Unitary Transformations Can Be Distinguished Locally

Xiang-Fa Zhou,* Yong-Sheng Zhang,† and Guang-Can Guo

Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China

(Received 11 April 2007; published 23 October 2007)

We show that, in principle, N-partite unitary transformations can be perfectly discriminated under local operations and classical communication despite their nonlocal properties. Based on this result, some related topics, including the construction of the appropriate quantum circuit together with the extension to general completely positive trace preserving operations, are discussed.

DOI: 10.1103/PhysRevLett.99.170401 PACS numbers: 03.65.Ud, 03.67.Mn

Superposition plays the central role in quantum mechanics, and puts many constraints on physically accessible transformations on quantum states. For instance, it is well-known that two pure states cannot be perfectly discriminated unless they are orthogonal [1]. Quantum states discrimination is an interesting problem in quantum information science, and has been extensively studied. However, things become very different when we refer to quantum operations. It was proved [2,3] that two nonorthogonal unitary operations U and V can be perfectly discriminated if we can run the selected unitary gate a finite number (k) of times in parallel and prepare a suitable input state $|\phi\rangle$ ($\langle\phi|(U^\dagger V)^{\otimes k}|\phi\rangle = 0$). This result is surprising and nontrivial, since for quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$, if $\langle\psi_1|\psi_2\rangle \neq 0$, then $|\psi_1\rangle^{\otimes k}$ and $|\psi_2\rangle^{\otimes k}$ cannot be told apart unless $k \to \infty$. Therefore, studying the distinguishability of quantum operations is an interesting problem.

In the original work of Refs. [2,3], the input state $|\phi\rangle$ is usually an entangled state. This becomes very common when the considered unitary transformations U and V act on many particles. Although quantum entanglement has been widely studied and viewed as a significant resource for quantum information processing, how to prepare multipartite entangled states efficiently in a typical experimental setup remains a great challenge to current technology. For example, in atomic system, spontaneous emission can destroy quantum correlation, and usually the disentanglement rate is the sum of the decay rate of individual atoms [4]. In the linear optical regime, experimental preparation of multiqubit entangled states is still a difficult and active area [5]. Therefore, one natural problem arises-whether it is possible to identify two different unitary operations only with local methods.

In this work, we consider to discriminate two multipartite unitary transformations under local operations and classical communications (LOCC). Compared with its counterpart, i.e., local identification of quantum states, which is often considered for orthogonal states [6,7], we find that any two unitary transformations can be perfectly identified locally despite their nonlocal properties.

Let us make a few remarks about the differences between the discrimination of quantum states and that of quantum operations. Generally to identify a quantum state, one should make a measurement on the given state followed by an estimation. Such a process usually destroy the input states which thus cannot be used any more. However, things become different when we refer to quantum operations. The reason lies in the fact that quantum operations never collapse, and in principle it can be repeated any number of times as needed. What's more, when unitary operations are considered, by exchanging the input and output ports of the whole setup we can obtain the reverse transformations. Actually, these facts make the discrimination of quantum operations very different from that of quantum states.

Generally the operation identification strategy can be formulated as this: we employ a quantum circuit $f(U)$ which is made up of the selected operation U (or V) on a suitable input state $\rho_{s,a}$, where $s(a)$ denotes the circuit system (auxiliary system). If only local methods are required, $\rho_{s,a}$ must also be separable. To obtain the maximal distinguishability, the overlap of the output states should be as small as possible for different quantum operations. Figure 1 shows the sketch of the identification process under LOCC. To simplify our consideration, in the following we mainly focus on bipartite system.

Let us begin with some simple observations. Here we mainly concentrate on unitary operations; one can check

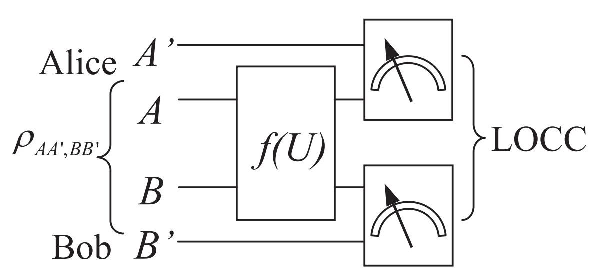

FIG. 1. Illustration of the identification of unitary transformations under local operations and classical communication. Alice and Bob input a locally implemented state $\rho_{AA',BB'}$ to a quantum circuit $f(U)$. After some local measurement operations on the output, the results are transmitted through classical channels to implement a perfect discrimination process.

