PHYSICAL REVIEW A **73**, 042301 (2006)

Unambiguous discrimination among quantum operations

Guoming Wang* and Mingsheng Ying†
State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084
(Received 19 December 2005; published 3 April 2006)

We address the problem of unambiguous discrimination among a given set of quantum operations. The necessary and sufficient condition for them to be unambiguously distinguishable is derived in the cases of single use and multiple uses, respectively. For the latter case we explicitly construct the input states and corresponding measurements that accomplish the task. It is also found that the introduction of entanglement can improve the discrimination.

DOI: 10.1103/PhysRevA.73.042301 PACS number(s): 03.67.Hk, 03.67.Mn

The study of open quantum systems is an important subject in the fields of quantum control and quantum-information theory. Such systems can be generally described in the quantum operations formalism. Specifically, the behavior of an open system can be represented by a linear, completely positive, trace-preserving map $\mathcal{E}$, which is written in the Kraus operator-sum form [1]

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{1}$$

where E_k are linear operators and satisfy the completeness condition $\Sigma_k E_k^\dagger E_k = I$ in order to preserve the trace of ρ.

Now the following problem naturally arises: if we are given a quantum mechanical black box that performs one of the operations $\mathcal{E}_1, \ldots, \mathcal{E}_n$, how can we identify which one it really performs? A natural idea is to input a probe state to the black box and then distinguish between the possible outputs. Moreover, if the black box can be accessed multiple times, we can repeat the procedure and collectively discriminate the output states of multiple uses.

Since this method relies on the discrimination of output states, it is necessary to review the results about quantum state discrimination at first. It is well known that a set of quantum states can be perfectly distinguished if and only if they are orthogonal to each other. How to distinguish a set of nonorthogonal quantum states in an optimal way according to some criterion has become an important problem and received a lot of attention in the past years [2]. Two strategies are widely used for this task. One is called minimum-error discrimination, which allows mistakes but minimizes the probability of giving an erroneous result. The other one, named unambiguous discrimination [3–21], may fail for a nonzero probability, but when it succeeds the result is absolutely right. To be specific, in the task of unambiguous discrimination among $\rho_1, \ldots, \rho_n$, we need to construct a positive-operator valued measure (POVM) comprising $n+1$ elements $\Pi_0, \Pi_1, \ldots, \Pi_n$ such that the measurement outcome i correctly indicates ρ_i for any $i=1, \ldots, n$ and the outcome 0 leads to no conclusion. Unambiguous discrimination cannot be applied to an arbitrary set of states. It is proved [14] that the states $\rho_1, \ldots, \rho_n$ can be unambiguously discriminated if and only if for any $i=1, \ldots, n$, $\text{supp}(\{\rho_1, \ldots, \rho_n\}) \neq \text{supp}(\{\rho_j : j \neq i\})$, or equivalently, $\text{supp}(\rho_i) \nsubseteq \text{supp}(\{\rho_j : j \neq i\})$, where $\text{supp}(\rho_i)$ is the support of ρ_i, and the support of a set of density operators is defined to be the sum of each one's support [22].

The two strategies above can both be extended to the case of quantum operations. However, neither of them is well studied so far. Most previous work was directed to the special cases of unitary operations [23–25] and Pauli channels [26,27]. Some measures were also defined to quantify the distinguishability of general quantum operations [28–30]. Only recently the problem of minimum-error discrimination between two general quantum operations was addressed by Sacchi [31].

In this paper we consider the problem of unambiguous discrimination among a given set of quantum operations. The necessary and sufficient condition for them to be unambiguously distinguishable is derived in the cases of single use and multiple uses, respectively. For the latter case we explicitly give a strategy. It is also found that the introduction of entanglement can improve the discrimination.

