Local copying and local discrimination as a study for nonlocality of a set of states

Masaki Owari[1,2] and Masahito Hayashi[1,3]
[1]*ERATO Quantum Computation and Information Project, JST, Tokyo 113-0033, Japan*
[2]*Department of Physics, The University of Tokyo, Tokyo 113-0033, Japan*
[3]*Superrobust Computation Project Information, Science and Technology Strategic Core (COE), Graduate School of Information Science and Technology, The University of Tokyo, Tokyo 113-0033, Japan*
(Received 17 August 2005; revised manuscript received 13 April 2006; published 27 September 2006)

We focus on the nonlocality concerning local copying and local discrimination, especially for a set of orthogonal maximally entangled states in any prime dimensional system, as a study of nonlocality of a set of states. As a result, for such a set, we completely characterize deterministic local copiability and show that local copying is more difficult than local discrimination.

DOI: 10.1103/PhysRevA.74.032108 PACS number(s): 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Nonlocality is one of the oldest topics in quantum physics, and also is one of the most important topics in one of the new fields of "quantum information." The history of nonlocality started with EPR's discussion of local realism in the 1930s [1], and then, it was followed by Bell's formulation of local hidden variable theory and Bell inequality in the 1960s [2]. In the early 1990s, the development of quantum information shed new light on this topic. The theory of nonlocality was reformulated as entanglement theory, which is a useful formulation to treat entangled states as resources of quantum communication, like teleportation, dense-coding, key distribution, etc. [3,4]. Mathematically speaking, the study of conventional entanglement theory is the study of convertibility between entangled states under locality restrictions for operations, [e.g., LOCC (local operation and classical communication), separable operations, and PPT (positive partial transpose) operations [5–11]].

On the other hand, there are problems of nonlocality which cannot be explained by one to one convertibility of states. One of such problems is "*local discrimination*" (a problem to discriminate an unknown states by only LOCC) [12–18]. The starting point was the discovery of a product basis which cannot be perfectly discriminated by LOCC by Bennett *et al.* [19], "*Non-locality without entanglement*." In Ref. [19], they proposed a locally indistinguishable product basis and regarded its impossibility for perfect discrimination under LOCC as nonlocality of it.

The study of Bennett *et al.* suggests the new kind of nonlocality, *Nonlocality of a set of states*. At first, in analogy to the nonlocality discussion in their paper, we can expand the concept of nonlocality as follows. If the local (LOCC) restriction causes difficulty for a task concerning a set of states, e.g., discrimination, copying, etc., then, we consider that this set has nonlocality, and regard the degree of this difficulty as *nonlocality of the set*. This concept of nonlocality is not unnatural, since it is consistent with the conventional entanglement theory because of the following reasons. In entanglement theory, entanglement cost [6] is one of the most established measures of entanglement, and can be regarded as a kind of difficulty of a task, i.e., the difficulty of entanglement dilution [6]. Moreover, if we consider the task to approximate a given state by separable states, we derive the relative entropy of entanglement [10] by measuring this difficulty in terms of accuracy of the approximation, using relative entropy. These can be regarded as the degrees of difficulty of tasks with the local restrictions.

Indeed, local discrimination can be regarded as tasks for a set of states with the local restriction, because these problems are usually treated based on a set of candidates of unknown states. Hence, we can measure *nonlocality of a set of states* by the degree of difficulty of local discrimination. We should note that this kind of difficulty cannot be often characterized only by entanglement of states of the given set. A typical example is the impossibility of local discrimination of the product basis of Bennett *et al.* mentioned before. In addition to local discrimination, similar nonlocality also appears commonly in various different fields of quantum information, e.g., quantum capacity, quantum estimation, etc. [20,21].

Recently, a similar problem to local discrimination,"*local copying*," was also raised [22,23], as a problem to study a cloning of unknown entangled states under the LOCC restriction with only minimum entanglement resource. Local copying is also defined for a set of states with the local restriction, therefore we can consider nonlocality of a set of states concerning local copying. Moreover, this nonlocality cannot be also characterized only by entanglement of states of the given set [22].

In this paper, as a study of nonlocality of a set of states, we focus on local copying and local discrimination. Specifically, we concentrate on a set of orthogonal maximally entangled states, and investigate the relationship between their local copiability and local distiniguishability. As a result, we give a local copying protocol (Fig. 2), and then, we completely characterize the local copiability of this kind of set in a prime dimensional system [24] by showing that such a protocol is the only possible local copying protocol. This protocol requires the following two properties. One is " canonical Bell form;" we say that a set of states $\{|\Psi_i\rangle\}_{i=0}^{N-1}$ has canonical Bell form, if it can be generated from $|\Psi_0\rangle$ by action of Weyl-Heisenberg group [17,25]. The other is "simultaneously Schmidt decomposability;" we say that a set of states $\{|\Psi_i\rangle\}_{i=0}^{N-1}$ is simultaneously Schmidt decomposable, if there exists a pair of orthonormal basis $\{|e_k\rangle\}_{k=0}^{D-1}$ and $\{|f_k\rangle\}_{k=0}^{D-1}$ such that all $|\Psi_i\rangle$ can be written down as $|\Psi_i\rangle=\Sigma_k \alpha_k^{(i)}|e_k\rangle$

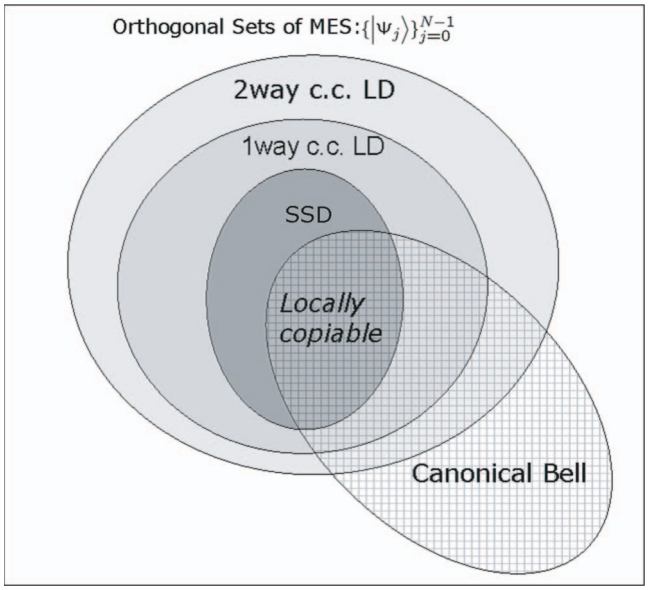

FIG. 1. (Color online) The hierarchy of nonlocality of sets of maximally entangled states. In this figure, LD, SSD, and c.c. mean locally distinguishable, simultaneously Schmidt decomposable, and classical communication, respectively.

$\otimes|f_k\rangle$with complex coefficients $\alpha_k^{(i)}$ [13,26]. Our main result is that this kind of set is locally copiable, if and only if it has a canonical Bell form and is simultaneously Schmidt decomposable (Theorem 7). Using this result, we prove the following two facts. First, the maximal size of locally copiable sets is equal to the dimension of the local space which is equal to the maximal size of local distinguishable sets. Second, we also show that if such a set is locally copiable, then it is locally distinguishable by one-way communication. In this case, local copying is strictly more difficult than one-way local discrimination, because we can find examples of a set of states which is one-way distinguishable, but not locally copiable. The relationship of local copiability and distinguishability is summarized in Fig. 1.

From this relationship, we derive the conclusion related to the nonlocality of a set concerning local copying and local discrimination: A simultaneously Schmidt decomposable set does not have nonlocality of a set of states beyond individual entanglement concerning local discrimination, since it is locally distinguishable. However, even if a set is simultaneous Schmidt decomposable, if such a set does not have a canonical Bell form, such a set still has nonlocality concerning local copying.

Although we mainly concentrate on the aspect of local copying and local discrimination as the study of nonlocality in this paper, local copying and local discrimination themselves are worth to investigate as basic protocols of quantum information processing with two parties. In the last part of this paper, we show that there are many important relationships between our local copying protocol and the other quantum information protocols. These results give many other interpretations for local copying.

This paper is organized as follows. In Sec. II, in preparation of our analysis, we review a necessary and sufficient condition for a locally copiable set, which is the main result of the paper [22]. In Sec. III, we give an example of a locally copiable set of D maximally entangled states, and then, prove that, in a prime-dimensional local system, the above example is the only case where local copying is possible for maximally entangled states. In Sec. IV, we discuss the relationship between local copying and LOCC discrimination by means of simultaneous Schmidt decomposition. In Sec. V, we present other protocols which are strongly related to our theory of local copying, i.e., channel copying, entanglement distillation protocol, error correction, and quantum key distribution. And then, we extend our results of local copying to these protocols. Finally, we summarize and discuss our results in Sec. VI.

II. THE LOCAL COPYING PROBLEM

In this section, in preparation of our analysis, we introduce formulation and known results of local copying from Ref. [22].

Many researchers treated approximated cloning, for example, universal cloning [27], asymmetric cloning [28], telecloning [29]. This is because the perfect cloning, i.e., copying, is impossible without prior knowledge (*no-cloning theorem*) [30]. That is, the possibility of copying depends on prior knowledge about the state to be copied, or, in other words, a set of candidates for the unknown target state, where we call the state to be copied the target state. If we know that the unknown state to be copied is contained by a set of orthogonal states, which is called the *copied set*, we can copy the given state. However, if our operation is restricted to local operations and classical communication (LOCC) [5], we cannot necessarily copy the given quantum state even with the above orthogonal assumption, perfectly. Thus, it is interesting from both viewpoints of entanglement theory and cloning theory to extend the cloning problem to the bipartite entangled setting. This is the original motivation of cloning problems with LOCC restriction [22,23].

Recently, Anselmi *et al.* [22] focused on the perfect cloning of bipartite systems under the following assumptions:

(1) Our operation is restricted to LOCC.

(2) It is known that the unknown state to be copied is contained in a set of known orthogonal entangled states (the copied set).

(3) A known entangled state of the same size is shared.

They called this problem local copying, and they have characterized copied sets which we can locally copy for special cases. In the following, for simplicity, we say the set is locally copiable if and only if local copying is possible with the prior knowledge to which the given state belongs.

