Local Distinguishability of Multipartite Unitary Operations

Runyao Duan,* Yuan Feng,† and Mingsheng Ying‡

State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084

(Received 18 May 2007; published 17 January 2008)

We show that any two different unitary operations acting on an arbitrary multipartite quantum system can be perfectly distinguished by local operations and classical communication when a finite number of runs is allowed. Intuitively, this result indicates that the lost identity of a nonlocal unitary operation can be recovered locally. No entanglement between distant parties is required.

DOI: 10.1103/PhysRevLett.100.020503 PACS numbers: 03.67.Hk, 03.65.Ta, 03.65.Ud, 03.67.Lx

Unitary operation is one of the most fundamental ingredients of quantum mechanics. The study of various properties of unitary operation lies at the heart of quantum information processing. Recently the discrimination of unitary operations has received considerable attention [1–3]. In particular, the well-known effect of quantum superdense coding [4] can be treated as an instance of distinguishing unitary operations [1,5]. Although two nonorthogonal quantum states cannot be perfectly distinguishable when only a finite number of copies is available [6], it was shown that any two different unitary operations can always be perfectly distinguishable by preparing a suitable entangled state as input and then applying only a finite number of runs of the unknown unitary operation [2]. This result was further refined by showing that the entangled input state is not necessary [3]. The probabilistic discrimination of unitary operations as well as general quantum operations has also been studied extensively [7].

All of the above discrimination schemes of quantum operations assume that the unknown quantum operation to be identified is under the complete control of a single party who can prepare any entangled state or perform any unconstrained quantum measurement. However, any reasonable quantum system in practice generally consists of many subsystems. Nonlocal unitary operation is a valuable resource to provide interaction between different subsystems [8]. The problem of distinguishing multipartite unitary operations naturally arises when several parties share a unitary operation but forget its real identity. As in this scenario different parties may be far from each other; a reasonable constraint is that each party is only allowed to perform local operations and classical communication (LOCC). Moreover, we assume there is no entanglement shared between any two distant parties. A general scheme for LOCC discrimination is intuitively depicted in Fig. 1. Two special kinds of schemes are of particular interest. A scheme is said to be *parallel* if the computational network in Fig. 1 reduces to the form of $U^{\otimes n}$ for some finite n. While a scheme is said to be *sequential* if no auxiliary quantum systems are involved. Clearly, a sequential scheme represents the most economic strategy for discrimination.

The purpose of this Letter is to give an explicit scheme to show that any two multipartite unitary operations can be perfectly distinguished even under the constraint of LOCC. Our scheme is rather simple as it only involves parallel and sequential schemes and only requires one party to prepare local entanglement. By similar arguments as those in Refs. [2,3], this result can be directly extended to the case when the number of the unitary operations to be discriminated is more than two. It is remarkable that the lost identity of a nonlocal unitary operation can be recovered locally without the assistance of any *a priori* entanglement. To the best of our knowledge, this is the first result about the local distinguishability of multipartite quantum operations. Hopefully, such a result may sharpen our understanding of the nature of nonlocal unitary operations and provide a potentially powerful new tool for quantum information theory. An immediate application is as follows. Suppose several parties share a unitary operation which is secretly chosen from a finite set of unitary operations, each of which is assumed to be capable of creating entanglement. Then these parties can always produce pure multipartite entanglement with certainty by employing the unknown operation shared among them as they can locally figure out the exact identity of this unitary. But the same task is not possible if we consider the distillation of nonorthogonal entangled states instead of unitary operations.

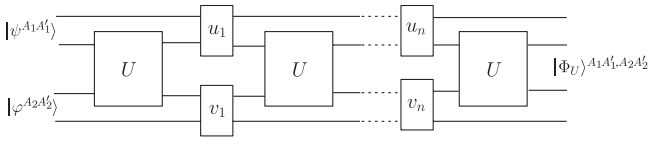

FIG. 1. Illustration of LOCC discrimination of unitary operations. Here $U \in \{U_1, U_2\}$ represents the unknown unitary operation. A general scheme for identifying U is as follows: (1) Prepare suitable input states $|\psi\rangle^{A_1A_1'}$ and $|\varphi\rangle^{A_2A_2'}$, where A_1' and A_2' are auxiliary systems of Alice and Bob, respectively; (2) perform a finite number of runs of U and insert appropriate local unitary operations u_k and v_k between every two successive runs; (3) distinguish the final output states $|\Phi_U\rangle$ by LOCC. U_1 and U_2 can be locally distinguished if and only if the output states $|\Phi_{U_1}\rangle$ and $|\Phi_{U_2}\rangle$ can be orthogonal [9].

