the following lemma:

Lemma 2. Let $\omega_d = e^{2\pi i/d}$, with d being a prime. Assume

$$\sum_{i=1}^{d}\omega_d^{\nu_i} = 0, \tag{33}$$

for some d integers, $0 \leqslant \nu_i \leqslant d-1$. This is possible if and only if all ν_i are distinct, i.e., $\{\nu_i\}_{i=1}^d = \{0, 1, \dots, d-1\}$.

The proof of Lemma 2 will be given at the end of this section. We have shown that if the GBS set $\mathcal{W}$ is one-way distinguishable, then $\kappa_{m,n} = 0$ for some integers m, n. According to Lemma 2, this implies that $n_i m - m_i n$ $(i = 1, \dots, d)$ are distinct modulo d for some integers m, n, and therefore, by Theorem 1, we conclude that the set $\mathcal{W}$ is F equivalent.

Thus we have shown that a set of d GBSs $\mathcal{W}$ in prime dimension is one-way LOCC distinguishable if and only if $\mathcal{W}$ is F equivalent.

As shown in the following, the restriction "one way" can actually be removed. For that, we employ the lemma of Yu and Oh [20].

Lemma: Yu and Oh. Assume that a set of d GBSs $\mathcal{W} = \{W_{m_i,n_i}\}_{i=1}^d$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ satisfies the following conditions: If $\sum_{i=1}^d \omega_d^{mn_i - nm_i} = 0$, then $(m, n) \equiv (m_i - m_j, n_i - n_j) \pmod d$ for some $i \neq j$. This is possible only when $\mathcal{W}$ is not distinguishable by LOCC.

Here LOCC is not restricted to be one way. This lemma was derived by a method of detecting the local indistinguishability proposed by Horodecki *et al.* [21]. It is based on the fact that the LOCC transition of bipartite states $|\psi\rangle \to \{p_i, |\psi_i\rangle\}$ is possible if and only if the vector $\sum_i p_i \lambda(\psi_i)$ majorizes $\lambda(\psi)$ [22], where λ is the vector of squared Schmidt coefficients. This is the reason why LOCC in this lemma is not restricted to be one way.

Suppose that the set $\mathcal{W}$ is not F equivalent. As shown before, this implies that there are no integers m, n such that $\sum_{i=1}^d \omega_d^{mn_i - nm_i} = 0$. The lemma of Yu and Oh tells that the set $\mathcal{W}$ is not distinguishable by LOCC. We thus obtain the main result of this paper.

Theorem 2. A d-GBS set $\mathcal{W} = \{W_{m_i,n_i}\}_{i=1}^d$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ with d being prime is distinguishable by LOCC if and only if W is F equivalent; that is,

$$m_i\alpha + n_i\beta \ (i = 1, \dots, d), \tag{34}$$

are all distinct modulo d for some integers α and β.

The rest of this section is devoted to the proof of Lemma 2. In the complex plane, the points $\{\omega_d^\nu\}_{\nu=0}^{d-1}$ are at the vertices of a regular d-sided polygon inscribed in the unit circle. The "if" part of the lemma is evident. For small primes ($d = 2,3$), the "only if" part also appears to be evident. For larger primes, however, some knowledge of the cyclotomic polynomials is needed.

The nth cyclotomic polynomial is defined to be

$$\Phi_n(x) \equiv \prod_{\substack{1 \leqslant \nu \leqslant n \\ \gcd(\nu, n) = 1}} \left(x - e^{\frac{2\pi i}{n}\nu}\right). \tag{35}$$

Its roots are all nth primitive roots of unity. It can be shown that the coefficients of the cyclotomic polynomials are integers. For example, we find

$$\begin{aligned} &\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1,\ \Phi_3(x) = x^2 + x + 1, \\ &\Phi_4(x) = x^2 + 1,\ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \\ &\Phi_6(x) = x^2 - x + 1, \dots . \end{aligned} \tag{36}$$

For a prime n, $\Phi_n(x)$ is clearly given by

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = \sum_{\nu=0}^{n-1} x^\nu, \tag{37}$$

since all nth roots of unity are primitive except for unity itself. One of the remarkable properties of the cyclotomic polynomials is that $\Phi_n(x)$ is irreducible over $\mathbb{Q}[x]$ (all polynomials with rational coefficients) [23,24]. It has no nontrivial factors in $\mathbb{Q}[x]$ with smaller degree, and therefore it is the unique minimal polynomial of $e^{\frac{2\pi i}{n}}$ over $\mathbb{Q}[x]$. This means that if a polynomial $f(x)$ in $\mathbb{Q}[x]$ is monic (the leading coefficient is 1) and it satisfies $f(e^{\frac{2\pi i}{n}}) = 0$, then we have $\deg f(x) > \deg \Phi_n(x)$ or $f(x) = \Phi_n(x)$.

Suppose that the relation $\sum_{i=1}^d \omega_d^{\nu_i} = 0$ holds, and consider the following polynomial of x:

$$f_d(x) \equiv \frac{\sum_{i=1}^d x^{\nu_i}}{\text{the leading coefficient of } \sum_{i=1}^d x^{\nu_i}}. \tag{38}$$

We then observe

(i) $f_d(x)$ is a polynomial of x with rational coefficients, and it is monic.