We first consider the simple case when the black box can be accessed only once. The problem can be formulated as follows: if the possible quantum operations are $\mathcal{E}_1, \ldots, \mathcal{E}_n$, can we find a state ρ in the input Hilbert space $\mathcal{H}$ such that $\mathcal{E}_1(\rho), \ldots, \mathcal{E}_n(\rho)$ are unambiguously distinguishable? More generally, we can introduce an ancilla and make the main system and ancilla entangled to improve our discrimination. Denoting the ancillary Hilbert space by $\mathcal{H}_a$, our task is to find a state ρ in the composite space $\mathcal{H} \otimes \mathcal{H}_a$ such that $(\mathcal{E}_1 \otimes \mathcal{I})(\rho), \ldots, (\mathcal{E}_n \otimes \mathcal{I})(\rho)$ can be unambiguously discriminated, where $\mathcal{I}$ is the identity operator acting on the space $\mathcal{H}_a$. If such ancillary space and input state exist, we say that $\mathcal{E}_1, \ldots, \mathcal{E}_n$ are unambiguously distinguishable by a single use.

Since any mixed input state can be purified by appending a reference system which can be viewed as a part of the ancilla, we just need to consider pure input states. Furthermore we know from Schmidt decomposition that any ancillary space has a subspace of dimension at most $\dim(\mathcal{H})$ that really matters in the discrimination. Thus, in the following

*Electronic address: wgm00@mails.tsinghua.edu.cn
†Electronic address: yingmsh@tsinghua.edu.cn

we only need to consider the pure states of the composite space $\mathcal{H}\otimes\mathcal{H}_a$ where $\dim(\mathcal{H}_a)=\dim(\mathcal{H})$.

Now we define the support of a quantum operation $\mathcal{E}$, denoted by $\mathrm{supp}(\mathcal{E})$, to be the span of its Kraus operators $\{E_k\}$, i.e.,

$$\mathrm{supp}(\mathcal{E}) \equiv \mathrm{span}\{E_k\} \equiv \left\{\sum_k \lambda_k E_k : \lambda_k \in \mathbb{C}\right\}. \tag{2}$$

It is proved that every two sets of Kraus operators describing the same quantum operation $\mathcal{E}$ can be related to each other by a unitary transformation [32]. This fact indicates that our concept $\mathrm{supp}(\mathcal{E})$ is independent of the specific choice of Kraus operators so it is well defined.

Furthermore, we define support of a set of quantum operations $\{\mathcal{E}_1,\ldots,\mathcal{E}_n\}$, denoted by $\mathrm{supp}(\{\mathcal{E}_1,\ldots,\mathcal{E}_n\})$, to be the sum of every operation's support, i.e.,

$$\mathrm{supp}(\{\mathcal{E}_1,\ldots,\mathcal{E}_n\}) \equiv \sum_{k=1}^{n} \mathrm{supp}(\mathcal{E}_k). \tag{3}$$

It is found out that the above concept of support of quantum operations plays a very similar role like the support of quantum states in determining the possibility of unambiguous discrimination, as the following theorem indicates:

Theorem 1. The quantum operations $\mathcal{E}_1,\ldots,\mathcal{E}_n$ can be unambiguously discriminated by a single use if and only if for any $i=1,\ldots,n$, $\mathrm{supp}(\mathcal{E}_i)\nsubseteq\mathrm{supp}(S_i)$, where $S_i=\{\mathcal{E}_j : j\neq i\}$.

Proof. Suppose $\mathcal{E}_i$ has Kraus operators $\{E_i^k : k=1,..,n_i\}$. If the operation $\mathcal{E}_i\otimes\mathcal{I}$ acts on the input $|\psi\rangle\in\mathcal{H}\otimes\mathcal{H}_a$, the corresponding output is

$$(\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|) = \sum_{k=1}^{n_i}(E_i^k\otimes I)|\psi\rangle\langle\psi|(E_i^k\otimes I)^\dagger. \tag{4}$$

It follows that its support is given by

$$\mathrm{supp}((\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|)) = \mathrm{span}\{(E_i^k\otimes I)|\psi\rangle : k=1,\ldots,n_i\}. \tag{5}$$

