Distinguishability and Indistinguishability by Local Operations and Classical Communication

Heng Fan

Quantum Computation and Information Project, ERATO, Japan Science and Technology Agency, Daini Hongo White Building 201, Hongo 5-28-3, Bunkyo-ku, Tokyo 113-0033, Japan

(Received 9 November 2003; published 30 April 2004)

It is well known that orthogonal quantum states can be distinguished perfectly. However, if we assume that these orthogonal quantum states are shared by spatially separated parties, the distinguishability of these shared quantum states may be completely different. We show that a set of linearly independent quantum states $\{(U_{m,n} \otimes I)\rho^{AB}(U_{m,n}^{\dagger} \otimes I)\}_{m,n=0}^{d-1}$, where $U_{m,n}$ are generalized Pauli matrices, cannot be discriminated deterministically or probabilistically by local operations and classical communication. On the other hand, any l maximally entangled states from this set are locally distinguishable if $l(l-1) \leq 2d$. The explicit projecting measurements are obtained to locally discriminate these states. As an example, we show that four Werner states are locally indistinguishable.

DOI: 10.1103/PhysRevLett.92.177905 PACS numbers: 03.67.–a, 03.65.Ta, 89.70.+c

Entanglement lies at the heart of many aspects of quantum information theory. It is a fundamental and interesting question to consider the distinguishability of entangled states shared by distant parties if only local operations and classical communication (LOCC) is allowed which is a standard condition to study the properties of entanglement [1]. Not only entangled states, but also the local discrimination of any quantum states shared by distant parties, have also been attracting considerable attention recently. It is clear that orthogonal quantum states can be distinguished, while nonorthogonal states can be distinguished only probabilistically if there are no restrictions for measurements. If the quantum states are shared by two distant parties, say Alice and Bob, and only LOCC is allowed, the possibility of distinguishing these quantum states may decrease since considerable restrictions are imposed for the measurements. Interestingly, Walgate *et al.* showed that any two orthogonal pure states shared by Alice and Bob can be distinguished by LOCC [2,3]. On the other hand, there is a set of orthogonal bipartite pure product states that cannot be distinguished with certainty by LOCC [1,4]. Recently, Horodecki *et al.* showed a phenomenon of "more nonlocality with less entanglement" [5]. It differentiates nonlocality from entanglement. A number of other interesting and often counterintuitive results have been obtained. It is thus necessary to explore further the local distinguishability problem.

In this Letter, we show two main results in the following. First, we show that a set of maximally entangled states in the standard form can be discriminated by local projective measurements and classical communication. Second, using the property of entanglement breaking channel, we show that a certain specific set of linearly independent quantum states cannot be distinguished deterministically or probabilistically by LOCC. Both are general results for the d-dimensional system. We assume that d is always prime in this Letter [6].

Let us first introduce some notations. We consider that the dimension of the Hilbert space is d. $U_{m,n} = X^m Z^n$, $m, n = 0, \ldots, d-1$ are generalized Pauli matrices constituting a basis of unitary operators, and $X|j\rangle = |j + 1 \bmod d\rangle$, $Z|j\rangle = \omega^j |j\rangle$, $\omega = e^{2\pi i/d}$, where $\{|j\rangle\}_{j=0}^{d}$ is an orthonormal basis. $|\Phi^+\rangle = (1/\sqrt{d})\sum_j |jj\rangle$. $|\Phi_{m,n}\rangle = (U_{m,n} \otimes I)|\Phi^+\rangle$ is a basis of maximally entangled states.

Set of maximally entangled states that are locally distinguishable.—Walgate *et al.* once showed that two Bell states can be distinguished by LOCC (their result is for the case of arbitrary two orthogonal states) [2]. On the other hand, three Bell states are locally distinguishable probabilistically, and four Bell states are locally indistinguishable no matter whether the protocol is deterministic or probabilistic [5,8,9]. We pose one straightforward question: What is the maximal set of quantum states that are locally distinguishable? In particular, we are interested in the following problem: Suppose $\{(U_{m,n} \otimes I)|\Psi\rangle^{AB}\}_{m,n=0}^{d-1}$ is a complete set of maximally entangled states in the $d \otimes d$ system. Are any d maximally entangled states from this set locally distinguishable? This set is the best known complete set of maximally entangled states. It is obvious that if we let $|\Psi\rangle^{AB} = |\Phi^+\rangle^{AB} = \sum_j |jj\rangle$, here we omit a normalized factor; then for arbitrary n_i, d maximally entangled states $\{(X^i Z^{n_i} \otimes I)|\Psi\rangle^{AB}\}_{i=0}^{d-1}$ are locally distinguishable by simply projecting measurements in the computational basis on both sides and subsequently by a classical communication. For the general case, we do not yet have a complete answer to this question. However, we can obtain a rather general result.