The scheme presented in this Letter automatically provides a new approach to show the perfect distinguishability between unitary operations in the global scenario [2,3]. However, due to the nonlocal nature of general multipartite unitary operations and the complicated structure of LOCC, the proof for the local distinguishability is rather involved and needs several completely new ideas and techniques.

Consider a multipartite quantum system consisting of N subsystems, which can be partitioned into m disjoint nonempty groups $A_1, \ldots, A_m$ for any $1 \le m \le N$. Each disjoint partition is naturally associated with a class of LOCC operations by treating A_k's as distant parties. Assume the kth group has a state space $\mathcal{H}_k$ with dimension d_k. The whole state space $\mathcal{H}$ is given by $\otimes_{k=1}^m \mathcal{H}_k$ with a total dimension $d = d_1 \cdots d_m$. The set of linear operations acting on $\mathcal{H}$ is denoted by $\mathcal{B}(\mathcal{H})$. A unitary operation $U \in \mathcal{B}(\mathcal{H})$ is said to be local or decomposable if $U = \otimes_{k=1}^m u_k$ such that $u_k \in \mathcal{B}(\mathcal{H}_k)$. Otherwise U is nonlocal or entangled. Two unitary operations U and V are said to be different if $U = e^{i\theta} V$ cannot hold for any real number θ. With these notations, our main result can be simply stated as follows: Any two different unitary operations U_1 and U_2 acting on $\mathcal{H}$ can be perfectly distinguished by LOCC operations associated with any disjoint partition of subsystems. In particular, unitary operations acting on a 2^m-dimensional state space can be locally distinguished by m distant parties each of which accesses the unknown unitary via a single qubit.

The results in this Letter heavily depend on the properties of a mathematical notion named numerical range. For $A \in \mathcal{B}(\mathcal{H})$, the numerical range of A is a subset of complex numbers defined as follows:

$$W(A) = \{\langle\psi|A|\psi\rangle : \langle\psi|\psi\rangle = 1\}. \quad (1)$$

If $|\psi\rangle$ in Eq. (1) can be made entangled, then the entanglement-assisted numerical range of A is defined as follows:

$$W_a(A) = \cup_{\mathcal{H}'} W(A \otimes I_{\mathcal{H}'}),$$

where $\mathcal{H}'$ ranges over all finite dimensional state spaces. The local numerical range of A is a subset of $W(A)$ with the additional requirement that $|\psi\rangle$ in Eq. (1) is a product state. That is,

$$W^{\text{local}}(A) = \{\langle\psi|A|\psi\rangle : |\psi\rangle = \otimes_{k=1}^m |\psi_k\rangle\},$$

where $|\psi_k\rangle \in \mathcal{H}_k$ and $\langle\psi_k|\psi_k\rangle = 1$. The local entanglement-assisted numerical range $W_a^{\text{local}}(A)$ can be defined similar to $W_a(A)$. One can verify by a direct calculation that $W_a(A) = \{\text{tr}(A\rho) : \rho \ge 0, \text{tr}(\rho) = 1\}$. Similarly,

$$W_a^{\text{local}}(A) = \{\text{tr}(A\rho) : \rho = \otimes_{k=1}^m \rho_k\},$$

where ρ_k is a density operator on $\mathcal{H}_k$.

If A is normal, i.e., $AA^\dagger = A^\dagger A$, then by spectral decomposition theorem it is easy to verify that $W(A) = \text{Co}(\sigma(A))$, where $\sigma(A)$ represents the set of eigenvalues of A and $\text{Co}(S)$ denotes the convex hull of S for $S \subseteq \mathcal{C}$. Interestingly, a celebrated result due to Toeplitz and Hausdorff states that the numerical range of a bounded linear operation is always convex [10].

Lemma 1: For any $A \in \mathcal{B}(\mathcal{H})$, $W(A)$ is convex. More precisely, for any finite set of normalized vectors $\{|\psi_k\rangle\}$ and any finite probability distribution $\{p_k\}$, there exists a normalized vector $|\psi\rangle \in \text{span}\{|\psi_k\rangle\}$ such that $\langle\psi|A|\psi\rangle = \sum_k p_k \langle\psi_k|A|\psi_k\rangle$.