that some of the discussions are also suitable for general quantum operations. As mentioned above, to realize perfect identification operation, one needs to find a suitable input state such that the corresponding output states are orthogonal to each other for different selected operations. Assume that we want to discriminate two unitary operations U and V. By inputting a locally implemented quantum state $\rho_{AA',BB'} = \sum_i \lambda_i \rho^i_{AA'} \otimes \rho^i_{BB'}$, we conclude that the two output states $\rho_U = (U \otimes I_{A'B'})\rho_{AA',BB'}(U^\dagger \otimes I_{A'B'})$ and $\rho_V = (V \otimes I_{A'B'})\rho_{AA',BB'}(V^\dagger \otimes I_{A'B'})$ should be orthogonal to each other. Now consider the spectral decompositions of $\rho^i_{AA'} = \sum_j r_j |r^i_j\rangle_{(AA')}\langle r^i_j|$ and $\rho^i_{BB'} = \sum_k s_k |s^i_k\rangle_{(BB')}\langle s^i_k|$. The requirement of $\rho_U \perp \rho_v$ is equivalent to $(U \otimes I_{A'B'})|r^i_j\rangle_{AA'}|s^i_k\rangle_{BB'} \perp (V \otimes I_{A'B'})|r^{i'}_{j'}\rangle_{AA'}|s^{i'}_{k'}\rangle_{BB'}$ for any i, i', j, j', k, k'. This observation shows that, in general, a pure input state $|r\rangle_{AA'}|s\rangle_{BB'}$ is enough to discriminate two unitary operations. Moreover, since two orthogonal pure states can be locally identified [6,7], in this case U and V can also be discriminated with local methods.

The above discussion shows that, to distinguish two unitary operation locally, one should find a suitable separable state as the input. Before concentrating on the specific topics, let us consider several simple examples.

Suppose two unitary transformations U_{AB} and V_{AB} with zero overlap, i.e., $\mathrm{Tr}(V^\dagger_{AB} U_{AB}) = 0$. Then by preparing the following input state

$$|\phi\rangle_{AB,A'B'} = |\phi\rangle_{AA'} \otimes |\phi\rangle_{BB'}, \tag{1}$$

where $|\phi\rangle_{AA'} = \sum_i |i\rangle_A |i'\rangle_{A'}$ (or $|\phi\rangle_{BB'} = \sum_i |i\rangle_B |i'\rangle_{B'}$) is a non-normalized entangled state between the system A and the corresponding local environment A' (or B and B'). Since

$$\langle\phi|V^\dagger_{AB} U_{AB} \otimes I|\phi\rangle = \mathrm{Tr}(V^\dagger_{AB} U_{AB}) = 0, \tag{2}$$

one immediately obtains that the two output states $U_{AB} \otimes I|\phi\rangle_{AB,A'B'}$ and $V_{AB} \otimes I|\phi\rangle_{AB,A'B'}$ are orthogonal, and hence can be locally discriminated perfectly. Equations (1) and (2) can be viewed as the extension of Jamiolkowski isomorphism in the local case [8]. The input state $|\phi\rangle_{AB,A'B'}$ is universal for any two operations U and V satisfying $\mathrm{Tr}(V^\dagger U) = 0$.

In the above case, a perfect identification is possible after a single run. Generally one needs to run the selected gate k times (k is finite). In the global case, the optimal k has been presented in Refs. [2,3], which asserts that if the minimal arclength δ spread by the eigenvalue of $(U^\dagger V)^{\otimes k}$ in the circle $|z| = 1$ is not less than π, then a perfect discrimination scheme is allowed. Now assume $U^\dagger V = U_1 \otimes U_2$, and δ_1, δ_2 are the minimal arclengths of $U_1^{\otimes k}$ and $U_2^{\otimes k}$, respectively. If only local input states (e.g., $|r\rangle|s\rangle$) are allowed, since

$$\langle r|U_1^{\otimes k}|r\rangle\langle s|U_2^{\otimes k}|s\rangle = 0 \Leftrightarrow \langle r|U_1^{\otimes k}|r\rangle = 0 \quad \text{or } \langle s|U_2^{\otimes k}|s\rangle = 0, \tag{3}$$

to distinguish U and V locally, at least one of the two arclength δ_1 and δ_2 must be not less than π. Therefore, generally in the local case the optimal running times k of the selected operation should be greater than that of the global case (in the global case, we have $\delta_1 + \delta_2 \geq \pi$).