Theorem: *Any l maximally entangled states from the set $\{(U_{m,n} \otimes I)|\Psi\rangle^{AB}\}_{m,n=0}^{d-1}$ can be distinguished by LOCC if $l(l-1)/2 \leq d$.* For example, if $d = 2$, then any two ($l = 2$) Bell states are locally distinguishable. If $d = 3$ or $d = 5$, then any three maximally entangled states from this set are locally distinguishable. An arbitrary maximally entangled state can always be transformed to

$|\Phi^+\rangle^{AB} = \sum_j |jj\rangle$ by a local unitary operation on one side (A or B; the difference between the unitary operators on A and B is a transposition). So, we need only to prove our claim in the case $|\Psi\rangle^{AB} = |\Phi^+\rangle^{AB}$. Let us suppose these l maximally entangled states take the form $\{(X^{m_i}Z^{n_i} \otimes I)|\Phi^+\rangle^{AB}\}_{i=0}^{l-1}$. To locally distinguish these states, we first let A and B do unitary operations U and V^t, respectively, where t is a transposition. This operation is equivalent to the transformation $U(X^{m_i}Z^{n_i})V$ on the A side. We next show that we can find these unitary operators that can transform these l maximally entangled states to the set $\{(X^{m_i'}Z^{n_i'} \otimes I)|\Phi^+\rangle^{AB}\}_{i=0}^{l-1}$ where there are no equal m_i'. As we mentioned, this set can be distinguished locally. Thus we can prove our previous claim. We remark that unitary operations U and V^t on the A and B sides followed by projective measurements in the computational bases is equivalent to projective measurements on the A and B sides in two bases corresponding to U and V^t.

As we analyzed, the problem of local distinguishability now is whether we can find two unitary operations U and V which transform $\{X^{m_i}Z^{n_i}\}_{i=0}^{l-1}$ to the set $\{X^{m_i'}Z^{n_i'}\}_{i=0}^{l-1}$ in which no m_i' are equal. Next we give these unitary operations. The case of $d = 2$ is trivial; with the help of the Hadamard transformation H_0, we can always discriminate two Bell states by Z basis measurements on both sides. In the following, we suppose $d \neq 2$. We define d unitary operators H_α, $(\alpha = 0, 1, \ldots, d-1)$ like this; the entries of matrices H_α take the form

$$(H_\alpha)_{jk} = \omega^{-jk}\omega^{-\alpha s_k}, \qquad j, k = 0, \ldots, d-1, \qquad s_k = k + (k+1) + \cdots + (d-1). \tag{1}$$

By using H_α, we have the relations $H_\alpha X H_\alpha^\dagger = Z^{-1}X^\alpha$ and $H_\alpha Z H_\alpha^\dagger = X$. Thus H_α can transform U_{m_i,n_i} as follows:

$$H_\alpha X^{m_i}Z^{n_i}H_\alpha^\dagger = X^{m_i\alpha+n_i}Z^{-m_i} \tag{2}$$

up to a whole phase. Given l maximally entangled states corresponding to $\{X^{m_i}Z^{n_i}\}_{i=0}^{l-1}$, we can always transform them to the case where the powers of X are different by identity (do nothing) or H_α, $\alpha = 0, \ldots, d-1$. If not, then for each transformation always at least two powers of X are equal. So at least we have $d + 1$ equations altogether. But different combinations between l elements $\{(m_i, n_i)\}_{i=0}^{l-1}$ is $\binom{l}{2} = l(l-1)/2$, which is less than or equal to d. This means two pairs, for example, (m_0, n_0) and (m_1, n_1) without loss of generality, appear twice in two different transformations, say α_0 and α_1. Thus we should have the following relations:

$$\begin{aligned} \alpha_0 m_0 + n_0 &= \alpha_0 m_1 + n_1 \qquad (\mathrm{mod}\, d). \\ \alpha_1 m_0 + n_0 &= \alpha_1 m_1 + n_1 \qquad (\mathrm{mod}\, d). \end{aligned} \tag{3}$$

Thus $(m_0, n_0) = (m_1, n_1)$, which contradicts our assumption that these l maximally entangled states are orthogonal. This completes our proof.