If there exists an operation $\mathcal{E}_i$ satisfying $\mathrm{supp}(\mathcal{E}_i)\subseteq\mathrm{supp}(S_i)$, then we have that each E_i^k can be written as the linear combination of the operators $\{E_j^l : j\neq i\}$. So for any input state $|\psi\rangle$, $(E_i^k\otimes I)|\psi\rangle$ can also be written as the linear combination of $\{(E_j^l\otimes I)|\psi\rangle : j\neq i\}$. By Eq. (5), this indicates

$$\mathrm{supp}\ (\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|)) \subseteq \mathrm{supp}(\{(\mathcal{E}_j\otimes\mathcal{I})(|\psi\rangle\langle\psi|) : j\neq i\}). \tag{6}$$

So it is impossible to unambiguously distinguish the output $(\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|))$ from other possible outputs $(\mathcal{E}_j\otimes\mathcal{I})(|\psi\rangle\langle\psi|)(j\neq i)$. Therefore, we cannot unambiguously distinguish the operation $\mathcal{E}_i$ from the others.

The proof of the converse needs a constructive method. Now we assume that the $\mathcal{E}_1,\ldots,\mathcal{E}_n$ fulfill the given condition. Let $|\psi\rangle$ be arbitrary pure state with full Schmidt number, i.e.,

$$|\psi\rangle = \sum_{t=1}^{d}\alpha_t|t\rangle|t_a\rangle, \tag{7}$$

where $\alpha_t>0$, $t=1,\ldots,d$, $\{|t\rangle : t=1,\ldots,d\}$ and $\{|t_a\rangle : t=1,\ldots,d\}$ are orthonormal bases for $\mathcal{H}$ and $\mathcal{H}_a$, respectively. We now prove that the set of output states $\{(\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|) : i=1,\ldots,n\}$ are unambiguously distinguishable. Otherwise, there exists one operation $\mathcal{E}_i$ satisfying

$$\mathrm{supp}((\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|)) \subseteq \mathrm{supp}(\{(\mathcal{E}_j\otimes\mathcal{I})(|\psi\rangle\langle\psi|) : j\neq i\}), \tag{8}$$

hence, by Eq. (5) we know that there exist coefficients $\{\lambda_{jl}^k\}$ such that for any

$$(E_i^k\otimes I)|\psi\rangle = \sum_{j\neq i,l=1,\ldots,n_j}\lambda_{jl}^k(E_j^l\otimes I)|\psi\rangle. \tag{9}$$

Taking Eq. (7) into Eq. (9), we have

$$\sum_{t=1}^{d}\alpha_t E_i^k|t\rangle|t_a\rangle = \sum_{t=1}^{d}\alpha_t\sum_{j\neq i,l=1,\ldots,n_j}\lambda_{jl}^k E_j^l|t\rangle|t_a\rangle. \tag{10}$$

Since $\{|t_a\rangle\}$ are orthogonal to each other and $\alpha_t>0$, we have that for any $|t\rangle$,

$$E_i^k|t\rangle = \sum_{j\neq i,l=1,\ldots,n_j}\lambda_{jl}^k E_j^l|t\rangle, \tag{11}$$

which implies that

$$E_i^k = \sum_{j\neq i,l=1,\ldots,n_j}\lambda_{jl}^k E_j^l. \tag{12}$$

So we obtain $\mathrm{supp}(\mathcal{E}_i)\subseteq\mathrm{supp}(S_i)$, which contradicts the assumption. ■

It should be noted that from the proof above, any entangled pure state with full Schmidt number can be used as input to universally distinguish arbitrary set of quantum operations that fulfill the condition in theorem 1.

A corollary of theorem 1 is that two quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$ can be unambiguously discriminated by a single use if and only if $\mathrm{supp}(\mathcal{E}_1)\nsubseteq\mathrm{supp}(\mathcal{E}_2)$ and $\mathrm{supp}(\mathcal{E}_2)\nsubseteq\mathrm{supp}(\mathcal{E}_1)$.