More generally, suppose $U^\dagger V = (U_1 \otimes U_2) \times (P_1 \otimes I + P_2 \otimes u)$ with $P_i P_j = \delta_{ij} P_i$ and $\sum_i P_i = I$. If $U_2 \neq u^\dagger$, then by inputting an appropriate state $|\psi\rangle_A|\psi\rangle_B$ with $|\psi\rangle_A$ lying in the support of P_1, $U^\dagger V$ is equivalent to the local transformation $(uU_2)|\psi\rangle_B$, and hence the two unitaries can be perfectly identified. Especially when $U_1 = U_2 = I$, one can find that the eigenvalues of $(U^\dagger V)^{\otimes k}$ belong to the set $\{1, b_1, b_2, \ldots\}$ with b_i and $|b_i\rangle$ being the eigenvalues and eigenvectors of $u^{\otimes k}$ separately. If only local input state $\rho_A \otimes \rho_B = \mathrm{Tr}(|\psi_{AA'}\rangle\langle\psi_{AA'}| \otimes |\psi_{BB'}\rangle \times \langle\psi_{BB'}|)$ is permitted, then

$$\mathrm{Tr}[(U^\dagger V)^{\otimes k}(\rho_A \otimes \rho_B)] = x + (1 - x)\sum_i b_i \langle b_i|\rho_B|b_i\rangle, \tag{4}$$

where $x = \mathrm{Tr}(P_1 \rho_A) \geq 0$ can be chosen arbitrarily by inputting appropriate ρ_A. In order to make the right-hand side of Eq. (4) to be zero, one can easily obtain that the minimal angular spread of $\{1, b_1, b_2, \ldots\}$ should be not less than π. Therefore, in this case the minimal k required equals to that of the global case.

In the above discussions, we have considered discriminating several special kinds of unitary transformations. They all can be perfectly identified and the corresponding quantum circuits and input states can be easily obtained. In the following, we mainly focus on the most general case. Although we cannot present the optimal quantum circuits and input states, we prove that, in principle, any two unitary operations U and V can be perfectly identified locally.

Following Refs. [9,10], we call a two-qudit gate U_{AB} to be primitive if U_{AB} maps a separable state to another separable state; otherwise, U_{AB} is imprimitive. Generally, a primitive gate U_{AB} can be expressed as the product of one-qudit gate up to a swap operation P, namely, $U_{AB} = U_A \otimes U_B$ or $U_{AB} = U_A \otimes U_B P$ with $P|\alpha\rangle_A|\beta\rangle_B = |\beta\rangle_A|\alpha\rangle_B$. For simplicity, in the following, we use H to denote the set of all two-qudit gates of the form $U_A \otimes U_B$. Under these assumptions, we then introduce the following lemma.

Lemma 1.—H together with an imprimitive gate U can generate the unitary group $U(d^2)$, where d is the dimension of the qudit Hilbert space.

A detailed proof of this lemma can be found in Ref. [10], which is used to study the university of quantum gates. This lemma indicates that if U and all local unitary transformations are permitted, we can then construct $H' = UHU^{-1}$. By choosing a suitable sequence of H and H', we can obtain any desired elements in $U(d^2)$. The sequence is finite; therefore, we only need to run the imprimitive gate a finite number of times.

Based on this lemma, we now prove the main theorem of this work.

Theorem 1.—Any two unitary transformation U_{AB} and V_{AB} can be perfectly identified with local methods.

Proof.—Following our former discussions, we obtain that if both U_{AB} and V_{AB} are primitive, then they can be perfectly discriminated locally.

Now assume that only one of the two unitary gates is primitive. Without loss of generality, we suppose V_{AB} to be imprimitive. According to the lemma, we obtain that there exists a quantum circuit $f(V_{AB})$ made up of the elements in H and $H' = V_{AB}HV_{AB}^{\dagger}$ such that $f(V_{AB}) \in (HH')^n$ is some control-unitary transformation. On the other hand, since U_{AB} is primitive, which means $H' = U_{AB}HU_{AB}^{\dagger} = H$, one immediately obtains that $f(U_{AB})$ is also primitive. Because $f(U_{AB}) \neq f(V_{AB})$, it follows that the two unitary operations can be locally identified.