The problem of local copying can be phrased as follows. We assume two players at a long distance, e.g., Alice and Bob in this protocol. They have two quantum systems $\mathcal{H}_A$ and $\mathcal{H}_B$ each of which is also composed by the same *two* D-dimensional systems, i.e., the systems $\mathcal{H}_A$ and $\mathcal{H}_B$ are described by $\mathcal{H}_A=\mathcal{H}_1\otimes\mathcal{H}_3$, $\mathcal{H}_B=\mathcal{H}_2\otimes\mathcal{H}_4$. In our problem, they try to copy an unknown state $|\Psi\rangle$ on the initial system $\mathcal{H}_1\otimes\mathcal{H}_2$ to the target system $\mathcal{H}_3\otimes\mathcal{H}_4$ with the prior knowl-

edge that $|\Psi\rangle$ belongs to the copy set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$. Moreover, we assume that they implement copying only by LOCC between them. Since LOCC operations do not increase the entanglement of whole states, they can copy no entangled state by LOCC without any entanglement resource. Thus, we also assume that they share a blank entangled state $|b\rangle$ in the target system $\mathcal{H}_3 \otimes \mathcal{H}_4$. Therefore, a set of states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is called locally copiable with a blank state $|b^{3,4}\rangle \in \mathcal{H}_3 \otimes \mathcal{H}_4$, if there exists a LOCC operation Λ on $\mathcal{H}_A \otimes \mathcal{H}_B$ which satisfies the following condition for all $j=0,\ldots,N-1$:

$$\Lambda(|\Psi_j^{12}\rangle \otimes |b^{34}\rangle\langle\Psi_j^{12}| \otimes \langle b^{34}|) = |\Psi_j^{12}\rangle \otimes |\Psi_j^{34}\rangle\langle\Psi_j^{12}| \otimes \langle\Psi_j^{34}|, \tag{1}$$

where we treat $\mathcal{H}_A = \mathcal{H}_1 \otimes \mathcal{H}_3$ and $\mathcal{H}_B = \mathcal{H}_2 \otimes \mathcal{H}_4$ as local spaces with respect to a LOCC operation Λ.

Even if the most simple case $N=1$, it is very hard to completely characterize which state $|b\rangle$ can be used as a blank state for a given state $|\Psi_1\rangle$ in Eq. (1). This is because the transformation in Eq. (1) is the entanglement transformation from $|b\rangle$ to $|\Psi_1\rangle$ using $|\Psi_1\rangle$ as entanglement catalysis [7], that is, even if $|b\rangle$ cannot be transformed to $|\Psi_1\rangle$, it may be possible for $|b\rangle$ to be transformed to $|\Psi_1\rangle$ with help of catalysis $|\Psi_1\rangle$. And it is very hard to characterize this catalytic transformation (for detail see Sec. II B of Ref. [22]). Thus, it is very hard to derive a necessary and sufficient condition for general settings of local copying. On the other hand, it is well known that no maximally entangled state works as entanglement catalysis [7]. In this paper, to avoid the difficulty of entanglement catalysis, we restrict our analysis to the case where all of $|\Psi_j\rangle$ are maximally entangled states, which are defined as states whose Schmidt coefficients (eigenvalues of the reduced density matrix) are all $\frac{1}{D}$ [31].

If we restrict a copy set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ to a set of maximally entangled states, we can simplify the problem setting as follows. First, because of monotonicity of entanglement under LOCC, a blank state $|b\rangle$ needs to be also maximally entangled, and we can always choose this blank state $|b\rangle = |\Psi_0\rangle$. This is because, before we implement a operation Λ in Eq. (1), we can always operate a local unitary operation for $|b\rangle$ to change $|b\rangle$ to an arbitrary maximally entangled state. Therefore, by the assumption $|b\rangle = |\Psi_0\rangle$ the problem does not lose generality. Second, if a set of states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally copiable, we can easily see that a set of states $\{U \otimes V|\Psi_j\rangle\}_{j=0}^{N-1}$ is also locally copiable for any local unitary operation $U \otimes V$. In other words, local copiability is invariant under an action of local unitary operation for a set of states. Thus, by means of this freedom of action of local unitary, we can fix one state in $\{|\Psi_j\rangle\}_{j=0}^{N-1}$. Here, we choose the standard maximally entangled state as $|\Psi_0\rangle$, that is, $|\Psi_0\rangle = \frac{1}{\sqrt{D}}\sum_{i=0}^{D-1}|i\rangle \otimes |i\rangle$, where $\{|i\rangle\}_{i=0}^{D-1}$ is a computational basis in each local space. Finally, all we need to consider is the following condition:

$$\Lambda(|\Psi_j^{12}\rangle \otimes |\Psi_0^{34}\rangle\langle\Psi_j^{12}| \otimes \langle\Psi_0^{34}|) = |\Psi_j^{12}\rangle \otimes |\Psi_j^{34}\rangle\langle\Psi_j^{12}| \otimes \langle\Psi_j^{34}|, \tag{2}$$

where $|\Psi_0\rangle$ is the standard maximally entangled state. In the following discussion, we always assume the above conditions.

Anselmi *et al.* [22] derived a necessary and sufficient condition for a specific locally copiable set (Lemma 1). Also, they completely characterize local copiability of maximally entangled states in the case of $N=2$. In following, in preparation for our analysis, we shortly summarize the Anselmi *et al.* results for local copying of maximally entangled states.

First, Anselmi *et al.* showed the following theorem.

Theorem 1 (Anselmi et al.). If a set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally copiable, then, it is copiable by only local unitary transformation.

That is, when all $|\Psi_j\rangle$ are maximally entangled states, we always choose a local unitary operation as the copying operation Λ in Eq. (1). In Ref. [22], by means of the above result, Anselmi *et al.* derived a necessary and sufficient condition of copiability for maximally entangled states. Here, we do not mention this necessary and sufficient condition in their original formula, but we present the modified version of their statement for benefit of later detail analysis in Sec. III.

Lemma 1 (Anselmi et al.). A set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally copiable, if and only if there exists a unitary operator A on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and unitary operations $\{U_j\}_{j=0}^{N-1}$ on $\mathcal{H}_1$ such that

$$A(U_j \otimes I)A^\dagger = U_j \otimes U_j, \tag{3}$$

and

$$|\Psi_j\rangle\langle\Psi_j| = U_j \otimes I|\Psi_0\rangle\langle\Psi_0|U_j^\dagger \otimes I. \tag{4}$$

Proof. (We look at the necessary condition.)

Suppose $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally copiable. Then, by Lemma 1, there exist a local unitary operation $A \otimes B$ and real numbers $0 \le \theta_j < 2\pi$ such that, for all j,

$$A^{12} \otimes B^{34}|\Psi_j^{13}\rangle \otimes |\Psi_0^{24}\rangle = e^{i\theta_j}|\Psi_j^{13} \otimes |\Psi_j^{24}\rangle, \tag{5}$$

where $e^{i\theta_j}$ are phase factors. Then, we define A' and θ_j' as $A' \overset{\text{def}}{=} e^{-i\theta_0}A$ and $\theta_j' \overset{\text{def}}{=} \theta_j - \theta_0$, respectively. From Eq. (5), we derive

$$A'^{12} \otimes B^{34}|\Psi_j^{13}\rangle \otimes |\Psi_0^{24}\rangle = e^{i\theta_j'}|\Psi_j^{13} \otimes |\Psi_j^{24}\rangle, \tag{6}$$

where $\theta_0'=0$. Since all $|\Psi_j\rangle$ are maximally entangled states, there exists a set of unitary operations $\{U_j\}_{j=0}^{N-1}$ such that

$$|\Psi_j\rangle = e^{-i\theta_j'}U_j \otimes I|\Psi_0, \tag{7}$$

where we can choose $U_0=I$. Then, we can easily see $|\Psi_j\rangle\langle\Psi_j| = U_j \otimes I|\Psi_0\rangle\langle\Psi_0|U_j^\dagger \otimes I$ and

$$(A'^{12} \otimes B^{34})(U_j^1 \otimes I^{234})|\Psi_0^{13}\rangle|\Psi_0^{24}\rangle = U_j^1 \otimes U_j^2 \otimes I^{34}|\Psi_0^{13}\rangle \otimes |\Psi_0^{24}\rangle. \tag{8}$$

By using the symmetry of the standard maximally entangled state, we derive

$$\{A'^{12}(U_j^1 \otimes I^2)B^{T12}\} \otimes I^{34}|\Psi_0^{13}\rangle|\Psi_0^{24}\rangle = U_j^1 \otimes U_j^2 \otimes I^{34}|\Psi_0^{13}\rangle \otimes |\Psi_0^{24}\rangle, \quad (9)$$

where B^T is transpose of B in the computational basis. Then, by projecting Eq. (9) to a state in computational basis $|k^1\rangle \otimes |l^2\rangle \otimes |m^3\rangle \otimes |n^4\rangle$, we have

$$\langle k^1| \otimes \langle l^2|A'^{12}(U_j^1 \otimes I^2)B^{T12}|m^1\rangle \otimes |n^2\rangle = \langle k^1| \otimes \langle l^2|U_j^1 \otimes U_j^2|m^1\rangle \otimes |n^2\rangle. \quad (10)$$

Since the above equation is valid for all states in the computational basis, we derive $A'(U_j \otimes I)B^T = U_j \otimes U_j$. By substituting $U_0 = I$ in the above formula, we can easily see $B = A'^*$, where A'^* means the complex conjugate of A' in the computational basis. Therefore, finally, we derive Eq. (3).

(We look at the sufficient condition.)

Suppose Eqs. (3) and (4) are valid. Then, by defining $B = A^*$, we can directly check Eq. (5).

Here, we remark the following two facts. First, from Eq. (3), we can easily see $\mathrm{Tr}\, U_j^\dagger U_{j'} = \delta_{jj'}$. Thus, for a locally copiable set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$, $|\Psi_j\rangle$ must be orthogonal to each other. Second, by the proof of the above lemma, the local copying operation Λ is explicitly represented as a local unitary transformation $A^{13} \otimes A^{*24}$.

In Ref. [22], Anselmi *et al.* also solved Eq. (3) in the case of $N=2$, that is, they completely characterized local copiability under the assumption that the copied set consists of two states. In this case, since $U_0 = I$, there is only one independent equation $A(U_1 \otimes I)A^\dagger = U_1 \otimes U_1$. The following theorem is the conclusion of their analysis of Eq. (3) for $N=2$.

Theorem 2 (Anselmi et al.). There exists a unitary operator A satisfying

$$A(U \otimes I)A^\dagger = U \otimes U, \quad (11)$$

if and only if a unitary operator U satisfies the following two conditions:

(1) The spectrum of U is the set of power of Mth roots of unity, where M is a factor of D.

(2) The distinct eigenvalues of U have equal degeneracy.