For the case in which we are not allowed to introduce any ancillary system, a similar argument shows that the condition presented in theorem 1 is still necessary. But in general it is not sufficient. Let us consider the following example. Suppose we are going to discriminate two Pauli channels, the bit-flip channel and the phase-flip channel, whose Kraus operators are $\{\sqrt{p}I,\sqrt{1-p}X\}$ and $\{\sqrt{q}I,\sqrt{1-q}Z\}$, respectively, i.e.,

$$\mathcal{E}_1(\rho) = p\rho + (1-p)X\rho X, \tag{13}$$

$$\mathcal{E}_2(\rho) = q\rho + (1-q)Z\rho Z. \tag{14}$$

It is impossible to unambiguously distinguish these two channels without use of ancilla. To see this, we notice that two qubit states can be unambiguously discriminated only if they are both pure. However, the inputs that make the output of the bit-flip channel pure are $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ but for the phase-flip channel such inputs are $\{|0\rangle,|1\rangle\}$. So for any input state $|\psi\rangle$, the outputs $\mathcal{E}_1(|\psi\rangle\langle\psi|)$ and $\mathcal{E}_2(|\psi\rangle\langle\psi|)$ cannot both be pure and thus they are not unambiguously distinguishable. On the other hand, from theorem 1 it is easy to see that when using ancillary systems these two channels can be unambiguously discriminated by a single use.

From the above example we see that the introduction of entanglement between the main system and ancilla not only increases the success probability but also in fact changes the possibility of unambiguous discrimination between quantum operations. It should be noted that for minimum-error discrimination the use of entangled input can also increase the efficiency [31].

Now we consider a more complicated case in which the black box can be accessed multiple times. We say that quantum operations $\mathcal{E}_1,\ldots,\mathcal{E}_n$ can be unambiguously discriminated by N uses if there exist an ancillary space $\mathcal{H}_a$ and a state ρ in the composite space $\mathcal{H}^{\otimes N}\otimes\mathcal{H}_a$ such that $(\mathcal{E}_1^{\otimes N}\otimes\mathcal{I})(\rho),\ldots,(\mathcal{E}_n^{\otimes N}\otimes\mathcal{I})(\rho)$ are unambiguously distinguishable, where $\mathcal{I}$ is the identity operators acting on $\mathcal{H}_a$. Still we only need to focus on the case of $\rho=|\psi\rangle\langle\psi|$ where $|\psi\rangle\in\mathcal{H}^{\otimes N}\otimes\mathcal{H}_a$ and $\dim(\mathcal{H}_a)=\dim(\mathcal{H}^{\otimes N})$.

One may think that when a repeated use of the black box is allowed, we can use quantum process tomography [33,34] to identify it. However, this method depends on the statistical data of measurement outcomes and thus requires considerable effort. Our method based on state discrimination accesses the black box a much smaller number of times, so it is more efficient.

Now it is necessary to review some results about unambiguous discrimination between quantum states with multiple copies because they play a central role in the proof of our following theorem. It is well known that a set of pure states can be unambiguously discriminated if and only if they are linearly independent. However, in Ref. [6] Chefles found that even linearly dependent pure states can be unambiguously discriminated if many sufficient copies of them are distinguished collectively. A bound on the number of copies needed was also obtained: for any n distinct pure states $|\psi_1\rangle,\ldots,|\psi_n\rangle$ in a d-dimensional space, $|\psi_1\rangle^{\otimes c},\ldots,|\psi_n\rangle^{\otimes c}$ can always be unambiguously discriminated if $c\geqslant n-d+1$. Here we find a similar result for mixed states.

Lemma 1. If the mixed quantum states $\rho_1,\ldots,\rho_n$ satisfy that for any $i\neq j$, $\mathrm{supp}(\rho_i)\nsubseteq\mathrm{supp}(\rho_j)$, then $\rho_1^{\otimes n},\ldots,\rho_n^{\otimes n}$ can be unambiguously discriminated. Otherwise, for arbitrary $N\geqslant 1$, $\rho_1^{\otimes N},\ldots,\rho_n^{\otimes N}$ are not unambiguously distinguishable.