One can easily verify that $W_a(A) = \text{Co}(W(A)) = W(A)$. Intuitively, local entanglement cannot broaden the local numerical range. Such a result holds even in the multipartite scenario.

Lemma 2: For any $A \in \mathcal{B}(\mathcal{H})$, $W_a^{\text{local}}(A) = W^{\text{local}}(A)$.

Proof: The key is to repeatedly apply Lemma 1. For simplicity, we consider only the bipartite case. Denote $f(\psi_1, \psi_2) = \text{tr}(A|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|)$. First we observe that $f(\psi_1, \psi_2) = \langle\psi_1|A_{\psi_2}|\psi_1\rangle$, where $A_{\psi_2} = \text{tr}_{\mathcal{H}_2}(AI_{\mathcal{H}_1} \otimes |\psi_2\rangle\langle\psi_2|)$. So it follows from Lemma 1 and the symmetry that $f(\psi_1, \psi_2)$ is convex in $|\psi_1\rangle\langle\psi_1|$ (or $|\psi_2\rangle\langle\psi_2|$) when $|\psi_2\rangle\langle\psi_2|$ ($|\psi_1\rangle\langle\psi_1|$) is fixed. Hence for any density operators ρ_1 and ρ_2 there should exist pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $\text{tr}(A\rho_1 \otimes \rho_2) = f(\psi_1, \psi_2)$. □

We shall employ a fundamental result by Walgate *et al.* [9] to study the local distinguishability of nonlocal unitary operations. That is, any two multipartite orthogonal pure states are perfectly distinguishable by LOCC. By this result, the relation between local distinguishability of unitary operations and the local numerical range now is clear; i.e., U_1 and U_2 are locally distinguishable if and only if $0 \in W_a^{\text{local}}(U_1^\dagger U_2)$. Applying Lemma 2, we have

Theorem 1: Two unitary operations U_1 and U_2 are perfectly distinguishable by LOCC in the single-run scenario if and only if $0 \in W^{\text{local}}(U_1^\dagger U_2)$.

Theorem 1 indicates that local entanglement is not necessary for the perfect local discrimination between two unitary operations in the single-run scenario. From now on, a state $|\psi\rangle$ such that $\langle\psi|A|\psi\rangle = 0$ is said to be an *isotropic vector* for A. The term *isotropic product vector* is used when $|\psi\rangle$ is a product state. As an illustrative example of Theorem 1, consider a special case where U_1 and U_2 are orthogonal, i.e., $\text{tr}(U_1^\dagger U_2) = 0$. Note that $\text{tr}(U_1^\dagger U_2) = 0$ can be reformulated as $\text{tr}(U_1^\dagger U_2 \otimes_{k=1}^m I_{\mathcal{H}_k}/d_k) = 0$. It follows from Lemma 2 that there exists a product state $|\psi\rangle$ such that $\text{tr}(U_1^\dagger U_2 |\psi\rangle\langle\psi|) = 0$, which means U_1 and U_2 are locally distinguishable with a single use and no local entanglement is needed.

Theorem 1 also implies that local discrimination of unitary operations is much more complicated than the global discrimination in the single-run scenario. To see this, take U_1 and U_2 such that $U_1^\dagger U_2 = |00\rangle\langle 00| + e^{i\theta_1}|01\rangle\langle 01| + e^{i\theta_2}|10\rangle\langle 10| - |11\rangle\langle 11|$ for $0 < \theta_1, \theta_2 < \pi$. One can directly verify that $0 \in W(U_1^\dagger U_2)$ but $0 \notin W^{\text{local}}(U_1^\dagger U_2)$.

Remarkably, if we are allowed to use the unknown unitary repeatedly, then any two different unitary operations become locally distinguishable. The proof of this fact is rather complicated and is summarized in Theorems 2 and 3 below.

Two technical lemmas are required to prove Theorem 2. The first lemma gives an alternative characterization of Hermitian operations.

Lemma 3: Let $\{\rho_k : 1 \le k \le d^2\}$ be a Hermitian basis for $\mathcal{B}(\mathcal{H})$. Then $A \in \mathcal{B}(\mathcal{H})$ is Hermitian if and only if $\mathrm{tr}(A\rho_k) \in \mathcal{R}$ for all $1 \le k \le d^2$.