Thus, if D is prime and $U \neq I$, then, the set of eigenvalues of U is completely determined to $\{\omega^a\}_{a=0}^{D-1}$, where $\omega \stackrel{\mathrm{def}}{=} \exp(2\pi i/D)$. We use this notation of ω throughout the following discussion.

Here, we should remark about the number of maximally entangled states as the resource. If we allow the use of three entangled states as a resource, Alice and Bob could always locally copy any orthogonal set of maximally entangled states by performing quantum teleportation [3]. (For the case when Alice and Bob share two entangled states as resources, see Ref. [23].)

III. LOCAL COPYING OF THE MAXIMALLY ENTANGLED STATES IN PRIME-DIMENSIONAL SYSTEMS

Our main purpose is developing the relation between local copiability and local distinguishability, and understanding nonlocality of a set of maximally entangled states concerning local copiability and local distinguishability. For this purpose, the necessary and sufficient condition given in Lemma 1 is rather abstract, and we need a simpler criterion by which we can easily determine whether a given set is locally copiable, or not. Therefore, in this section, we construct such a simple criterion for local copiability, and completely characterize local copiability of a set of maximally entangled states. That is, we solve Eq. (3) and get the simpler necessary and sufficient condition of local copiability for all N in the case of *prime-D*-dimensional local systems (Theorem 4). As a consequence, we show that D is the maximum size of a locally copiable set.

In the first step, we construct an example of a locally copiable set of D maximally entangled states.

Theorem 3. When the set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is defined by

$$|\Psi_j\rangle = (U_j \otimes I)|\Psi_0 \quad (12)$$

and

$$U_j = \sum_{k=0}^{D-1} \omega^{jk}|k\rangle\langle k|, \quad (13)$$

where $\{|k\rangle\}_{k=0}^{D-1}$ is an orthonormal basis of the $\mathcal{H}_1$, then the set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ can be locally copied.

Proof. We define the unitary operator A by

$$A^{12} = A_{c-}^{12} \stackrel{\mathrm{def}}{=} \sum_{a,b} |a \ominus b\rangle^1|b\rangle^2\langle a|^1\langle b|^2, \quad (14)$$

where A_{c-} is an extension of controlled-NOT (CNOT) gate represented in $\{|k\rangle\}_{k=0}^{D-1}$ for D-dimensional systems ("Controlled Minus gate"), and $\ominus$ is subtraction modulo D. Note that in our notation of generalized controlled-NOT gate, the first register is the target state, and the second register is the control state. Then, we can easily verify Eq. (3) as

$$A^{12}(U_j^1 \otimes I^2)A^{12\dagger} = A_{c-}^{12}(U_j^1 \otimes I^2)A_{c-}^{12\dagger} = \sum_{a_1,a_2,b_1,b_2} |a \ominus b\rangle^1|b\rangle^2\langle a_1|^1\langle b_1|^2(\omega^{ja_3}|a_3\rangle^1\langle a_3|^1 \otimes I^2)|a_2\rangle^1|b_2\rangle^2\langle a_2 \ominus b_2|^1\langle b_2|^2$$

$$= \sum_{a_1,b_1} \omega^{ja_1}|a_1 \ominus b_1\rangle^1\langle a_1 \ominus b_1|^1 \otimes |b_1\rangle^2\langle b_1|^2 = \sum_{c,b_1} \omega^{j(b_1 \oplus c)}|c\rangle^1\langle c|^1 \otimes |b_1\rangle^2\langle b_1|^2 = U_j^1 \otimes U_j^2,$$

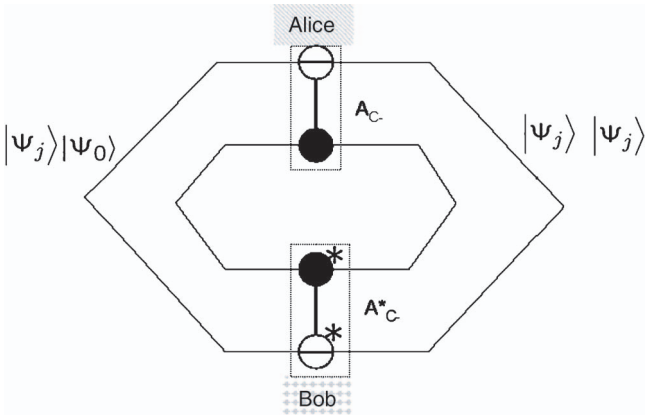

FIG. 2. (Color online) The protocol of local copying (cf. Theorem 3).

where we set $c=a_1\ominus b_1$. Therefore, Lemma 1 guarantees that the set $\{|\Psi_j\rangle\}_{j=0}^{D-1}$ can be locally copied. ■

As we already mentioned in the preceding section, the copying operation can be chosen to be the local unitary operation $A^{12}\otimes A^{34*}=A_{c-}^{12}\otimes A_{c-}^{34*}$. Therefore, this protocol of local copying used in the above proof is written as Fig. 2.

Here, we should remark that U_1 is the generalized Pauli's Z operator which is one of the generators of the Weyl-Heisenberg group, and another U_j is the jth power of $U_1=Z$. Hence, in the case of non-prime-dimensional local systems, the spectrum of U_j is different from that of U_1 if j is a nontrivial factor of D.

Moreover, the property of the Weyl-Heisenberg group not only guarantees that the above example satisfies (3), but also is essential for the condition (3). That is, as is proved below, any locally copiable set of maximally entangled states is restricted exclusively to the above example. Therefore, our main theorem can be written down as follows.

Theorem 4. For systems whose local spaces are prime dimensional, the set of maximally entangled states $\{U_j\otimes I|\Psi_0\rangle\langle\Psi_0|U_j^\dagger\otimes I\}_{j=0}^{N-1}$ can be locally copied if and only if there exist an orthonormal basis $\{|a\rangle\}_{a=0}^{D-1}$ and a set of integers $\{n_j\}_{j=0}^{N-1}$ such that the unitary U_j can be written as

$$U_j=\sum_{a=0}^{D-1}\omega^{n_j a}|a\rangle\langle a|, \tag{15}$$

where ω is the Dth root of unity.

From Eq. (15), we can easily see that the number of different candidates of U_j is at most D. Thus, D, that is equal to the dimension of local space, is the maximum size of a locally copiable set of maximally entangled states with prime-dimensional local systems. In comparison with the case without LOCC restriction, where we can copy D^2 orthogonal states, this is actually the square root.

The proof of Theorem 4 is as follows.

Proof. (If part) We have already proven that $\{U_j\otimes I|\Psi_j\rangle\}_{j=0}^{D-1}$ can be copied by LOCC in Theorem 3. Therefore, any subset of them can be trivially copied by LOCC.

(Only if part) Assume that a unitary operator A satisfies the condition (3) for all j.

By applying Theorem 2 to U_1, we can choose an orthonormal basis $\{|a\rangle\}_{a=0}^{D-1}$ such that

$$U_1=\sum_{a=0}^{D-1}\omega^a|a\langle a|, \tag{16}$$

where ω is Dth root of unity. Then, we focus on Eq. (3) in the case of $j=1$. In this equation, $|a\rangle\langle a|\otimes\mathcal{H}$ is the eigenspace of the corresponding eigenvalue ω^a of $U_1\otimes I$ in the left-hand side, and $\mathrm{span}\{|a\ominus c\rangle\langle a\ominus c|\otimes|c\rangle\langle c|\}_{c=0}^{D-1}$ is the eigenspace of the corresponding eigenvalue ω^a of $U_1\otimes U_1$ on the right-hand side. Since $U_1\otimes I$ is transformed to $U_1\otimes U_1$ by the action of the unitary A in Eq. (3), the unitary A should transform the subspace $|a\rangle\langle a|\otimes\mathcal{H}$to subspace $\mathrm{span}\{|a\ominus c\rangle\times\langle a\ominus c|\otimes|c\rangle\langle c|\}_{c=0}^{D-1}$, and the remaining freedom of A is unitary transformations between these subspaces. That is, A is expressed as

$$A=\sum_{a,b,c}\xi_{b,c}^a|a\ominus c\rangle|c\rangle\langle a|\langle b|, \tag{17}$$

where $\xi_{b,c}^a$ is a unitary matrix for b, c for the same a, that is, $\Sigma_{c=0}^{D-1}\xi_{b,c}^a\bar{\xi}_{b',c}^a=\delta_{b,b'}$ and $\Sigma_{b=0}^{D-1}\xi_{b,c}^a\bar{\xi}_{b,c'}^a=\delta_{c,c'}$. For every a, $\xi_{b,c}^a$ determines a unitary transformation from $|a\rangle\langle a|\otimes\mathcal{H}$ to $\mathrm{span}\{|a\ominus c\rangle\langle a\ominus c|\otimes|c\rangle\langle c|\}_{c=0}^{D-1}$. Thus, based on the basis $\{|a\rangle\}_{a=0}^{D-1}$, the matrix elements of Eq. (3) for all $|a_1\rangle\langle a_2|\otimes|b_1\rangle\langle b_2|$ is written down as

$$\langle a_1|\langle b_1|A(U_j\otimes 1)A^\dagger|a_2\rangle|b_2\rangle=\langle a_1|U_j|a_2\rangle\langle b_1|U_j|b_2\rangle. \tag{18}$$

Therefore, substituting Eq. (17) to Eq. (18) for any integer j, we obtain

$$\sum_{b=0}^{D-1}\xi_{b,b_1}^{a_1\oplus b_1}\bar{\xi}_{b,b_2}^{a_2\oplus b_2}\langle a_1\oplus b_1|U_j|a_2\oplus b_2\rangle=\langle a_1|U_j|a_2\rangle\langle b_1|U_j|b_2\rangle, \tag{19}$$

for all a_1, a_2, b_1, and b_2.

To see that U_1 and U_j can be simultaneously diagonalized, we need to prove the following lemma.

Lemma 2. A nonzero $D\times D$ matrix U_{ab} satisfies the following equation:

$$\Xi_{b_1b_2}^{a_1\oplus b_1,a_2\oplus b_2}U_{a_1\oplus b_1a_2\oplus b_2}=U_{a_1a_2}U_{b_1b_2}, \tag{20}$$

where $\Xi_{b_1b_2}^{cc}=\delta_{b_1b_2}$ and all indices have their value between 0 and $D-1$, then U_{ab} is a diagonal matrix.

Proof. See the Appendix.