We next clarify our proof in the case $d = 3$. Explicitly, the three operators H_α take the form

$$H_0 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}, \qquad H_1 = \begin{pmatrix} 1 & 1 & \omega \\ 1 & \omega^2 & \omega^2 \\ 1 & \omega & 1 \end{pmatrix}, \qquad H_2 = \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \\ 1 & \omega & \omega \end{pmatrix}. \tag{4}$$

Given three maximally entangled states corresponding to $\{X^{m_i}Z^{n_i}\}_{i=0}^2$, if $\{m_i\}_{i=0}^2 = \{0, 1, 2\}$, it is obvious that they are distinguishable by LOCC. If $\{n_i\}_{i=0}^2 = \{0, 1, 2\}$, by transformation H_0, they can be distinguished locally. The left unsolved cases have the form $\{(m_0, n_0), (m_0, n_1), (m_2, n_0)\}$ where $n_0 \neq n_1, m_0 \neq m_2$. This form can neither be locally distinguished by direct measurements in the computational basis nor can be distinguished by H_0 followed by measurements in the computational basis. But H_1 or H_2 will transfer the power of X to the set $\{0, 1, 2\}$. If not, that means that

$$m_0 + n_1 = m_2 + n_0, \qquad 2m_0 + n_1 = 2m_2 + n_0, \qquad \mathrm{mod}3. \tag{5}$$

Then we know that $m_0 = m_2$, $n_0 = n_1$, which contradicts our assumption. Therefore *any three maximally entangled states from the set* $\{(U_{m,n} \otimes I)|\Psi\rangle^{AB}\}_{m,n=0}^2$ *can be distinguished by LOCC.*

We give one example to explain our local discrimination method. Suppose the given set is $\{X, Z, XZ\}$; by H_2, we have $\{XZ^2, X^2, Z^2\}$ corresponding to $|10\rangle + \omega^2|21\rangle + \omega|02\rangle$, $|20\rangle + |01\rangle + |12\rangle$, and $|00\rangle + \omega^2|11\rangle + \omega|22\rangle$, which can simply be discriminated locally.

In the general d case, the d independent transformations H_α are not enough to locally distinguish arbitrary d maximally entangled states in the set $\{(X^{m_i}Z^{n_i} \otimes I)|\Phi^+\rangle^{AB}\}_{i=0}^{d-1}$, so we need to find other transformations. Here we can remark that any transformation which changes the power of X to $jm_i + kn_i$, $j, k = 0, \ldots, d-1$ cannot provide new transformations different from identity and these d transformations H_α.

Set of quantum states that are locally indistinguishable by LOCC by entanglement breaking channel.—Horodecki *et al.* showed that an arbitrary complete set of orthogonal states of any bipartite system is locally indistinguishable if at least one of the vectors is entangled [5]. Next we show the following result: An ensemble of linearly independent quantum states $\{\rho_{m,n}^{AB}\}_{m,n=0}^{d-1}$ cannot be discriminated deterministically or probabilistically by LOCC, where $\rho_{m,n}^{AB} = (U_{m,n} \otimes I)\rho^{AB}(U_{m,n}^\dagger \otimes I)$. We remark that the quantum states of this ensemble are generally mixed states. This set may include both orthogonal and nonorthogonal quantum states.