We can construct a special Hermitian basis containing only rank one operations [11]. Let $\{|k\rangle : 1 \le k \le d\}$ be orthonormal basis for $\mathcal{H}$. For $1 \le p < q \le d$, let $|\psi^+_{pq}\rangle = (|p\rangle + |q\rangle)/\sqrt{2}$ and $|\psi^-_{pq}\rangle = (|p\rangle + i|q\rangle)/\sqrt{2}$. In addition, for $1 \le p \le d$ let $|\psi_{pp}\rangle = |p\rangle$. Then

$$\{|\psi^\pm_{pq}\rangle\langle\psi^\pm_{pq}| : 1 \le p < q \le d\} \cup \{|\psi_{pp}\rangle\langle\psi_{pp}| : 1 \le p \le d\}$$

is a Hermitian basis for $\mathcal{B}(\mathcal{H})$. Consequently, for a multipartite state space $\mathcal{H} = \otimes_{k=1}^m \mathcal{H}_k$, we can construct a Hermitian basis S for $\mathcal{B}(\mathcal{H})$ such that any $s \in S$ is a product pure state.

The second Lemma supplies a connection between numerical range and tensor product. Note $\lceil x \rceil$ represents the minimum of the integers that are not less than x.

Lemma 4: Let $A \in \mathcal{B}(\mathcal{H})$, and let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two vectors such that $\langle\psi_1|A|\psi_1\rangle = r_1 e^{i\theta_1}$ and $\langle\psi_2|A|\psi_2\rangle = r_2 e^{i\theta_2}$ satisfy $r_1, r_2 > 0$ and $0 \le \theta_1 < \theta_2 < 2\pi$, i.e., with different arguments. Define $\theta = \min\{\theta_2 - \theta_1, 2\pi + \theta_1 - \theta_2\}$ and $N = \lceil \pi/\theta \rceil$. Then $0 \in W(A^{\otimes N})$, and the isotropic vector $|\psi\rangle$ can be chosen from $\mathrm{span}\{|\psi_1\rangle^{\otimes N-k}|\psi_2\rangle^{\otimes k} : 0 \le k \le N\}$.

Proof: To be specific, let us assume $\theta_1 = 0$ and $0 < \theta_2 = \theta \le \pi$. Denote $z_k = r_1^{N-k} r_2^k e^{ik\theta}$ and $|\Phi_k\rangle = |\psi_1\rangle^{\otimes N-k}|\psi_2\rangle^{\otimes k}$ for $0 \le k \le N$. Then $z_k = \langle\Phi_k|A^{\otimes N}|\Phi_k\rangle$ and $z_k \in W(A^{\otimes N})$. By Lemma 1 we have $\mathrm{Co}(\{z_k\}) \subseteq W(A^{\otimes N})$. To complete the proof, we only need to show that $0 \in \mathrm{Co}(\{z_k\})$. If $N\theta = \pi$, we have $z_N < 0$ and $z_0 > 0$. That means $0 \in \mathrm{Co}(\{z_0, z_N\})$. Otherwise we have $N\theta > \pi$ and $0 < (N-1)\theta < \pi$. By a geometrical observation one can easily verify that $0 \in \mathrm{Co}(\{z_0, z_{N-1}, z_N\})$. So $0 \in W(A^{\otimes N})$. By Lemma 1 again, the isotropic state $|\psi\rangle$ for $A^{\otimes N}$ can be chosen as a linear combination of $|\Phi_k\rangle$. □

Lemma 4 is extremely useful in studying the distinguishability of quantum operations. For instance, it implies the perfect distinguishability between unitary operations by a parallel scheme [2].

With Lemma 4 in hand, we are ready to show that a perfect discrimination between two multipartite unitary operations U_1 and U_2 by a parallel scheme is always possible except for a peculiar case.

Theorem 2: Suppose U_1 and U_2 satisfy that $U_1^\dagger U_2$ is non-Hermitian (up to some phase factor), then there exists a finite N such that $0 \in W^{\mathrm{local}}((U_1^\dagger U_2)^{\otimes N})$.

Proof: Since $U_1^\dagger U_2$ is non-Hermitian, it follows from Lemma 3 that any product Hermitian basis for $\mathcal{B}(\mathcal{H})$ should contain two product states $|\psi\rangle = \otimes_{k=1}^m |\psi_k\rangle$ and $|\varphi\rangle = \otimes_{k=1}^m |\varphi_k\rangle$ such that $\langle\psi|U_1^\dagger U_2|\psi\rangle$ and $\langle\varphi|U_1^\dagger U_2|\varphi\rangle$ are with different arguments. Without loss of generality, we may assume that $|\psi_k\rangle$ and $|\varphi_k\rangle$ are not equal (up to some phase factor) for each $1 \le k \le m$.