If U_{AB} and V_{AB} are both imprimitive, following the lemma, we obtain that there is a quantum circuit such that $f(U_{AB}) = e^{iL_{12}^A \otimes L_{12}^B}$ with $(L_{12}^A)_{ij} = \delta_{i1}\delta_{j2} + \delta_{i2}\delta_{j1}$ [or $(L_{12}^B)_{ij}$]. If $f(V_{AB})$ is primitive, then perfect local discrimination can be realized. Otherwise, both $f(U_{AB})$ and $f(V_{AB})$ are imprimitive. Since $f(U_{AB})^{\dagger} = Af(U_{AB})A^{\dagger}$ with $A = \mathrm{diag}\{\sigma_z, I_{(d-2)}\} \otimes I$, $I \otimes \mathrm{diag}\{\sigma_z, I_{(d-2)}\}$, $\mathrm{diag}\{\sigma_y, I_{(d-2)}\} \otimes I$, or $I \otimes \mathrm{diag}\{\sigma_y, I_{(d-2)}\}$ [$I_{(d-2)}$ is the identity operation in the $(d-2)$-dimensional Hilbert space], one can easily check that if the similar result can be obtained for V_{AB}, then $f(V_{AB})$ can be expressed as $f(V_{AB}) = e^{ixL_{12}^A \otimes L_{12}^B}$ for some $x \in \mathbb{R}$. Therefore the whole question can be divided into the following two parts:

(i) If $f(V_{AB}) \neq e^{ixL_{12}^A \otimes L_{12}^B}$ for any $x \in \mathbb{R}$, then by employing the transformation $Af(\cdot)A^{\dagger}f(\cdot)$, we can obtain an identity operation for U_{AB}. Because $Af(V_{AB})A^{\dagger}f(V_{AB}) \neq I$, the two operations thus are locally distinguishable.

(ii) If $f(V_{AB}) = e^{ixL_{12}^A \otimes L_{12}^B}$, then when $x \neq 1$, $f(U_{AB})$ and $f(V_{AB})$ can be reduced to $e^{iL_{12}^A} \otimes I$ and $e^{ixL_{12}^A} \otimes I$ by inputting a product state $|\phi\rangle|\psi\rangle$ with $|\psi\rangle$ being an eigenvector of L_{12}^B, which, therefore, can be perfectly identified locally by running the circuit a finite number of times in parallel. Otherwise we have $f(U_{AB}) = f(V_{AB})$. Since $e^{iL_{12}^A \otimes L_{12}^B}$ is imprimitive, it can be used to construct the desired operator $U_{AB}^{\dagger}$. Thus the original problem is reduced to the local identification of I and $U_{AB}^{\dagger}V_{AB}$, which can be implemented perfectly.

This completes the proof.

The above theorem shows that, in principle, to realize a perfect local identification we only need to run the selected unitary operation a finite number of times. Although we have assumed that the two subsystems A and B have equal dimensions, one can easily obtain that the same result holds even when A and B have different dimensions. For example, if $\dim \mathcal{H}_A < \dim \mathcal{H}_B$, then by introducing another subsystem A_1 in Alice's side such that $\dim \mathcal{H}_A + \dim \mathcal{H}_{A_1} = \dim \mathcal{H}_B$, we can obtain two extended unitary transformations $U \oplus I_{A_1}$ and $V \oplus I_{A_1}$, which thus can be identified with the methods described above [11].

From the practical viewpoint, it will be valuable if one can provide an optimal circuit to implement such kinds of identification operations [12]. Generally, it is not easy to do this. Here, to simplify our consideration, we take two-qubit gates as an example.