We say that a quantum channel Λ is entanglement breaking if, for all input states, the output states of the channel $\Lambda \otimes I$ are separable states. We define a quantum channel Λ^{AC} as follows:

$$\Lambda^{AC}(\rho^{AC}) = \frac{1}{d^2}\sum_{mn} U_{m,n} \otimes U_{m,-n}(\rho^{AC})U_{m,n}^{\dagger} \otimes U_{m,-n}^{\dagger}. \quad (6)$$

Next we prove that this is an entanglement breaking quantum channel. To prove that a quantum channel Λ is an entanglement breaking one, it is enough to show that $\Lambda \otimes I$ maps a maximally entanglement state into a separable state[10–12]. Considering that the quantum state $|\Phi_{0,0}^{AB}\rangle \otimes |\Phi_{0,0}^{CD}\rangle$ of four systems $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$ is a maximally entangled state across the $AC{:}BD$ cut, from definition (6), we should show that

$$\Lambda^{AC} \otimes I^{BD}(\Phi_{0,0}^{AB} \otimes \Phi_{0,0}^{CD}) = \frac{1}{d^2}\sum_{mn} |\Phi_{m,n}^{AB}\rangle\langle\Phi_{m,n}^{AB}| \otimes |\Phi_{m,-n}^{CD}\rangle\langle\Phi_{m,-n}^{CD}| \quad (7)$$

is a separable state. Actually, we have the following symmetry:

$$\frac{1}{d^2}\sum_{mn} |\Phi_{m,n}^{AB}\rangle\langle\Phi_{m,n}^{AB}| \otimes |\Phi_{m,-n}^{CD}\rangle\langle\Phi_{m,-n}^{CD}| = \frac{1}{d^2}\sum_{kl} |\Phi_{k,l}^{AC}\rangle\langle\Phi_{k,l}^{AC}| \otimes |\Phi_{k,-l}^{BD}\rangle\langle\Phi_{k,-l}^{CD}|. \quad (8)$$

It is obvious that this is a separable state across the $AC{:}BD$ cut. Thus we show that Λ^{AC} defined in Eq. (6) is an entanglement breaking channel. Equation (8) can be proven, and we substitute the relation

$$|\Phi_{0,0}^{AB}\rangle \otimes |\Phi_{0,0}^{CD}\rangle = \frac{1}{d}\sum_{m,n} |\Phi_{m,n}^{AC}\rangle \otimes |\Phi_{m,-n}^{BD}\rangle \quad (9)$$

into $\Lambda^{AC} \otimes I^{BD}(|\Phi_{0,0}^{AB}\rangle \otimes |\Phi_{0,0}^{CD}\rangle)$. With the help of the relation $U_{m,n}U_{k,l} = \omega^{nk-ml}U_{k,l}U_{m,n}$, and knowing that $|\Phi_{0,0}\rangle$ is invariant under the action of $U_{m,n} \otimes U_{m,-n}$, one can readily show Eq. (8). We remark that the quantum state (8) is the so-called unlockable bound entangled state in the d dimension [13].

Now we are ready for our result of local indistinguishability. Given the set of linearly independent states $\{\rho_{m,n}^{AB}\}_{m,n=0}^{d-1}$ to be discriminated, we can construct a quantum state

$$\rho = \frac{1}{d^2}\sum_{mn} \rho_{m,n}^{AB} \otimes |\Phi_{m,-n}^{CD}\rangle\langle\Phi_{m,-n}^{CD}| = \Lambda^{AC} \otimes I^{BD}(\rho^{AB} \otimes \Phi^{CD}). \quad (10)$$

Here the maximally entangled states $\{|\Phi_{m,-n}^{CD}\rangle\}$ act as detectors. Since we know that the quantum channel Λ^{AC} is an entanglement breaking one, so this mixed state ρ is a separable state across the $AC{:}BD$ cut. Thus we can show that *a set of linearly independent quantum states* $\{\rho_{m,n}\}_{m,n=0}^{d-1}$ *cannot be distinguished deterministically or probabilistically by LOCC* [14]. If they could be distinguished deterministically or probabilistically, one could distill nonzero entanglement by LOCC. This contradicts the observation that ρ is a separable state across the $AC{:}BD$ cut. Here we follow the same reasoning as in [5,8,9]. Note that $\{\rho_{m,n}^{AB}\}_{m,n=0}^{d-1}$ is in the $d \otimes d'$ system, and d, d' are not necessarily the same. We also should point out that if $\rho^{AB} = |\Psi^{AB}\rangle\langle\Psi^{AB}|$, which is a pure state, $\{|\Psi_{m,n}\rangle\}_{m,n=0}^{d-1}$ are not necessarily orthogonal to each other, where we denote $|\Psi_{m,n}\rangle = U_{m,n} \otimes I|\Psi\rangle$. Therefore this case is not covered by the result in [5,9]. Certainly, distinguishability of nonorthogonal states is less than that of orthogonal states, but still they can be distinguished probabilistically by global measurements and for some cases by LOCC [15,16]. We do not discuss the case that $\{|\rho_{m,n}^{AB}\}_{m,n=0}^{d-1}$ are linearly dependent.