We apply Lemma 2 to the case when $U_{ab}=\langle a|U_j|b\rangle$ and $\Xi_{b_1\ b_2}^{a_1\ a_2}=\Sigma_{b=0}^{D-1}\xi_{bb_1}^{a_1}\bar{\xi}_{bb_2}^{a_2}$. Then, this lemma shows that, $\langle a|U_j|b\rangle$ is a diagonal matrix for all j, therefore unitaries $\{U_j\}_{j=0}^{N-1}$ are simultaneously diagonalizable in the eigenbasis $\{|a\rangle\}_{a=0}^{D-1}$ of U_1. Then, we can get the formula of $\{U_j\}_{j=0}^{N-1}$ explicitly as follows. From the diagonal element of (19), we derive

$$\langle a \oplus b|U_j|a \oplus b\rangle = \langle a|U_j|a\rangle\langle b|U_j|b\rangle. \tag{21}$$

From Theorem 2 and Lemma 1, all U_j have the same eigenvalues $\{\omega^n\}_{n=0}^{D-1}$, and from the above discussion, all U_j also have the same eigenbasis $\{|a\rangle\}_{a=0}^{D-1}$. Therefore, we can express U_j as

$$U_j = \sum_{a=0}^{D-1} \omega^{P_j(a)}|a\rangle\langle a|, \tag{22}$$

where $P_j(a)$ is a bijection from $\{a\}_{a=0}^{D-1}$ to themselves. Then, Eq. (21) guarantees that $P_j(a)$ is a self-isomorphism of the cyclic group $\{a\}_{a=0}^{D-1}$. Since a self-isomorphism of a cyclic group is identified by the image of the generator [32], we derive the formula (15) with $P_j(1)=n_j$. ■

This theorem completely characterizes local copiability of maximally entangled states in the case of prime-dimensional local spaces.

So far, we have solved the LOCC copying problem only for a *prime*-dimensional local space. Now, we discuss about the case of a non-prime-dimensional local space. Since Theorem 3 is valid in this case, the "*if*" part of Theorem 4 is also valid in non-prime-dimensional local systems. However, the "*only if*" part is extended straightforwardly, if the set $\{U_j\}_{j=0}^{N-1}$ contains at least one unitary whose eigenvalues are generated by ω, in other words, in the set of $\{U_j\}_{j=0}^{N-1}$, there exists U_k whose eigenspace is not degenerate. We can only show the following statement for the "only if" part.

Theorem 5. If a set of maximally entangled states $\{U_j \otimes I|\Psi_0\rangle\langle\Psi_0|U_j^\dagger \otimes I\}$ is locally copiable, and if there exists k such that ω is eigenvalue of U_k, then, there exist an orthonormal basis $\{|a\rangle\}_{a=0}^{D-1}$ and a set of integers $\{n_j\}_{j=0}^{N-1}$ such that, for all j, U_j can be written down in the form of Eq. (15).

Proof. The proof does not lose generality by the assumption that U_1 has eigenvalue ω. Then, by Theorem 2, Eq. (16) holds. By the same procedure of the prime-dimensional case, Eqs. (17) and (18) hold. Thus, we obtain Eq. (19) in the same way as the prime-dimensional case. Then, Lemma 2 implies that $\{U_j\}_{j=0}^{N-1}$ can be simultaneously diagonalized, and also implies Eq. (21) for all U_j. By writing U_j as (22), we get the equation $P_j(a \oplus b)=P_j(a) \oplus P_j(b)$ and, so, $P_j(a)=aP_j(1)$. Hence, Theorem 2 guarantees the same representation of U_j as (15).

Therefore, we can solve the problem of local copying in non-prime-dimensional local spaces as the direct extension of Theorem 4, only in the case where eigenspace of one of U_j is not degenerate. On the other hand, if eigenvalues of all U_j are degenerate, our proof of the "*if*" part does not hold.

IV. RELATIONSHIP BETWEEN LOCC COPYING AND LOCC DISCRIMINATION

If we have no LOCC restriction, the possibility of the deterministic copying is equivalent to that of the perfect distinguishability. However, we can easily see that under the restriction of LOCC, this relation is not trivial at all. As we have already mentioned in the introduction, these two problems share the common feature, that is, their difficulty can be regarded as a nonlocality of a set of states, and this nonlocality cannot be explained only by entanglement convertibility. Therefore, the study of this relationship is really important to understand the nonlocality of a set of states. In this section, we compare the locally distinguishability and the locally copiability for a set of orthogonal maximally entangled states. Thus, by introducing simultaneous Schmidt decomposition, we show the relationship between these two problems of nonlocality.

At first, we review the definition of a locally distinguishable set, and then mention several known and new results of local distinguishability. A set of states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is called two-way (one-way) classical communication locally distinguishable, if there exists a POVM $\{M_j\}_{j=0}^{N-1}$ which can be performed by two-way (one-way) LOCC and also satisfies the following conditions:

$$\langle\Psi_i|M_j|\Psi_i\rangle = \delta_{ij}, \quad \forall\, i,j. \tag{23}$$

In order to compare local copying and local discrimination, we should take care of the following point: We assume an extra maximally entangled state only in the local copying case. This is because local copying of a set of maximally entangled states is trivially impossible without a blank entangled state. This fact is contrary to local discrimination, that is, we do not allow the parties to share maximal entanglement in the local discrimination problem, since if we allow, they can always discriminate by teleportation.

Before we compare local copying and local discrimination, we review the known relation between local copying and local discrimination. In the paper of Anselmi *et al.* [22], they showed that in the case where the copy set consist of two maximally entangled states $\{|\Psi_0\rangle,|\Psi_1\rangle\}$, local copying is strictly more difficult than local discrimination. That is, from Ref. [12], we know that a couple of bipartite states are always one-way local distinguishable. Also, from Theorem 2, not all bipartite maximally entangled states are locally copiable. One example is $\{|\Psi_0\rangle, I \otimes U|\Psi_0\rangle\}$, where

$$U \overset{\text{def}}{=} e^{i(\pi/3)}|0\rangle\langle 0| + e^{i(2\pi/3)}|1\rangle\langle 1| + e^{i(4\pi/3)}|2\rangle\langle 2| + e^{i(5\pi/3)}|3\rangle\langle 3| \tag{24}$$

in 4×4 dimensional systems. The above set is not locally copiable since the condition 1 of Theorem 2 is not satisfied. In the following part of this section, by using the result of the preceding section, we show that local copying is strictly more difficult than local discrimination for the set of maximally entangled states $\{|\Psi_i\rangle\}_{i=0}^{N-1}$ with $N>3$.

In the preceding section, we have already proved that D is the maximum size of a locally copiable set of maximally entangled states. In the case of local discrimination, we can also prove that D is the maximum size of a locally distinguishable set of maximally entangled states. This statement was proved by Ref. [18] only when the set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ consists of canonical form Bell states, where a canonical form Bell state $|\Psi_{nm}\rangle$ is defined as

$$|\Psi_{nm}\rangle \overset{\text{def}}{=} Z^n X^m \otimes I|\Psi_{00}\rangle,$$

$$|\Psi_{00}\rangle \overset{\text{def}}{=} \sum_{k=0}^{d-1} |k\rangle \otimes |k\rangle,$$

$$X \overset{\text{def}}{=} \sum_{k=1}^{d} |k\rangle\langle k \oplus 1|.$$

Such a set is a special case of a set of maximally entangled states. Here, we give a simple proof of this statement for a general set of maximally entangled states by the same technique as Ref. [33].

Theorem 6. If an orthogonal set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally distinguishable, then $N \leq D$.

Proof. Suppose $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ is locally distinguishable by LOCC POVM $\{M_j\}_{j=0}^{N-1}$. Then, since LOCC operation is always separable, $\{M_j\}_{j=0}^{N-1}$ can be decomposed as $M_i = \Sigma_{k=0}^{L} p_{ik} |\psi_k\rangle\langle\psi_k| \otimes |\phi_k\rangle\langle\phi_k|$, where p_{ik} is a positive coefficient satisfying $\Sigma_k p_{ik} = \mathrm{Tr}\, M_i$, and $\{|\psi_k\rangle\}_{k=0}^{L}$ and $\{|\phi_k\rangle\}_{k=0}^{L}$ are normalized, but not generally orthogonal sets of states. Then, we can derive an upper bound of $\langle\Psi_j|M_i|\Psi_j\rangle$as follows:

$$\begin{aligned}\langle\Psi_j|M_i|\Psi_j\rangle &= \sum_{k=0}^{L} p_{ik}\langle\Psi_j||\psi_k\rangle\langle\psi_k| \otimes |\phi_k\rangle\langle\phi||\Psi_j\rangle \\ &\leq \sum_{k=0}^{L} p_{ik}\langle\psi_k|\left(\frac{1}{D}I\right)|\psi_k\rangle \\ &= \frac{\mathrm{Tr}\, M_i}{D},\end{aligned}$$

where the inequality comes from the monotonicity of the fidelity under partial trace operations concerning the system B. Since $\langle\Psi_j|M_j|\Psi_j\rangle = 1$, we have $1 \leq \mathrm{Tr}(M_j)/D$. Finally, taking the summation of the inequality for j, we obtain $N \leq D^2/D = D$, since $\Sigma_{j=0}^{N-1}\mathrm{Tr}(M_j) = D^2$.

Therefore, in this case, the maximal size of both locally copiable and locally distinguishable sets is equal to the dimension of the local space.

When we consider the relationship between local discrimination and local copying of a set of maximally entangled states, it is quite useful to introduce "*simultaneous Schmidt decomposition*" [13,26]. A set of states $\{|\Psi_\alpha\rangle\}_{\alpha\in\Gamma} \subset \mathcal{H}_1 \otimes \mathcal{H}_2$ is called simultaneously Schmidt decomposable, if they can be written down as

$$|\Psi_\alpha\rangle = \sum_{k=0}^{d-1} b_k^{(\alpha)} |e_k\rangle|f_k\rangle, \tag{25}$$

where Γ is a parameter set, $\{|e_k\rangle\}_{k=0}^{d-1}$ and $\{|f_k\rangle\}_{k=0}^{d-1}$ are orthonormal bases of local spaces (simultaneous Schmidt basis) and $b_k^{(\alpha)}$ is a *complex number* coefficient. Actually, it is already known that for a set of orthogonal maximally entangled states, simultaneous Schmidt decomposability is a sufficient condition for one-way local distinguishability [13], and, as we will show in this section, a necessary condition for local copiability of it. Moreover, simultaneous Schmidt decomposability is not a necessary and sufficient condition for both cases. Therefore, a family of locally copiable sets of maximally entangled states is strictly included by a family of one-way locally distinguishable sets of maximally entangled states. In the following, we prove this relationship.