For any two-qubit unitary transformation U, it has the following canonical decomposition [13]:

$$U = (U_1 \otimes U_2)e^{i(h_x\sigma_x\otimes\sigma_x + h_y\sigma_y\otimes\sigma_y + h_z\sigma_z\otimes\sigma_z)}(U_3 \otimes U_4), \quad (5)$$

where σ_x, σ_y, σ_z are the usual Pauli matrices, U_i are local single-qubit gates, and $\pi/4 \geq h_x \geq h_y \geq |h_z|$. Benefitting from the nice decomposition (5), one need not to reverse the whole setup because $U^{\dagger}$ can be constructed from U directly. Now suppose we have two unitary operations U and V. After applying the selected gate at most two times, we can transform one of them, e.g., U, into $f(U) = e^{ih_x^U\sigma_x\otimes\sigma_x}$. If $f(V) \neq e^{ih_x^V\sigma_x\otimes\sigma_x}$ for some $h_x^V \in \mathbb{R}$, we can employ the manipulation $g(\cdot) = Af(\cdot)A^{\dagger}f(\cdot)$ ($A = \sigma_y \otimes I$, $\sigma_z \otimes I$, $I \otimes \sigma_y$, or $I \otimes \sigma_z$) to reduce the original U and V to I and $g(V)$, respectively. Similarly, by running $g(V)$ at most four times, we can then obtain two local unitary transformations U' and V'. One can easily check that by choosing suitable single-qubit gates, U' and V' can always be different. Therefore, after repeating the selected gate at most 20 times, we obtain two local gates, which can be perfectly implemented with the methods described above.

The same question can also be investigated in the multipartite case. To answer this problem, we should introduce the generalized version of the primitive gates (see Ref. [14] for technique details). We call $U_{12\ldots N}$ $\{[i_s, \ldots, i_e], \ldots, [j_s, \ldots, j_e], \ldots\}$-primitive if $U_{12\ldots N}$ together with all single-qudit gates can generate the group $\mathcal{U}_\beta = U_{i_s\ldots i_e} \otimes \ldots \otimes U_{j_s\ldots j_e}$. Similarly, if $\mathcal{U}_\beta = U(d^N)$, then $U_{12\ldots N}$ is imprimitive. Following the same routine as in Ref. [10], we can obtain that a $\{[i_s, \ldots, i_e], \ldots, [j_s, \ldots, j_e], \ldots\}$-primitive gate can be expressed as $U_{i_s\ldots i_e} \otimes \ldots \otimes U_{j_s\ldots j_e} P_{\{[i_s,\ldots,i_e],\ldots,[j_s,\ldots,j_e],\ldots\}}$, where $P_{\{[i_s,\ldots,i_e],\ldots,[j_s,\ldots,j_e],\ldots\}}$ is a permutation operator which preserves the structure of the partition $\{[i_s, \ldots, i_e], \ldots, [j_s, \ldots, j_e], \ldots\}$. For example, if $U_{12\,345}$ is $\{[1,2],[3,4],5\}$-primitive, then $P_{\{[1,2],[3,4],5\}} = P_{12,34} \otimes I_5$ or $I_{12\,345}$, where $P_{12,34}$ is the swap operation between Hilbert spaces $\mathcal{H}_1 \otimes \mathcal{H}_2$ and $\mathcal{H}_3 \otimes \mathcal{H}_4$; if $U_{12\,345}$ is $\{1,2,3,4,5\}$-primitive, then $P_{\{1,2,3,4,5\}}$ can be any element in the permutation group S_5.

We take three-partite unitary transformations as an instance. According to the above discussion, if one of the two three-partite unitary transformations U_{ABC} and V_{ABC} is $\{A, B, C\}$-primitive, then a perfect local identification is possible. If both of the two selected transformations are imprimitive, then there exists a sequence $f(U_{ABC}) = (H'H)\ldots(H'H)$ with $H' = U_{ABC}HU_{ABC}^{\dagger}$, such that $f(U) = e^{iL_{12}^{A}\otimes L_{12}^{B}\otimes L_{12}^{C}}$. Following the discussion of bipartite case, we conclude that U_{ABC} and V_{ABC} can be locally discriminated. Finally, if U_{ABC} is $\{[A, B], C\}$-primitive with V_{ABC} being $\{A, [B, C]\}$-primitive, then there exists a circuit such that $f(U_{ABC}) = (U_{A_1} \otimes P_{B_1} + U_{A_2} \otimes P_{B_2}) \otimes U_C$ and $f(V_{ABC}) = V_A \otimes V_{BC}$, where $(U_{A_1} \otimes P_{B_1} + U_{A_2} \otimes P_{B_2})$ is a control-unitary transformation. Since $U_{A_1} \neq V_A$ or $U_{A_2} \neq V_A$, by choosing suitable input state, the original problem can be reduced to the discrimination of two different local unitary manipulations, and hence can be implemented perfectly.