Proof. If there exist two states ρ_i and ρ_j such that $\mathrm{supp}(\rho_i)\subseteq\mathrm{supp}(\rho_j)$, then we have that for any $N\geqslant 1$, $\mathrm{supp}(\rho_i^{\otimes N})\subseteq\mathrm{supp}(\rho_j^{\otimes N})$, so it is impossible to unambiguously distinguish between the state $\rho_i^{\otimes N}$ and $\rho_j^{\otimes N}$.

Now suppose that for any $i\neq j$, $\mathrm{supp}(\rho_i)\nsubseteq\mathrm{supp}(\rho_j)$. Then we know that for any $i\neq j$, $\mathrm{supp}(\rho_i)$ is not fully orthogonal to $\ker(\rho_j)$, where $\ker(\rho_j)$ is the kernel of ρ_j [35]. Denoting the projection operators onto $\mathrm{supp}(\rho_j)$ and $\ker(\rho_j)$ by P_j,Q_j, respectively, then we obtain

$$\mathrm{tr}(Q_j\rho_i)>0, \tag{15}$$

for any $i\neq j$.

If we have n copies of the unknown state, numbered from 1 to n, we perform the projective measurement $\{P_i,Q_i\}$ on the ith copy individually. Equivalently, a projective measurement consisting of all the projection operators $\{\Xi_1\otimes\Xi_2\ldots\otimes\Xi_n\}$ is performed on the n-fold copies, where for any $k=1,\cdots,n$, $\Xi_k=P_k$ or Q_k.

Consider the probability of getting the measurement outcome corresponding to $Q_1\otimes\ldots Q_{i-1}\otimes P_i\otimes Q_{i+1}\otimes\cdots\otimes Q_n$. If the unknown state is $\rho_i^{\otimes n}$, the probability is

$$\mathrm{tr}((Q_1\otimes\ \ldots Q_{i-1}\otimes P_i\otimes Q_{i+1}\otimes\ \cdots\ \otimes Q_n)\rho_i^{\otimes n}) \\ =\mathrm{tr}(P_i\rho_i)\prod_{j\neq i}\mathrm{tr}(Q_j\rho_i)>0, \tag{16}$$

where the last inequality is derived from Eq. (15) and $\mathrm{tr}(P_i\rho_i)=1$.

Otherwise, if the unknown state is $\rho_j^{\otimes n}$ for some $j\neq i$, the probability is

$$\mathrm{tr}((Q_1\otimes\ \ldots Q_{i-1}\otimes P_i\otimes Q_{i+1}\otimes\ \cdots\ \otimes Q_n)\rho_j^{\otimes n}) \\ =\mathrm{tr}(P_i\rho_j)\prod_{k\neq i}\mathrm{tr}(Q_k\rho_j)=0, \tag{17}$$

where the second equality holds because the formula of the second step includes the item $\mathrm{tr}(Q_j\rho_j)=0$.

Therefore, the measurement outcome corresponding to $Q_1\otimes\ldots Q_{i-1}\otimes P_i\otimes Q_{i+1}\otimes\cdots\otimes Q_n$ correctly indicates the state $\rho_i^{\otimes n}$ for any $i=1,\ldots,n$. For any other measurement outcome, we get an inconclusive result. This is an unambiguous discrimination strategy among the states $\rho_1^{\otimes n},\ldots,\rho_n^{\otimes n}$. ■

Applying lemma 1, we find the necessary and sufficient condition for a set of quantum operations to be unambiguously distinguishable by multiple uses.

Theorem 2. If the quantum operations $\{\mathcal{E}_1,\ldots,\mathcal{E}_n\}$ satisfy that for any $i\neq j$, $\mathrm{supp}(\mathcal{E}_i)\nsubseteq\mathrm{supp}(\mathcal{E}_j)$, then they can be unambiguously discriminated by n uses. Otherwise, for any $N\geqslant 1$, they cannot be unambiguously discriminated by N uses.

Proof. If there exist $\mathcal{E}_i$ and $\mathcal{E}_j$ such that $\mathrm{supp}(\mathcal{E}_i)\subseteq\mathrm{supp}(\mathcal{E}_j)$, then it is easy to see that for any $N\geqslant 1$, $\mathrm{supp}(\mathcal{E}_i^{\otimes N})\subseteq\mathrm{supp}(\mathcal{E}_j^{\otimes N})$. It follows from theorem 1 that $\mathcal{E}_i^{\otimes N}$ and $\mathcal{E}_j^{\otimes N}$ cannot be unambiguously discriminated by a single use.