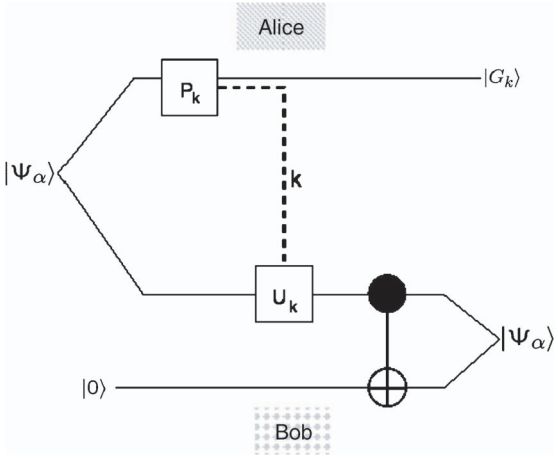

FIG. 3. (Color online) A set of simultaneous Schmidt decomposable states can be sent to Bob's space by LOCC.

First, we explain the relationship between local discrimination and simultaneous Schmidt decomposition which has been already obtained by Ref. [13]. If an unknown state $|\Psi_\alpha\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is in a simultaneously Schmidt decomposable set of states $\{|\Psi_\alpha\rangle\}_{\alpha\in\Gamma}$, such a state can be transformed to a single local space $\mathcal{H}_A$ or $\mathcal{H}_B$ by LOCC. Rigorously speaking, there exists an LOCC Λ on $\mathcal{H}_A \otimes \mathcal{H}_{B_1B_2}$ which transforms $|\Psi_\alpha^{AB_1}\rangle \otimes |0^{B_2}\rangle$ to $\sigma^A \otimes |\Psi_\alpha^{B_1B_2}\rangle$ for all $\alpha \in \Gamma$, and there also exists an LOCC Λ'on $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_B$ which transforms $|0^{A_1}\rangle \otimes |\Psi_\alpha^{A_2B}\rangle$ to $|\Psi_\alpha^{A_1A_2}\rangle \otimes \sigma^B$ for all $\alpha \in \Gamma$. This LOCC transformation Λ can be written down as the following Kraus representation [13]:

$$\Lambda, \quad \rho \mapsto \sum_{k=0}^{d-1} F_k \rho F_k^\dagger,$$

where

$$F_k \overset{\text{def}}{=} (I_A \otimes \mathrm{CNOT}_{B_1B_2})(U_k \otimes I_{A,B_2})(P_k \otimes I_{B_1,B_2}),$$

$$P_k \overset{\text{def}}{=} 1/D\left(\sum_i \omega^{ki}|e_i\rangle\right)\left(\sum_l \omega^{kl}\langle e_l|\right)$$

$$U_k \overset{\text{def}}{=} \sum_i \omega^{ki}|f_i\rangle\langle f_i|$$

$$\mathrm{CNOT}_{B_1B_2} \overset{\text{def}}{=} \sum_{kl} |e_k^{B_1}\rangle \otimes |f_{k\oplus l}^{B_2}\rangle\langle f_k^{B_1}| \otimes \langle l^{B_2}|.$$

In the above formula, both $\{|e_k\rangle\}_{k=0}^{D-1}$ and $\{|f_l\rangle\}_{k=0}^{D-1}$ are simultaneous Schmidt bases of $\{|\Psi_\alpha\rangle\}_{\alpha\in\Gamma}$, and $\{|l\rangle\}_{l=0}^{D-1}$ is the standard computational basis. This protocol can be depicted in Fig. 3, where $|G_k\rangle$ is a garbage state with no information. Using the above protocol, if a set $\{|\Psi_\alpha\rangle\}$ is simultaneously

Schmidt decomposable, there exists a one-way-LOCC POVM $M'=\{M'_i\}$ for a given arbitrary POVM $M=\{M_i\}$ such that

$$\langle\Psi_\alpha|M_i|\Psi_\alpha\rangle=\langle\Psi_\alpha|M'_i|\Psi_\alpha\rangle, \quad \forall\, i, \forall\, \alpha.$$

That is, any POVM can be essentially realized by one-way LOCC. Therefore, "*a simultaneously Schmidt decomposable set of orthogonal maximally entangled states is one-way locally distinguishable.*"

On the other hand, there exists a set of orthogonal maximally entangled states which is not simultaneously Schmidt decomposable, but locally distinguishable. For example, a set of maximally entangled states $\{|\Psi_0\rangle, X\otimes I|\Psi_0\rangle, Z\otimes I|\Psi_0\rangle\}$ is not simultaneously Schmidt decomposable in any prime-dimensional systems, since $[X,Z]\neq 0$. However, this set is one-way locally distinguishable in $D\geq 3$ dimensional systems, since all N-canonical Bell states are one-way locally distinguishable, if $N(N-1)/2\leq D$ [17]. Note that we can easily extend this example for the set with $N>3$. That is, if a set of canonical Bell states $\{|\Psi_i\rangle\}_{i=0}^{N-1}$ include the above three states, and if $N(N-1)/2\leq D$ is valid, then, such a set is locally distinguishable, but not locally copiable. Note that, the set of $\{|\Psi_0\rangle, I\otimes U|\Psi_0\rangle\}$ with unitary (24) is another type of example of a locally disitinguishable, but not locally copiable set. In this case, they are simultaneously Schmidt decomposable (actually all couples of bipartite maximally entangled states is simultaneously Schmidt decomposable), however not canonical Bell states.

Thus, a family of simultaneously Schmidt decomposable sets of maximally entangled states is strictly included by a family of locally distinguishable sets of maximally entangled states.

On the other hand, the relationship between simultaneous Schmidt decomposability and local copiability can be described by the following theorem.

Theorem 7. In prime-dimensional local systems, an orthogonal set of maximally entangled states $\{|\Psi_j\rangle\langle\Psi_j|\}_{j=0}^{N-1}$ is locally copiable, if and only if it is a simultaneously Schmidt decomposable subset of canonical form Bell states under the same local unitary operation.

Proof. We can easily see the "*only if*" part of the above statement from Theorem 4 as follows. In Theorem 4, since Eq. (15) means that each U_j is equivalent to Z^{n_j} under the same unitary operation, a set of maximally entangled states $\{U_j\otimes I|\Psi_0\rangle\}_{j=0}^{N-1}$ is local unitary equivalent to $\{Z^{n_j}\otimes I|\Psi_0\rangle\}_{j=0}^{N-1}$, which is a simultaneous Schmidt decomposable subset of canonical form Bell states. The "*if*" part can be shown as follows. Reference [26] shows that a canonical Bell set $|\Psi_{n_\alpha m_\alpha}\rangle$ $(\alpha=1,2,\ldots,l)$ are simultaneously Schmidt decomposable, if and only if there exist integers p, q, and r $(p\neq 0$ or $q\neq 0)$ satisfying $pn_\alpha\oplus qm_\alpha=r$ for all α, where $\oplus$ is the summation modulo D. Since the ring $\mathbb{Z}_D$ is a field in the prime number D case, the above condition is reduced to the existence of f and g such that $m_\alpha=fn_\alpha\oplus g$. Then, we get

$$|\Psi_{n_\alpha m_\alpha}\rangle=|\Psi_{n_\alpha(fn_\alpha+g)}\rangle=C_\alpha(ZX^f)^{n_\alpha}X^g\otimes I|\Psi_{00}\rangle, \quad (26)$$

where $C_\alpha \overset{\text{def}}{=} \omega^{-f\{(n_\alpha-1)!\}}$ is a phase factor. Since ZX^f is unitary equivalent to Z [17], the state $|\Psi_{n_\alpha m_\alpha}\rangle\langle\Psi_{n_\alpha m_\alpha}|$ is locally unitary equivalent with $U_j\otimes I|\Psi_0\rangle\langle\Psi_0|U_j^\dagger\otimes I$ in Theorem 4. ■

We add a remark here. Under the assumption of simultaneous Schmidt decomposition, a set has canonical Bell form, if and only if the set of corresponding unitary operators is a cyclic group, that is, the group with only one generator. Therefore, we can rephrase this necessary and sufficient condition as follows, the set is simultaneously Schmidt decomposable and satisfies the following condition by a renumbering:

$$U_1^D=I, \quad U_k=\overbrace{U_1\cdots U_1}^{k}. \quad (27)$$

Finally, we derive Fig. 1, and, therefore, for maximally entangled states, a family of locally copiable sets is strictly included by a family of simultaneously Schmidt decomposable sets. In other words, local copying is more difficult than local discrimination.

In this last part of this section, we discuss our main results in Fig. 1, in the viewpoint of nonlocality of a set of states.

In the case of bipartite pure states, all information of a bipartite state $|\Psi\rangle=\Sigma_{i=0}^{D-1}\lambda_i|e_i\rangle\otimes|f_i\rangle$ can be separated to two parts, that is, Schmidt coefficients λ_i and Schmidt basis $\{|e_i\rangle,|f_i\rangle\}_{i=0}^{D-1}$, where $\lambda_i\geq 0$. Because of local unitary equivalence, Schmidt coefficients completely determine entanglement convertibility [5]. Therefore, conversely, we can regard the nonlocality coming from interrelationship among Schmidt basis as nonlocality of a set of states which is purely beyond entanglement of individual states. In the following discussion, we try to separate nonlocality which depends on Schmidt coefficients and Schmidt basis.

At first, all sets in Fig. 1 are sets of maximally entangled states, that is, they have the same Schmidt coefficients and the same amount of entanglement. Thus, the structure of nonlocality in Fig. 1 is determined only by the interrelationship of Schmidt bases, and the effect of Schmidt coefficients do not appear directly in this figure. On the other hand, when we calculate the maximal sizes of local distinguishable and copiable sets, we need to optimize all possible choices of Schmidt bases. That is, the maximal sizes depend only on Schmidt coefficients. Therefore, Schmidt coefficients may affect only the maximal size of local distinguishable and copiable sets.