Construct a sequence of product states as follows:

$$|\Phi_n\rangle = (\otimes_{k=1}^{m-n}|\psi_k\rangle) \otimes (\otimes_{l=m-n+1}^{m}|\varphi_l\rangle), \qquad 0 \le n \le m.$$

Denote $z_n = \langle\Phi_n|U_1^\dagger U_2|\Phi_n\rangle$. We have $|\Phi_0\rangle = |\psi\rangle$ and $|\Phi_m\rangle = |\varphi\rangle$. Furthermore, any two successive states $|\Phi_n\rangle$ and $|\Phi_{n+1}\rangle$ differ at exactly one subsystem. Hence any state from $\mathrm{span}\{|\Phi_n\rangle, |\Phi_{n+1}\rangle\}$ is a product state. If $z_n = 0$ for some $0 \le n \le m$, then $|\Phi_n\rangle$ is an isotropic product vector for $U_1^\dagger U_2$ and the proof is completed. Otherwise there exists n such that z_n and z_{n+1} are with different arguments, as z_0 and z_m are with different arguments. Applying Lemma 4 we know there exists N such that $0 \in W((U_1^\dagger U_2)^{\otimes N})$. Moreover, the isotropic vector $|\phi\rangle$ can be chosen from $\mathrm{span}\{|\Phi_n\rangle, |\Phi_{n+1}\rangle\}^{\otimes N}$ and is clearly a product state. □

From the above proof it is clear that only one party is required to prepare local entanglement.

The local distinguishability of U_1 and U_2 such that $U_1^\dagger U_2$ is Hermitian has not yet been confirmed. For the $2 \otimes n$ case one can easily show that any such U_1 and U_2 are locally distinguishable by a single run. For a higher dimensional case, there exist unitary operations U_1 and U_2 that are not locally distinguished by a parallel scheme. An explicit instance is obtained by taking $U_1^\dagger U_2 = I - 2|\Phi\rangle\langle\Phi|$, where $|\Phi\rangle$ is a $d \otimes d$ maximally entangled state and $d > 2$.

Nevertheless, we can transform the Hermitian case to the non-Hermitian case by applying a sequential scheme. The following Lemma is helpful in doing such transformation.

Lemma 5: Let A and B be Hermitian operations acting on $\mathcal{H}$ such that $u^\dagger AuB$ is Hermitian for any local unitary u. Then $\mathrm{tr}(u^\dagger AuB) = \mathrm{tr}(A)\mathrm{tr}(B)/d$ for any local unitary u, where d is the dimension of $\mathcal{H}$.

Proof: Let $f(u) = \mathrm{tr}(u^\dagger AuB)$. Then $f(u) \in \mathcal{R}$ for any local unitary u. By continuity, the set of $f(u)$ is a real line segment or a singleton. On the other hand, $u^\dagger AuB$ is Hermitian implies that $u^\dagger Au$ and B are simultaneously diagonalizable under some unitary operation. Therefore $f(u)$ should be of the form $\sum_{k=1}^d \lambda_{\xi(k)}\mu_k$ for some permutation ξ, where λ_k and μ_k are eigenvalues of A and B, respectively. So $f(u)$ can take at most $d!$ possible values and should be a constant C for any local unitary u. To calculate C explicitly, choose a set of local unitary operations $\{u_k : 1 \le k \le d^2\}$ on $\mathcal{H}$ such that the following identity holds:

$$1/d^2 \sum_{k=1}^{d^2} u_k^\dagger T u_k = \mathrm{tr}(T) I_{\mathcal{H}}/d, \quad \forall\ T \in \mathcal{B}(\mathcal{H}).$$

Such local unitary operations do exist as one may choose $\{u_k\}$ as the tensor products of the generalized Pauli matrices acting on $\mathcal{H}_l$. Setting $T = A$ and multiplying B yields

$$1/d^2 \sum_{k=1}^{d^2} u_k^\dagger A u_k B = \mathrm{tr}(A) B/d.$$

Taking trace and noticing that $\mathrm{tr}(u_k^\dagger A u_k B) = C$ for any $1 \le k \le d^2$, we have $C = \mathrm{tr}(A)\mathrm{tr}(B)/d$. □

The following theorem deals with the case when $U_1^\dagger U_2$ is Hermitian.