Now suppose that for any $i\neq j$, $\mathrm{supp}(\mathcal{E}_i)\nsubseteq\mathrm{supp}(\mathcal{E}_j)$. From theorem 1 we know that for any $i\neq j$, $\mathcal{E}_i$ and $\mathcal{E}_j$ are unambiguously distinguishable by a single use. Furthermore, it is from the proof of theorem 1 that for any entangled input $|\psi\rangle$ with a full Schmidt number, the outputs $(\mathcal{E}_i\otimes\mathcal{I})(|\psi\rangle\langle\psi|)$ and $(\mathcal{E}_j\otimes\mathcal{I})(|\psi\rangle\langle\psi|)$ are unambiguously distinguishable. So the set of states $\{(\mathcal{E}_1\otimes\mathcal{I})(|\psi\rangle\langle\psi|),\ldots,(\mathcal{E}_n\otimes\mathcal{I})(|\psi\rangle\langle\psi|)\}$ satisfy the condition of lemma 1, we hereby conclude that their n-fold copies $((\mathcal{E}_1\otimes\mathcal{I})(|\psi\rangle\langle\psi|))^{\otimes n},\ldots,((\mathcal{E}_n\otimes\mathcal{I})(|\psi\rangle\langle\psi|))^{\otimes n}$ can be unambiguously discriminated. Thus, $\mathcal{E}_1,\ldots,\mathcal{E}_n$ can be unambiguously discriminated by n uses with the input $|\psi\rangle^{\otimes n}$. ■

Combining the proof of lemma 1 and theorem 2, we have explicitly constructed the input states and corresponding measurements that unambiguously discriminate the given quantum operations in the case of multiple uses. It should be noted that the measurement presented in the proof lemma 1 is actually separable so it is practically implementable.

Comparing the condition of theorem 2 with that of theorem 1, we can see that the former is looser. So it is possible that a set of quantum operations can be unambiguously discriminated only by multiple uses. For example, consider three Pauli channels $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ which have Kraus operators $\{\sqrt{p}I, \sqrt{1-p}X\}$, $\{\sqrt{q}I, \sqrt{1-q}Z\}$, and $\{\sqrt{s}X, \sqrt{1-s}Z\}$, respectively, i.e.,

$$\mathcal{E}_1(\rho) = p\rho + (1-p)X\rho X, \tag{18}$$

$$\mathcal{E}_2(\rho) = q\rho + (1-q)Z\rho Z, \tag{19}$$

$$\mathcal{E}_3(\rho) = sX\rho X + (1-s)Z\rho Z. \tag{20}$$

Since $\mathrm{supp}(\mathcal{E}_3) \subseteq \mathrm{supp}(\{\mathcal{E}_1, \mathcal{E}_2\})$, we know from theorem 1 that they cannot be unambiguously discriminated by a single use. However, they satisfy the condition of theorem 2 and thus can be unambiguously discriminated by three uses.

It is also found that when distinguishing two quantum operations, the conditions of theorem 1 and theorem 2 coincide, which means that multiple uses do not change the distinguishability in this case. By theorem 2, the only scenario in which unambiguous discrimination cannot be applied to a given set of quantum operations is that one of them has support totally contained in the support of another one.

Our discussions above mainly focus on the possibility of unambiguous discrimination. It is certainly beneficial to consider how to achieve the best efficiency. Specifically, we should find the input state that maximizes the optimal success probability of unambiguous discrimination between the corresponding output states. But even for a set of known states, the optimal success probability of unambiguous discrimination between them has no analytical formulation in general so far [13]. So our problem is difficult to solve analytically. Even so, since in most cases the quantum operation to be identified is repeatable, we can repeat a nonoptimal procedure to make the total failure probability exponentially decrease, obtaining the result quickly. Because our strategy is error-free, once we get a conclusive result it can be immediately accepted.