The interrelationship of Schmidt bases is determined by the unitary operator $U=\Sigma_{i=0}^{D-1}|e_i\rangle\langle f_i|$. In Fig. 1, the two properties of the interrelationship of Schmidt basis, that is, such unitary operators, are related to nonlocality of a set. That is, simultaneous Schmidt decomposability and canonical Bell form seems to reduce nonlocality of a set. For simultaneous Schmidt decomposable sets, we can explain their lack of nonlocality as follows. As we well know, in the case of pure bipartite states, one person can always apply the local operation which causes the same transformation for a given state as another person's local operation causes (Lo-Popescu's

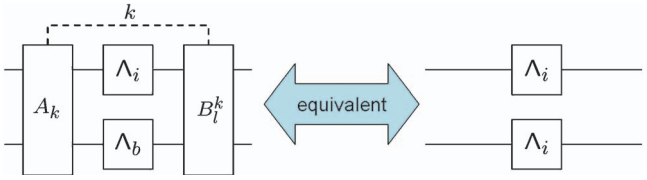

FIG. 4. (Color online) Definition of channel copying with one-way classical communication. By suitable encoding $\{A_k\}$ and decoding $\{B_l^k\}$ operations, each Λ_i works as $\Lambda_i \otimes \Lambda_i$.

theorem [34]). The simple structure of entanglement convertibility originates in the above symmetry between local systems. This symmetry is caused by the existence of Schmidt decomposition. Similarly, in the case of local discrimination, the protocol Fig. 4 seems to utilize this kind of symmetry between local systems. Therefore, the existence of simultaneous Schmidt decomposable basis can give the symmetry between the local systems, and this fact may decrease the nonlocality of the sets of states.

In the case of canonical Bell form, the interesting fact is that the algebraic property of Weyl-Heisenberg group is related to local copiability, and not to local distinguishability. As we have already seen, since a simultaneous Schmidt decomposable set can be transformed to a single local space by LOCC, we can use any global discrimination protocols to such a set by only LOCC. Therefore, concerning local discrimination, the sets of simultaneous Schmidt decomposable states seem not to possess any nonlocality which originates in interrelationship between their Schmidt basis. However, if such a set does not have a canonical Bell form, it is not locally copiable. That is, a set has extra nonlocality beyond individual entanglement concerning local copying, if it has no algebraic structure given in (27), even if it is simultaneous Schmidt decomposable. Finally, we can conclude that, in the view point of problems of nonlocality beyond individual entanglement, the above algebraic nonlocality is a most remarkable difference between local copying and local discrimination.

V. APPLICATION TO CHANNEL COPYING, ENTANGLEMENT DISTILLATION, AND ERROR CORRECTION

So far, we have treated local copying mainly in the context of nonlocality of a set. On the other hand, we now consider how local copying itself is a benefit to the information processing. In this last section, we apply our results, especially Theorem 7 on different contexts, and give several other interpretations for our results, like channel copying, entanglement distillation, error correction, and QKD. Thus, these many connections imply the fruitfulness of local copying problems as a fundamental two-party protocol. Moreover, seeing local copying from these various points of view, we may also derive some clue which helps us to construct further development of understanding of nonlocality beyond entanglement convertibility.

A. Channel copying

In Sec. III, in the analysis of local copying, we treated not directly maximally entangled states, but unitary operators which represent the maximally entangled states based on some standard maximally entangled states. This method is a kind of operator algebraic method, or equivalent to Heisenberg picture. Therefore, we can interpret our results as directly the results for these unitary operators themselves. Then, as a result, we can look at the problem of "*unitary channel copying*."

Here, we consider a problem "*channel copying*," that is, a problem in which we ask a question as follows: in the case that we do not have complete description of a channel, "Can we simulate two copies of an unknown channel by using the unknown channel only once and also using a known *blank channel* once." For example, such a question may occur in the following case. There exists an unknown and rare quantum operation, of which we would like to have the outputs (results of the operation) be as many as possible. However, we can not restrict inputs of the channel, therefore the inputs might be arbitrary states. Under the above condition, we would like to decrease the frequency of use of the operation. Such a situation may occur in query complexity problem [35]. In this case, an unknown channel is a query which is represented by a unitary operation.

As we will see in the following discussion, channel copying with the help of one-way classical communication between sender and receiver is equivalent to local copying of corresponding entangled states with the help of one-way classical communication between Alice and Bob. The problem setting of channel copying can be written as follows.

Definition 1. We call that a set of channel $\{\Lambda_i\}_{i=1}^N; \mathfrak{B}(\mathcal{H}_{A1}) \to \mathfrak{B}(\mathcal{H}_{B1})$ is copiable with one-way classical communication and a blank channel Λ_b, if for all i, there exists sets of Kraus's operators $\{A_k\}_{k=1}^K \subset \mathfrak{B}(\mathcal{H}_{A1} \otimes \mathcal{H}_{A2})$, $\{B_l^k\}_{l=1}^L \subset \mathfrak{B}(\mathcal{H}_{B1} \otimes \mathcal{H}_{B2})$ such that $\Sigma_{k=1}^K A_k^\dagger A_k = I_A$, $\Sigma_{l=1}^L B_l^{k\dagger} B_l^k = I_B$ for all l, and for all i and ρ on $\mathcal{H}_{A1} \otimes \mathcal{H}_{A2}$,

$$\sum_{kl} B_l^k [\Lambda_i \otimes \Lambda_b (A_k \rho A_k^\dagger)] B_l^{k\dagger} = \Lambda_i \otimes \Lambda_i(\rho). \tag{28}$$

The meaning of the above definition can be sketched as Fig. 4, that is, by an encoding operation $\{A_k\}_{k=1}^K$ and a decoding operation $\{B_l^k\}_{l=1}^L$, one copy of unknown channel Λ_i with one copy of blank channel (may be noisy) Λ_b works as two copies of unknown channels $\Lambda_i \otimes \Lambda_i$. For simplicity, we always assume $\dim \mathcal{H}_{A1} = \dim \mathcal{H}_{A2} = \dim \mathcal{H}_{B1} = \dim \mathcal{H}_{B2}$ in the following discussion.

Then, we can easily show that the channel copying problem with one-way classical communication is exactly the same as the local copying of corresponding entangled states with one-way classical communication.

Theorem 8. A set of channel $\{\Lambda_i\}_{i=0}^{N-1}$ is copiable with one-way classical communication and a blank channel Λ_b, if and only if a set of entangled states $\{\Lambda_i \otimes I(|\Psi\rangle\langle\Psi|)\}_{i=N}$ is locally copiable with one-way classical communication and blank states $\Lambda_b \otimes I(|\Psi\rangle\langle\Psi|)$, where $|\Psi\rangle$ is an arbitrarily fixed maximally entangled state.

Proof. Suppose $\{\Lambda_i\}_{i=0}^{N-1}$ is copiable with one-way classical communication and a blank channel Λ_b. Consider four systems $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3\otimes\mathcal{H}_4$, and prepare two copies of maximally entangled states $|\Psi\rangle\langle\Psi|$ on $\mathcal{H}_1\otimes\mathcal{H}_3$ and $\mathcal{H}_2\otimes\mathcal{H}_4$, respectively. Then, by applying channel copying protocol for $\mathcal{H}_1\otimes\mathcal{H}_2$, we derive the following calculations:

$$\begin{aligned}
&\sum_{kl} B_l^{k12}\otimes I^{34}[\Lambda_i^1\otimes\Lambda_b^2\otimes I^{34}(A_k^{12}\otimes I^{34}|\Psi^{13}\rangle\langle\Psi^{13}| \\
&\quad\otimes|\Psi^{24}\rangle\langle\Psi^{24}|A_k^{\dagger 12}\otimes I^{34})]B_l^{k\dagger 12}\otimes I^{34} \\
&=\sum_{kl} B_l^{k12}\otimes I^{34}[\Lambda_i^1\otimes\Lambda_b^2\otimes I^{34}(I^{12}\otimes A_k^{t34}|\Psi^{13}\rangle\langle\Psi^{13}| \\
&\quad\otimes|\Psi^{24}\rangle\langle\Psi^{24}|I^{12}\otimes A_k^{*34})]B_l^{k\dagger 12}\otimes I^{34} \\
&=\sum_{kl} B_l^{k12}\otimes A_k^{t34}[(\Lambda_i^1\otimes I^3(|\Psi^{13}\rangle\langle\Psi^{13}|) \\
&\quad\otimes(\Lambda_b^2\otimes I^4|\Psi^{24}\rangle\langle\Psi^{24}|)]B_l^{k\dagger 12}\otimes A_k^{*34} \\
&=\Lambda_i^1\otimes I^3(|\Psi^{13}\rangle\langle\Psi^{13}|)\otimes\Lambda_i^2\otimes I^4(|\Psi^{24}\rangle\langle\Psi^{24}|),
\end{aligned}$$

where the last equality comes from Eq. (4). Therefore, $\Lambda_i\otimes I(|\Psi\rangle\langle\Psi|)$ is locally copiable with one-way classical communication. We can also easily check the opposite direction of the proof. ■

The correspondence between channels Λ and entangled states $\Lambda\otimes I(|\Psi\rangle\langle\Psi|)$ is called Choi-Jamiolkowski's isomorphism [36]. The above theorem shows that the channel copying problems can be always identified to corresponding local copying problems of entangled states in the case of one-way classical communication. On the other hand, since not all states can be written down as $\Lambda\otimes I(|\Psi\rangle\langle\Psi|)$ for some maximally entangled state $|\Psi\rangle$, not all local discrimination problems can be considered as a channel copying problem.

Choosing all Λ_i as unitary channels, we derive maximally entangled states for corresponding entangled states. Therefore, our results in Secs. III and IV give also results for unitary channel copying as follows.

Corollary 1. In a prime-dimensional system, a set of unitary channels $\{\Lambda_i\}_{i=0}^{N-1}$ where $\Lambda_i(\rho)=U_i\rho U_i^\dagger$ is copiable with blank noiseless channel $\Lambda_b=I$ and one-way classical communication, if and only if $\{U_i\}_{i=0}^{N-1}$ is a simultaneous diagonalizable subset of Weyl-Heisenberg (generalized Pauli) group.

Proof. We can easily see from Theorems 7 and 8.

As we will see later, the above analysis of channel copying can also be used in the context of error correction of the quantum channel.

B. Entanglement distillation

As the next example of applications of our results, we consider entanglement distillation. Although we have only considered the local copying of pure states so far, we apply our protocol for mixed states in backward directions in this section.