(ii) $f_d(\omega_d) = 0$.

(iii) $\deg f_d(x) \leqslant d - 1$.

Since $\deg \Phi_d(x) = d - 1$ for a prime d, we conclude $f_d(x) = \Phi_d(x)$, which is possible only if all ν_i are distinct. This completes the proof of Lemma 2.

V. DISCUSSION AND CONCLUDING REMARKS

We have shown that local distinguishability is equivalent to F equivalence for a set of d GBSs in $\mathbb{C}^d \otimes \mathbb{C}^d$ with prime d. Here it should be emphasized that the GBS set that cannot be transformed to be F type is not distinguishable even with two-way LOCC. Theorems 1 and 2 provide a computable simple criterion for that: a finite number of integer calculations are sufficient to test whether a GBS set is F equivalent.

It is not straightforward to extend this conclusion to general $\ell < d$ cases. One reason for this can be seen in the rewriting of "orthogonality" in Eq. (28) to "completeness" in Eq. (29), which is possible only if the number of states is equal to the space dimension.

Let us take some cases where the dimension d is not prime. Consider d-GBS sets with $d = d_1^2$. In the case of $d = 4$, there are two types of one-way LOCC distinguishable GBS sets that are not F equivalent [12,13]. One of them is $\mathcal{W} = \{(0,0), (0,2), (2,0), (2,2)\}$. This set can easily be generalized to general $d = d_1^2$ cases. Consider the GBS set given by

$$\mathcal{W} = \{X^{\mu d_1} Z^{\nu d_1}\}_{\mu,\nu=0}^{d_1-1}. \tag{39}$$

Clearly the set $\mathcal{W}$ is not F type. It is not even F equivalent since it is invariant under the $Sp(d)$ transformations given in Eq. (22). However, the set $\mathcal{W}$ is one-way LOCC distinguishable. To see this, take

$$|\phi\rangle = \frac{1}{\sqrt{d_1}}(\overbrace{1, 1, \dots, 1}^{d_1}, \overbrace{0, 0, \dots\dots\dots, 0}^{d_1^2 - d_1}). \tag{40}$$

Then we find that d states given by

$$X^{\mu d_1} Z^{\nu d_1} |\phi\rangle = 0, \ \mu, \nu = 0, \dots, d_1 - 1, \tag{41}$$

are pairwise orthogonal, showing that $\mathcal{W}$ is one-way LOCC distinguishable. When $d = d_1^2$, we thus found that distinguishability by one-way LOCC $\supsetneq$ F equivalence.

We performed some numerical analysis to test distinguishability by one-way LOCC for all sets of six GBSs in 6×6 dimension, which is the simplest example for $d = d_1 d_2$ with relatively prime d_1 and d_2. The results indicate that distinguishability by one-way LOCC is equivalent to F equivalence in this example. Further studies are needed in order to clarify how this equivalence persists in general $d = d_1 d_2$ cases.

[1] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[2] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[3] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[5] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[6] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).
[7] M. Nathanson, Phys. Rev. A **88**, 062316 (2013).
[8] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004).
[9] M. Nathanson, J. Math. Phys. **46**, 062103 (2005).
[10] M. Owari and M. Hayashi, Phys. Rev. A **74**, 032108 (2006).
[11] H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).
[12] G. Tian, S. Yu, F. Gao, and Q. Wen, Phys. Rev. A **94**, 052315 (2016).
[13] T. Singal, R. Rahaman, S. Ghosh, and G. Kar, Phys. Rev. A **96**, 042314 (2017).
[14] Y.-L. Wang, M.-S. Li, S.-M. Fei, and Z.-J. Zheng, Quantum Inf. Proc. **16**, 126 (2017).
[15] Y.-H. Yang, C.-H. Wang, J.-T. Yuan, X. Wu, and H.-J. Zuo, Quantum Inf. Proc. **17**, 29 (2018).
[16] Y.-H. Yang, J.-T. Yuan, C.-H. Wang, S.-J. Geng, and H.-J. Zuo, Phys. Rev. A **98**, 042333 (2018).
[17] B. Wu, J. Jiang, J. Zhang, G. Tian, and X. Sun, Phys. Rev. A **98**, 022304 (2018).
[18] Y.-L. Wang, M.-S. Li, and Z.-X. Xiong, Phys. Rev. A **99**, 022307 (2019).
[19] D. Watanabe, T. Hashimoto, M. Horibe, and A. Hayashi, J. Phys.: Conf. Ser. **1194**, 012112 (2019).
[20] S. Yu and C. H. Oh, arXiv:1502.01274.
[21] M. Horodecki, A. Sen (De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
[22] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
[23] M. R. Schroeder, *Number Theory in Science and Communication*, Springer Series in Information Sciences, Vol. 7 (Springer, Berlin, 2006).
[24] S. Lang, *Algebra*, Graduate Texts in Mathematics, Vol. 211 (Springer-Verlag, New York, 2002).