Next we give three examples:

Example 1: According to our result, an ensemble of states $|\Psi_{0,0}\rangle = \alpha|00\rangle + \beta|11\rangle$, $|\Psi_{0,1}\rangle = \alpha|00\rangle - \beta|11\rangle$, $|\Psi_{1,0}\rangle = \alpha|10\rangle + \beta|01\rangle$, and $|\Psi_{1,1}\rangle = \alpha|10\rangle - \beta|01\rangle$ cannot be distinguished by LOCC [17]. Here we do not consider the special cases such as $\alpha\beta = 0$, which lead to the result that the quantum states of this ensemble are linearly dependent. One can find that $|\Psi_{0,0}\rangle$ and $|\Psi_{0,1}\rangle$ are generally nonorthogonal, while they are orthogonal with $|\Psi_{1,0}\rangle, |\Psi_{1,1}\rangle$. Thus this ensemble consists of both orthogonal and nonorthogonal states. Also, this case is not studied previously. As a special case, we can show that four Bell states cannot be distinguished by LOCC, which has already been pointed out in [8].

Example 2: We can choose a quantum state in $|\Psi^{AB}\rangle$ in a $2 \otimes d'$ system, say, let $d' = 4$. For example, let $|\Psi^{AB}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |12\rangle + |13\rangle)$, and we have four orthogonal states $\{(U_{m,n} \otimes I)|\Psi^{AB}\rangle\}_{m,n=0}^{1}$. According to our criterion, they cannot be distinguished by LOCC. Horodecki *et al.* once showed that an arbitrary complete set of orthogonal states in a bipartite system cannot be distinguished by LOCC if at least one of these states is entangled, deterministically or probabilistically [5]. We know that three Bell states that are incomplete can be distinguished probabilistically, and two Bell states can be distinguished deterministically [2]. An interesting question concerns whether there exist incomplete sets of orthogonal states that cannot be distinguished even probabilistically. Here we present an example to show that there exists an incomplete set of orthogonal states which cannot be distinguished by LOCC no matter whether the protocol is deterministic or probabilistic. Certainly, we can also give an example of nonorthogonal states with the same property. In Ref. [5], Horodecki *et al.* presented an example of an incomplete set of orthogonal states that is indistinguishable by LOCC deterministically. However, it is still possible that this set is locally distinguishable probabilistically. One may point out that these four states are essentially four Bell states. It is true; however, our conclusion is not trivial. In general, for a bipartite system $d \otimes d'$, there exist d^2 orthogonal states that cannot be distinguished by LOCC [18], even probabilistically. These d^2 orthogonal states are not a complete set if $d \neq d'$.

Example 3: Our result is generally for mixed states. For the qubits case, let $\rho^{AB} = \frac{4p-1}{3}|\Phi^+\rangle\langle\Phi^+| + \frac{1-p}{3}I$ be the Werner state. Then we know that four different Werner state sets $\{(U_{m,n} \otimes I)\rho^{AB}(U_{m,n}^\dagger \otimes I)\}_{m,n=0}^{1}$ are locally indistinguishable, where $p \neq 1/4$.

We can generalize the previous result to states in the $2^N \otimes 2^N$ case. It is straightforward to show that $\{|\Psi_{m_1,n_1}^{A_1B_1}\rangle \otimes |\Psi_{m_2,n_2}^{A_2B_2}\rangle \otimes \cdots \otimes |\Psi_{m_N,n_N}^{A_NB_N}\rangle\}_{m_i,n_i=0}^{1}$ are indistinguishable by LOCC across the $A_1 \cdots A_N$:$B_1 \cdots B_N$ cut, irrespective that the protocol is deterministic or probabilistic, where $|\Psi_{m_i,n_i}^{A_iB_i}\rangle = (U_{m_i,n_i} \otimes I)(\alpha_i|00\rangle + \beta_i|11\rangle)$, $\alpha_i\beta_i = 0$, and $m_i, n_i = 0, 1$.