Since our local copying protocol consists of local unitary operations, we can also consider the opposite direction of our protocol. This inverse of local copying protocol is actually entanglement distillation protocol by local unitary. Since we usually use measurements in entanglement distillation protocols [6,8,37], this is a really rare example of entanglement distillation by unitary transformation. As we can see in Fig. 2, the inverse of our protocol transforms $|\Psi_i\rangle\otimes|\Psi_i\rangle$ to $|\Psi_i\rangle\otimes|\Psi_0\rangle$ by a local unitary operation. Therefore, if we consider mixed states like

$$\rho=\sum_{ij} a_{ij}|\Psi_i\rangle\otimes|\Psi_i\rangle\langle\Psi_j|\otimes\langle\Psi_j|, \tag{29}$$

and apply our local copying protocol, where $\{|\Psi_i\rangle\}_{i=0}^{D-1}$ is a set of simultaneous Schmidt decomposable subset of canonical Bell states, then we derive

$$A^\dagger\otimes A^t\rho A\otimes A^*=\left(\sum_{ij} a_{ij}|\Psi_i\rangle\langle\Psi_j|\right)\otimes|\Psi_0\rangle\langle\Psi_0|, \tag{30}$$

where A is a local unitary operator defined at (17). This protocol is actually entanglement distillation protocol deriving one e-bits for all mixed states which satisfy the above condition. Moreover, in the case $a_{ij}=\delta_{ij}/D$, since $\Sigma_{i=0}^{D-1}\frac{1}{D}|\Psi_i\rangle\langle\Psi_i|$ is a separable state, this distillation protocol by the local unitary is optimal. Actually, the states (29) belong to a class of states called "maximally correlated states," and the simple formula of distillable entanglement for maximally correlated states has been already known [8]. However the above protocol is deterministic and moreover unitary, this is actually an important point. Generally speaking, deterministic distillable entanglement is strictly less than the usual asymptotic one [9]. Therefore, this is a very rare case where we can derive the meaningful lower bound of deterministic entanglement distillation for mixed states.

C. Error correction and QKD

As another application, we apply our result to error correction and quantum key distribution with the following specific noisy channel in this section. Now, we consider the inverse of channel copying protocols in Sec. V A, and we derive the error correcting protocol which corresponds to the above distillation protocol. Consider a channel $\Lambda(\rho)=\Sigma_{k=1}^N E_k\rho E_k^\dagger$ on $\mathcal{H}_1\otimes\mathcal{H}_2$, where E_k satisfies $\Sigma_{k=1}^N E_k^\dagger E_k=I$ and can be written down as $E_k=\Sigma_{i=0}^{D-1}c_{ki}U_i\otimes U_i$ by a simultaneous diagonalized subset $\{U_i\}_{i=0}^{D-1}$ of generalized Pauli's group. (In particular, when a channel can be decomposed by a set of Kraus operators which have a form $E_k=p_kU_k\otimes U_k$, the channel is called collective noise. Such a noise may occur, for example, in the case when we send two photonic qubits simultaneously through optical fiber or free space [38].) Since whole dimension of operator space $\mathfrak{B}(\mathcal{H}_1\otimes\mathcal{H}_2)$ is D^4, these error operators have very limited forms. However, in this case, the inverse of our copying protocol gives one noiseless channel as follows. If the channel Λ satisfies the above condition, then the channel Λ can be written down as $\Lambda(\rho)=\Sigma_{ij}a_{ij}U_i\otimes U_i\rho U_j^\dagger\otimes U_j^\dagger$. Then, by the inverse of channel copying operation, we have the following relation:

$$A^\dagger[\Lambda(A\rho A^\dagger)]A = \sum_{ij} a_{ij} A^\dagger(U_i \otimes U_i) A\rho A^\dagger (U_j^\dagger \otimes U_j^\dagger) A$$
$$= \sum_{ij} a_{ij} (U_i \otimes I)\rho(U_j \otimes I).$$

Thus, using an ancilla σ_0, encoding operation A and decoding operation $A^\dagger$, we derive a noiseless channel in $\mathcal{H}_2$ as follows:

$$\mathrm{Tr}_1 A^\dagger[\Lambda(A(\sigma_o \otimes \sigma)A^\dagger)]A = \sigma.$$

Similarly to the distillation case, as is shown later, when $a_{ij}=\delta_{ij}/D$, this error correcting protocol attains the asymptotic optimal rate of transmitting the quantum state through the channel Λ. That is, the transmission rate of this protocol is equal to the quantum capacity of this rate.

This fact can be seen by the correspondence between quantum capacity and distillable entanglement given in Ref. [6]. Thus, for generalized Pauli's channel, quantum capacity coincides with distillable entanglement of the corresponding state, which is the state derived as the output state when inputting a part of a maximally entangled state, i.e., $\Sigma_{i=0}^{D-1} \frac{1}{D} |\Psi_i\rangle \otimes |\Psi_i\rangle\langle\Psi_i| \otimes \langle\Psi_i|$. Since our protocol is the optimal distillation protocol for this state, this channel coding protocol is also optimal.

Next, we apply this error correcting protocol to QKD. In the D-dimensional case, we apply the above encoding and decoding operations for D-dimensional version of Bennett-Brassard 1984 (BB84) protocol [39]. Here, we fix noise operators as $U_i \overset{\mathrm{def}}{=} X^i = FZF^\dagger$, and encoding operation as $A \overset{\mathrm{def}}{=} F \otimes F(\mathrm{CNOT})F^\dagger \otimes F^\dagger$, where $F \overset{\mathrm{def}}{=} \Sigma_i |\tilde{i}\rangle\langle i|$ is Fourier transformation, and $|\tilde{i}\rangle \overset{\mathrm{def}}{=} \frac{1}{\sqrt{D}} \Sigma_{j=0}^{D-1} \omega^{ij} |j\rangle$ is a Fourier transformed basis. Then, we can easily see these U_i and A satisfy Eq. (3). For simplicity, we choose ancilla $\sigma_0 = |\tilde{0}\rangle\langle\tilde{0}|$.Then, applying the error correcting code to BB84 protocol, we derive the following protocol.

Protocol (1) State preparation: Alice randomly chooses a basis from $\{|0\rangle \otimes |i\rangle\}_{i=0}^{D-1}$ and $\{|0\rangle \otimes |\tilde{i}\rangle\}_{i=0}^{D-1}$, and generates one state from the chosen basis randomly. (2) State transmission: Alice sends those two qudits to Bob. (3) Decoding: Bob randomly chooses measurement basis from $\{\Sigma_{j=0}^{D-1} |a\rangle\langle a| \otimes |a \oplus i\rangle\langle a \oplus i|\}_{i=0}^{D-1}$ and $\{I \otimes |\tilde{i}\rangle\langle\tilde{i}|\}_{i=0}^{D-1}$, and measures the states. (4) Basis announcement: Alice and Bob discard any digits where they prepared and measured in a different basis.

We can easily see that the step (1) can be decomposed into the following steps (1A) and (1B), and the step (3) can be decomposed into the following steps (3A) and (3B). (1A) Preparation of BB84 states: Alice randomly chooses a basis from $\{|i\rangle\}_{i=0}^{D-1}$ and $\{|\tilde{i}\rangle\}_{i=0}^{D-1}$, and creates a qubits from the chosen basis. (1B) Encoding: Alice encodes the qubits by our error correcting code, that is, applies encoding operation $A = F \otimes F(\mathrm{CNOT})F^\dagger \otimes F^\dagger$ with ancilla qubit $|\tilde{0}\rangle$. (3A) Error correction: Bob applies the decoding operation $F \otimes F(\mathrm{CNOT}^\dagger)F^\dagger \otimes F^\dagger$, and throws away the ancilla qudit. (3B) Detection: Bob randomly chooses a basis from $\{|i\rangle\}_{i=0}^{D-1}$ and $\{|\tilde{i}\rangle\}_{i=0}^{D-1}$, and measures the decoded qudits. Therefore, if the noise of the quantum channel satisfies our assumption (that is, noise operator E_k can be written as $E_k = \Sigma_{i=0}^{D-1} c_{ki} X^i \otimes X^i$), by means of the error correction code, we can realize the noiseless QKD by the above protocol.

VI. DISCUSSION

In this paper, we focus on a set consisting of several maximally entangled states in a prime-dimensional system. In this case, we completely characterized locally copiability and showed the relationship between locally copiability and local distinguishability. In Secs. III and IV, we proved that such a set is locally copiable, if and only if it has a canonical Bell form and a simultaneous Schmidt decomposable (Theorem 7). This theorem deduces the following two conclusions. At first, as well as the maximal size of local distinguishable sets, the maximal size of locally copiable sets is D, that is, equal to the dimension of the local space. This maximal size is the square root of the maximal size without the LOCC restriction. Second, as we can see in Fig. 1, when such a set is locally copiable, it is also one-way locally distinguishable, and the opposite direction is not true. In other words, at least in prime-dimensional systems, local copying is more difficult than one-way local discrimination for a set of maximally entangled states.

In the case of local discrimination, a simultaneous Schmidt decomposable set is locally distinguishable. However, if such a set of states does not have canonical Bell form, the set is not locally copiable. We can interpret the above fact as follows. A simultaneous Schmidt decomposable set does not possess nonlocality beyond individual entanglement concerning local discrimination. On the other hand, if such a set does not have canonical Bell form, such a set still has nonlocality concerning local copying.

Although we only treated orthogonal sets of maximally entangled states in this paper, our result of Fig. 1 also regard as the classification of sets of Schmidt basis by their nonlocality. Therefore, in the case of a set of general entangled states, the structure of nonlocality of sets of Schmidt basis may be similar to Fig. 1, though it possesses additional nonlocality which originates in various Schmidt coefficients. Therefore, our result may be useful as the base for more general discussion of nonlocality problems of Schmidt basis, especially for general discussion of the local copying problems.

In Sec. IV, we showed that our results and protocol of local copying can be interpret as results of several different and closely related quantum information processing, that is, channel copying, entanglement distillation, error correction, and quantum key distribution. These close relations with many other protocols suggests the importance of local copying as a fundamental protocol of nonlocal quantum information processing.

Finally, we should mention a remaining open problem. In this paper, we showed the necessity of the form of states (15) for LOCC copying only in prime-dimensional local systems. However, we restrict this dimensionality only by the technical reason, and this restriction has no physical meaning.

Thus, the validity of Theorem 7 for non-prime-dimensional systems still remains an open question.

After finishing the first draft [40], the authors found a related paper [41] which contains a different approach to Theorem 6, and also found a paper which extends our result to a set of nonmaximally entangled states based on our main theorem (Theorem 4) [42].

ACKNOWLEDGMENTS

The authors would like to express gratitude to F. Anselmi, Dr. A. Chefles, and Professor M.B. Plenio for their useful discussions. The authors would like to thank Dr. S. Virmani for a useful discussion. The authors are particularly indebted to Professor M. Murao for her helpful advice, discussion, and checking the introduction. The authors are grateful to Professor K. Matsumoto for his advice, Dr. D. Markham for discussion and checking the paper, and Professor H. Imai for his support and encouragement. The authors are also grateful to Professor M.B. Ruskai for informing them of Ref. [41]. M.O. was partially supported by the Japan Society of the Promotion of Science for Young Scientists and by Asahi Glass Foundation. M.H. was supported by JST ERATO program.