Theorem 3: Let U_1 and U_2 be two different unitary operations acting on $\mathcal{H}$ such that $U_1^\dagger U_2$ is Hermitian. Then there exists a finite $n > 1$ and a sequence of local unitary operations $u^{(1)}, \ldots, u^{(n-1)}$ such that $W_1^\dagger W_2$ is non-Hermitian, where $W_k = U_k u^{(1)} \cdots u^{(n-1)} U_k$, $k = 1, 2$.

Proof: Without loss of generality, we may assume that $U_1^\dagger U_2 = D$ for some Hermitian D such that $0 < \mathrm{tr}(D) < d$. By contradiction, assume $W_1^\dagger W_2$ is always Hermitian. Let $D^{(n)} = (U_1^n)^\dagger U_2^n$. We shall prove that

$$\mathrm{tr}\,(D^{(n)}) = (\mathrm{tr}(D)/d)^{n-1}\,\mathrm{tr}(D), \qquad n \ge 1. \tag{2}$$

The case of $n = 1$ holds trivially. Assume $n > 1$. By the assumption we have

$$(U_1^{n-1} u U_1)^\dagger (U_2^{n-1} u U_2) = U_1^\dagger [u^\dagger D^{(n-1)} u U_1 D U_1^\dagger] U_1$$

is Hermitian for any local unitary u. Applying Lemma 5 and setting $u = I_{\mathcal{H}}$ we have

$$\mathrm{tr}\,(D^{(n)}) = \mathrm{tr}(D^{(n-1)})\,\mathrm{tr}(U_1 D U_1^\dagger)/d.$$

Solving this relation we obtain Eq. (2).

However, Eq. (2) cannot be true for all $n > 1$ as $0 < \mathrm{tr}(D) < d$. Actually, for sufficiently large n we should have $\mathrm{tr}(D^{(n)}) < 1$, which contradicts the fact that $\mathrm{tr}(D^{(n)})$ is a positive integer. □

The proofs of Lemma 5 and Theorem 3 provide a constructive method to calculate an upper bound of n and local unitary operations $u^{(k)}$ such that $W_1^\dagger W_2$ is non-Hermitian. Combining with Theorem 2, we obtain an explicit scheme for locally distinguishing any two multipartite unitary operations.

In conclusion, we study the problem of distinguishing multipartite unitary operations using LOCC only, and show that a perfect local discrimination according to arbitrary partition is always possible. It remains unknown whether a perfect discrimination can be achieved by merely a sequential scheme. Another challenging problem is to determine the minimal number of runs needed for a perfect discrimination between two multipartite unitary operations in the LOCC scenario. These problems have been completely solved in the global scenario [2,3].

We thank Z. Ji, G. Wang, J. Chen, Z. Wei, and C. Zhang for helpful conversations. This work was partly supported by the Natural Science Foundation of China (Grants No. 60702080, No. 60736011, No. 60621062, and No. 60503001) and the Hi-Tech Research and Development Program of China (863 project) (Grant No. 2006AA01Z102). Y. F. was also partly supported by the FANEDD under Grant No. 200755.

*dry@tsinghua.edu.cn
†feng-y@tsinghua.edu.cn
‡yingmsh@tsinghua.edu.cn

[1] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000).
[2] A. Acín, Phys. Rev. Lett. **87**, 177901 (2001); G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).
[3] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **98**, 100503 (2007).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[5] J. Oppenheim and B. Reznik, Phys. Rev. A **70**, 022312 (2004); S. Mozes, J. Oppenheim, and B. Reznik, Phys. Rev. A **71**, 012311 (2005).
[6] A. Chefles, Phys. Rev. A **64**, 062305 (2001); K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, and F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007).
[7] A. Chefles and M. Sasaki, Phys. Rev. A **67**, 032112 (2003); A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley, J. Phys. A **40**, 10 183 (2007); M. F. Sacchi, Phys. Rev. A **71**, 062340 (2005); G. M. Wang and M. S. Ying, Phys. Rev. A **73**, 042301 (2006); Z. F. Ji, Y. Feng, R. Y. Duan, and M. S. Ying, Phys. Rev. Lett. **96**, 200401 (2006).
[8] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301(R) (2000); B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001); G. Vidal, K. Hammerer, and J. I. Cirac, Phys. Rev. Lett. **88**, 237902 (2002); M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines, Phys. Rev. A **67**, 052301 (2003).
[9] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[10] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis* (Combridge University Press, Cambridge, England, 1991).
[11] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997).