The above discussion can be extended to N-partite case, and we have that it is always possible to discriminate two unitary operations locally, although in general we need to run the selected operation many times. Interestingly, unlike the previous results for quantum states, where "the hidden entanglement" plays a very important role, it seems that the nonlocality of unitary transformations does not affect the distinguishability much (in this work, it only changes the total run times k). We can also generalize this result to the case of M unitary transformations. To discriminate the selected operation from others, we should perform $M - 1$ tests; after each test, one of the M operations can be ruled out. Therefore a perfect local identification is possible after a finite number of runs.

One can also consider the same problem for nonunitary transformations [15]. For general completely positive trace preserving operations ξ_1 and ξ_2, the reverse transformations do not always exist unless they are unitary. Moreover, the output states usually are mixed even if we employ a pure input state, and ξ_1, ξ_2 may contain common Kraus operators. To realize a perfect identification process, these components should be ruled out. Totally solving this problem seems to be quite complicated.

To summarize, we have shown that multipartite unitary transformations can also be discriminated perfectly with local methods. Nonlocal schemes together with entangled input states usually can improve the efficiency of the identification process; i.e., we can run the selected operations fewer times. However, it does not affect the distinguishability of the whole problem. In principle, by running the secretly chosen operations a finite number of times, we can also discriminate them perfectly under LOCC. From the practical viewpoint, one need to provide an optimal method to implement the discrimination procedure. Our investigation indicates that this question has a close relation to the exact universality of unitary evolution and the optimal quantum circuits in d-level systems [16].

The authors thank R. Duan for helpful comments and suggestions and drawing our attention to the closely related works [17]. This work was funded by the National Fundamental Research Program (No. 2006CB921900), the National Natural Science Foundation of China (Grant No. 10674127), the Innovation Funds from the Chinese Academy of Sciences, and Program for New Century Excellent Talents in University.

*xfzhou@mail.ustc.edu.cn
†yshzhang@ustc.edu.cn

[1] C. W. Helstron, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[2] A. Acín, Phys. Rev. Lett. **87**, 177901 (2001).
[3] G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).
[4] T. Yu and J. H. Eberly, Phys. Rev. B **66**, 193306 (2002).
[5] C.-Y. Lu *et al.*, Nature Phys. **3**, 91 (2007).
[6] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[7] C. H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).
[8] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972); J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[9] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995); T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995); A. Barenco, Proc. R. Soc. A **449**, 679 (1995); S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995); D. Deutsch *et al.*, Proc. R. Soc. A **449**, 669 (1995); A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995); G. Vidal and C. M. Dawson, Phys. Rev. A **69**, 010301(R) (2004).
[10] J.-L. Brylinski and R. Brylinski, *Mathematics of Quantum Computation*, edited by R. Brylinski and G. Chen (CRC Press, Boca Raton, 2002) or see arXiv:quant-ph/0108062.
[11] R. Duan (private communication). Lemma 1 is also tenable when the two subsystem A and B have different dimensions. In this case, the swap operation P doesnot exist.
[12] M. J. Bremner *et al.*, Phys. Rev. Lett. **89**, 247902 (2002).
[13] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001); B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[14] X.-F. Zhou, Y.-S. Zhang, and G.-C. Guo, arXiv:0705.1814v3.
[15] A. Chefles, Phys. Rev. A **72**, 042332 (2005); G. M. D'Ariano, M. F. Sacchi, and J. Kahn, Phys. Rev. A **72**, 052302 (2005); G. M. D'Ariano, P. Mataloni, and M. F. Sacchi, Phys. Rev. A **71**, 062337 (2005); Z. Ji, Y. Feng, R. Duan, and M. Ying, Phys. Rev. Lett. **96**, 200401 (2006).
[16] A. Muthukrishnan and C. R. Stroud Jr., Phys. Rev. A **62**, 052309 (2000); J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004); S. S. Bullock, D. P. OLeary, and G. K. Brennen, Phys. Rev. Lett. **94**, 230502 (2005); M. A. Nielsen, M. R. Dowling, M. Gu, and A. C. Doherty, Science **311**, 1133 (2006).
[17] R. Duan, Y. Feng, and M. Ying, Phys. Rev. Lett. **98**, 100503 (2007); R. Duan, Y. Feng, and M. Ying, arXiv:0705.1424.