APPENDIX: PROOF OF LEMMA 2

In this appendix, we prove Lemma 2 by induction.

Proof. First, in Eq. (20) by choosing $c=a_1\oplus b_1=a_2\oplus b_2$, we have

$$\delta_{b_1 b_2} U_{cc} = U_{c\ominus b_1\ c\ominus b_2} U_{b_1 b_2}. \tag{A1}$$

In addition, choosing $b_1 \neq b_2$, we derive

$$U_{c\ominus b_1\ c\ominus b_2} U_{b_1 b_2} = 0 \tag{A2}$$

for all c. The above equation means,

$$b_1 \neq b_2 \Rightarrow U_{b_1 b_2} = 0 \quad \text{or } U_{c\ominus b_1\ c\ominus b_2} = 0, \quad \forall\, c, \tag{A3}$$

By means of the above fact, we prove

$$U_{b\ b\oplus n} = U_{b\ b\ominus n} = 0 \tag{A4}$$

for all b and for all $0\le n\le D-1$ by induction concerning the integer n. At first, we prove $U_{b\ b\ominus 1}=0$ and $U_{b\ b\oplus 1}=0$ for all b by a contradiction, and then, under the assumption of $U_{b\ b\ominus k}=U_{b\ b\oplus k}=0$ for all b and for all $k\le n-1$, we prove $U_{b\ b\ominus n}=U_{b\ b\oplus n}=0$ for all b.

Proof of $U_{b\ b\ominus 1}=0$ *for all b.* We prove $U_{b\ b\ominus 1}=0$ for all b by contradiction. We assume that there exists b_1 such that $U_{b_1\ b_1\ominus 1}\neq 0$, then, Eq. (A3) implies $U_{b\ b\oplus 1}=0$ for all b. In order to show the contradiction, we prove $U_{b\ b\oplus k}=0$ for all b and k by induction concerning k.

We assume $U_{b\ b\oplus k}=0$ for all b, and show $U_{b\ b\oplus k\oplus 1}=0$ for all b. By substituting $a_1=b\ominus b_1$, $a_2=b\ominus b_1\oplus k\oplus 1$, and $b_2=b_1\ominus 1$, Eq. (20) guarantees that

$$\Xi^{b\ b\oplus k}_{b_1\ b_1\ominus 1} U_{b\ b\oplus k} = U_{b\ominus b_1\ b\ominus b_1\oplus k\oplus 1} U_{b_1\ b_1\ominus 1}. \tag{A5}$$

Then, by substituting $U_{b\ b\oplus k}=0$, Eq. (A5) guarantees that

$$U_{b\ominus b_1\ b\ominus b_1\oplus k\oplus 1} U_{b_1\ b_1\ominus 1} = 0 \tag{A6}$$

for all b. Since we assumed $U_{b_1\ b_1\ominus 1}\neq 0$, Eq. (A6) guarantees that $U_{b\ominus b_1\ b\ominus b_1\oplus k\oplus 1}=0$ for all b, that is, $U_{b\ b\oplus k\oplus 1}=0$ for all b.

Therefore, by induction concerning k, we derive $U_{b\ b\oplus k}=0$ for all b and k by induction. This is a contradiction for the assumption that $U_{b_1\ b_1\ominus 1}\neq 0$. So, we derive $U_{b\ b\ominus 1}=0$ for all b.

Proof of $U_{b\ b\oplus 1}=0$ *for all b.* Similarly, we can prove $U_{b\ b\oplus 1}=0$ for all b by a contradiction as follows. Suppose there exists b_1 such that $U_{b_1\ b_1\oplus 1}\neq 0$, then, Eq. (A3) implies $U_{b\ b\ominus 1}=0$ for all b. In order to show the contradiction, we prove $U_{b\ b\ominus k}=0$ for all b and k by induction concerning k. Eq. (20) implies

$$\Xi^{b\ b\ominus k}_{b_1\ b_1\ominus 1} U_{b\ b\ominus k} = U_{b\ominus b_1\ b\ominus b_1\ominus k\ominus 1} U_{b_1\ b_1\oplus 1}. \tag{A7}$$

Thus, if $U_{b\ b\ominus k}=0$ for all b, we derive $U_{b\ b\ominus k\ominus 1}=0$ for all b. Therefore, by induction, we have $U_{b\ b\ominus k}=0$ for all k and b. This is a contradiction for the assumption $U_{b_1\ b_1\oplus 1}\neq 0$. Therefore, $U_{b\ b\oplus 1}=0$ for all b.

Proof of $U_{b\ b\ominus n}=U_{b\ b\oplus n}=0$ *for all b and* $0\le n\le D-1$. As the final step, in order to proof $U_{b\ b\ominus n}=U_{b\ b\oplus n}=0$ for all b and $1\le n\le D-1$, we use induction for n again. We assume $U_{b\ b\ominus k}=U_{b\ b\oplus k}=0$ for all $k\le n-1$ and show $U_{b\ b\ominus n}=U_{b\ b\oplus n}=0$ for any b by a contradiction. Assume that there exists b_1 such that $U_{b_1\ b_1\ominus n}\neq 0$, then Equation (A3) implies that $U_{b\ b\oplus n}=0$ for all b. To show the contradiction, under the above assumption, we prove $U_{b\ b\oplus k}=0$ for all b, all $0\le k\le ln-1$, and all l, (that is, for all k), by induction concerning $1\le l$. We assume $U_{b\ b\oplus k}=0$ for all b and all $(l-1)n\le k\le ln-1$, and show $U_{b\ b\oplus k}=0$ for all b and all $ln\le k\le (l+1)n-1$. By substituting $a_1=b\ominus b_1$, $a_2=b\ominus b_1\oplus n\oplus k$, and $b_2=b_1\ominus n$, Eq. (20) implies

$$\Xi^{b\ b\oplus k}_{b_1\ b_1\ominus n} U_{b\ b\oplus k} = U_{b\ominus b_1\ b\ominus b_1\oplus n\oplus k} U_{b_1\ b_1\ominus n}. \tag{A8}$$

By substituting $U_{b\ b\oplus k}=0$ for all b and $(l-1)n\le k\le ln-1$, we have $U_{b\ b\oplus k}=0$ for all $ln\le k\le (l+1)n-1$ and b. Therefore, by induction concerning l, we derive $U_{b\ b\oplus k}=0$ for all b and all $1\le k$. This contradicts $U_{b_1\ b_1\ominus n}\neq 0$. Therefore, $U_{b\ b\ominus n}=0$ for all b.

By means of the same discussion for $U_{b\ b\oplus n}$, we can prove $U_{b\ b\oplus n}=0$ for all b, (what we only have to do is changing $\ominus$ to $\oplus$ in the above proof). Finally, by the mathematical induction concerning n, we prove $U_{b\ b\oplus n}=U_{b\ b\ominus n}=0$ for all b and all $0\le n\le D-1$. Therefore, U_{ab} is a diagonal matrix. ■

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); A. K. Ekert, *ibid.* **67**, 661 (1991); Hai-Kwong Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996); M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999); G. Vidal, *ibid.* **83**, 1046 (1999).
[6] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[7] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
[8] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).
[9] F. Morikoshi and M. Koashi, Phys. Rev. A **64**, 022316 (2001).
[10] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[11] V. Vedral and E. Kashefi, Phys. Rev. Lett. **89**, 037903 (2002); M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi, and A. Winter, J. Phys. A **36**, 527 (2003); S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004); M. Owari, K. Matsumoto, and M. Murao, Phys. Rev. A **70**, 050301(R) (2004).
[12] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[13] S. Virmani, M. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001).
[14] Y.-X. Chen and D. Yang, Phys. Rev. A **66**, 014303 (2002).
[15] A. Chefles, Phys. Rev. A **69**, 050307(R) (2004).
[16] S. Virmani and M. B. Plenio, Phys. Rev. A **67**, 062308 (2003).
[17] H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).
[18] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004).
[19] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[20] A. S. Kholevo, Probl. Inf. Transm. **15**, 247 (1979); A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997); A. Fujiwara and H. Nagaoka, IEEE Trans. Inf. Theory **44**, 1071 (1998).
[21] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995); M. Hayashi, *Quantum Computation, Measurement, and Computing 2* (Kluwer/Plenum, New York, 2000), p. 99.
[22] F. Anselmi, A. Chefles, and M. B. Plenio, New J. Phys. **6**, 164 (2004).
[23] S. Ghosh, G. Kar, and A. Roy, Phys. Rev. A **69**, 052312 (2004).
[24] Here, we clarify which theorems and lemmas are depend on prime dimensionality of local systems. Theorems 4, 7 and Corollary 1 are valid only in prime dimensional local systems. On the other hand, Theorems 1, 2, 3, 5, 6, 8, Lemmas 1 and 2 are valid in all finite dimensional systems.
[25] H. Weyl, *Gruppentheorie und Quantenmechanik* (Verlag von S. Hirzel, Leipzig, 1928). English translation, The Theory of Groups and Quantum Mechanics (Dover, New York, 1950).
[26] T. Hiroshima and M. Hayashi, Phys. Rev. A **70**, 030302(R) (2004).
[27] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996); N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997); R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[28] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[29] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, Phys. Rev. A **59**, 156 (1999).
[30] W. K. Wootters and W. H. Zurek, Nature (London) **229**, 802 (1982); R. Jozsa, e-print quant-ph/0204153.
[31] The paper [22] showed that if a copied set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ has at least one maximally entangled state and is locally copiable, then all of states $|\Psi_j\rangle$ in the copied set must be maximally entangled.
[32] S. Lang, *Algebra* (Addison-Wesley, New York).
[33] M. Hayashi, K. Matsumoto, and Y. Tsuda, e-print quant-ph/0504203.
[34] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
[35] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A, 439, 553 (1992); L. K. Grover, *Proceedings of the 28th ACM Symposium on Theory of Computing*, 1996, p. 212; M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998); W. van Dam, *Proceedings of the 39th IEEE Symposium on the Foundation of Computer Science*, 1998, p. 362; E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, Phys. Rev. Lett. **81**, 5442 (1998).
[36] M. D. Choi, Lin. Alg. Appl. **10**, 285 (1975); A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[37] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[38] X. B. Wang, e-print quant-ph/0406100.
[39] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, India, 1984), pp. 175–179.
[40] M. Owari and M. Hayashi, e-print quant-ph/0411143.
[41] M. Nathanson, J. Math. Phys. **46**, 062103 (2005).
[42] A. Kay and M. Ericsson, Phys. Rev. A **73**, 012343 (2006).