It is a surprising fact that the conditions for unambiguous discrimination of quantum operations are in the form similar to those for quantum states. This can be understood partially from the point that our strategy has a natural dependence on unambiguous discrimination of quantum states. A profounder understanding is that there exist inherent relations between quantum states and operations. Some previous work has been devoted to this topic [36–38] and it deserves further research.

In conclusion, we consider the problem of unambiguous discrimination among a given set of quantum operations. We derive the necessary and sufficient condition for them to be unambiguously distinguishable in the cases of single use and multiple uses, respectively. In the latter case a strategy is explicitly given. It is also found that the use of entanglement can improve the efficiency and even change the possibility of unambiguous discrimination between the given quantum operations. We hope our work can stimulate further research on discrimination of quantum operations.

We are thankful to the colleagues in the Quantum Computation and Quantum Information Research Group for helpful discussions. This work was supported by the Natural Science Foundation of China (Grants Nos. 60273003, 60433050, and 60305005).

[1] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
[2] For a review, see J. Bergou, U. Herzog, and M. Hillery, *Quantum State Estimation*, Lecture Notes in Physics Vol. 649 (Springer, Berlin, 2004), p. 417.
[3] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[4] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[5] A. Peres, Phys. Lett. A **128**, 19 (1988).
[6] A. Chefles, Phys. Rev. A **64**, 062305 (2001).
[7] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **66**, 032315 (2002).
[8] Y. C. Eldar, IEEE Trans. Inf. Theory **49**, 446 (2003).
[9] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
[10] M. Takeoka, M. Ban, and M. Sasaki, Phys. Rev. A **68**, 012307 (2003).
[11] P. Raynal, N. Lütkenhaus, and S. J. van Enk, Phys. Rev. A **68**, 022308 (2003).
[12] A. Chefles, Phys. Rev. A **69**, 050307(R) (2004).
[13] Y. C. Eldar, M. Stojnic, and B. Hassibi, Phys. Rev. A **69**, 062318 (2004).
[14] Y. Feng, R. Y. Duan, and M. S. Ying, Phys. Rev. A **70**, 012308 (2004).
[15] U. Herzog and J. A. Bergou, Phys. Rev. A **70**, 022302 (2004).
[16] M. Mohseni, A. M. Steinberg, and J. A. Bergou, Phys. Rev. Lett. **93**, 200403 (2004).
[17] J. Mimih and M. Hillery, Phys. Rev. A **71**, 012329 (2005).
[18] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. A **71**, 042314 (2005).
[19] U. Herzog and J. A. Bergou, Phys. Rev. A **71**, 050301(R) (2005).
[20] J. A. Bergou and M. Hillery, Phys. Rev. Lett. **94**, 160501 (2005).
[21] P. Raynal and N. Lütkenhaus, Phys. Rev. A **72**, 022342 (2005).
[22] The support of a density operator is the space spanned by its eigenvectors with nonzero eigenvalues. The sum of sets $S_1 + \ldots + S_n$ is defined to be the set of all the elements that can be written as $x_1 + \ldots + x_n$ where $x_i \in S_i$.
[23] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000).
[24] A. Acín, Phys. Rev. Lett. **87**, 177901 (2001).
[25] A. Chefles, Phys. Rev. A **72**, 042332 (2005).
[26] G. M. D'Ariano, M. F. Sacchi, and J. Kahn, Phys. Rev. A **72**, 052302 (2005).
[27] M. F. Sacchi, J. Opt. B: Quantum Semiclassical Opt. **7**, S333

(2005).

[28] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).

[29] V. P. Belavkin, G. M. D'Ariano, and M. Raginsky, J. Math. Phys. **46**, 062106 (2005).

[30] D. Yang, e-print quant-ph/0504073.

[31] M. F. Sacchi, Phys. Rev. A **71**, 062340 (2005).

[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), p. 372.

[33] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997).

[34] J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).

[35] The kernel of a density operator is the space orthogonal to its support.

[36] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).

[37] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).

[38] G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **91**, 047902 (2003).