Similarly, we can study a more general case of the $\prod_{i=1}^{N} \otimes(d_i \otimes d_i')$ system. We define the quantum channel Λ^{AC}, in Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_C$, where $\mathcal{H}_A = \mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_N}$, similarly for $\mathcal{H}_C$. We can find that the quantum channel defined as

$$\Lambda^{AC}(\rho^{AC}) = \sum_{\vec{m}\,\vec{n}} U_{\vec{m},\vec{n}} \otimes U_{\vec{m},-\vec{n}}(\rho^{AC})U_{\vec{m},\vec{n}}^\dagger \otimes U_{\vec{m},-\vec{n}}^\dagger \quad (11)$$

is an entanglement breaking channel, where we use the notations $U_{\vec{m},\vec{n}} = U_{m_1,n_1} \otimes \cdots \otimes U_{m_N,n_N}$. And thus we can show that for an ensemble of linearly independent quantum states $\{\rho_{m_1,n_1}^{A_1B_1} \otimes \cdots \otimes \rho_{m_N,n_N}^{A_NB_N}\}_{m_i,n_i=0}^{d-1}$, they can be distinguished neither deterministically nor probabilistically. Note that the A side has subsystems $A_1 \otimes \cdots \otimes A_N$ and collective measurements are allowed in discrimination. But A and B are spatially separated parties and only classical communication is allowed.

Horodecki *et al.* also proposed a method to construct a pure quantum state by the superposition rather than the mixture [5]. Then by the Jonathan-Plenio criterion [19] based on the majorization scheme[20,21], one can check whether the given quantum states can be distinguished or not if only LOCC is allowed. Generally, this method relies on some numerical search which may be complicated. Chefles recently showed a necessary and sufficient condition for LOCC unambiguous state discrimination [22]. In this Letter, we develop the method of constructing a mixed state [5,8,9,23]; then, by the definition of entanglement breaking channel, we show a family of states that are indistinguishable by LOCC, deterministically or probabilistically.

In summary, we proposed a family of unitary transformations $\{H_\alpha\}_{\alpha=0}^{d-1}$ in (1). By projective measurements corresponding to these transformations, we can locally discriminate any l maximally entangled states chosen from the set $\{(U_{m,n} \otimes I)|\Psi\rangle^{AB}\}_{m,n=0}^{d-1}$ if $l(l-1) \leq 2d$. This is the first explicit result for locally discriminating several states in a general d-dimensional system. However, an interesting problem arises here: in case $l(l-1) > 2d, l \leq d$, can we find l maximally entangled states from the given set that is locally indistinguishable?

The author thanks K. Matsumoto, M. Plenio, T. Shimono, and X. B. Wang for useful discussions and suggestions.

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[2] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000)
[3] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
[4] 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).
[5] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
[6] The reason that we restrict d to the prime case is that the transformations H_α corresponding to mutually unbiased states [7] are valid only when d is prime.
[7] S. Bandyopadhyay *et al.*, Algorithmica **34**, 512 (2002).
[8] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).
[9] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De), and U. Sen, Phys. Rev. A **65**, 062307 (2002).
[10] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[11] G. Vidal, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **89**, 027901 (2002).
[12] M. Horodecki, P.W. Shor, and M. B. Ruskai, quant-ph/0302031.
[13] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
[14] In this Letter, we consider only the case that one copy of the quantum state is provided.
[15] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001).
[16] Y. X. Chen, and D. Yang, Phys. Rev. A **64**, 064303 (2001); **65**, 022320 (2002).
[17] When we say that the quantum states cannot be distinguished by LOCC, we mean that they cannot be distinguished by LOCC deterministically or probabilistically.
[18] Without loss of generality, we assume $d' \geq d$.
[19] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
[20] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[21] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
[22] A. Chefles, quant-ph/0302066.
[23] B. M. Terhal, D. P. DiVincenzo, and D.W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).