Perfect Distinguishability of Quantum 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 100084, China and Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology, Sydney, New South Wales 2007, Australia

(Received 7 August 2009; published 20 November 2009)

We provide a feasible necessary and sufficient condition for when an unknown quantum operation (quantum device) secretly selected from a set of known quantum operations can be identified perfectly within a finite number of queries, and thus complete the characterization of the perfect distinguishability of quantum operations. We further design an optimal protocol which can achieve the perfect discrimination between two quantum operations by a minimal number of queries. Interestingly, we find that an optimal perfect discrimination between two isometries is always achievable without auxiliary systems or entanglement.

DOI: 10.1103/PhysRevLett.103.210501 PACS numbers: 03.67.Ac, 03.65.Ta, 03.67.Hk

One of the fundamental features of quantum mechanics is that it is impossible to distinguish between two nonorthogonal states perfectly, even when arbitrarily large but finite copies of states are available. A recent highlight of this fact is the identification of the quantum Chernoff bound [1]. In view of this, the perfect distinguishability of quantum states is completely characterized by the orthogonality.

A problem closely related to quantum state discrimination is the discrimination of quantum operations (or interchangeably quantum devices), which formalize all physically realizable operations in quantum mechanics including unitary operations, quantum measurements, and quantum channels, etc. The goal of quantum operation discrimination is to find out the identity of an unknown device secretly chosen from two known quantum operations. Recently this problem has received great interest and many results have been reported (See Refs. [2–8] for a partial list). It is now clear that distinguishing quantum operations has many interesting properties that are similar to that of quantum state discrimination if the device is probed only once [2–5]. On the other hand, quantum devices are very different from quantum states in the following three aspects. First, a quantum device is reusable. Second, the input state of quantum device can be chosen freely, and thus can be entangled with an auxiliary system or between different uses. Third, perhaps most importantly, a quantum device can be used in many essentially different ways such as in parallel, in sequential, or in any other scheme allowed by quantum mechanics while the optimal way to manipulate many copies of quantum states is uniquely in parallel [1]. Consequently, it is extremely difficult to identify the behavior of quantum operations when multiple queries are used.

Several works have been devoted to the perfect distinguishability of special quantum operations including unitary operations [3,4,6,7] and projective measurements [8]. Most notably, unitary operations can be identified with certainty either in parallel [4], or in sequential [6]. Projective measurements also enjoy this kind of perfect distinguishability [8]. Experimental results concerning with the perfect discrimination of unitary operations and measurements have been reported [9]. All these progresses indicate that the notion of perfect distinguishability of general quantum operations would be much more complicated and flexible than that of quantum states.

The purpose of this Letter is to provide a complete characterization of the perfect distinguishability of quantum operations (see Theorem 1 below). We show that two simple properties are responsible for the perfect discrimination between two quantum operations within a finite number of queries. The first property says that these two quantum operations should produce two quantum states with nonoverlapping supports upon some input state, which may be entangled with an auxiliary system. The second property states that any such two quantum operations are capable of boosting some two nonorthogonal pure states, which are provided to the quantum operations as their respective inputs, into orthogonal states. Both of these properties can be rephrased into analytical forms in terms of the Kraus operators and can be verified quite efficiently. Our result reveals the essential nature of the perfect distinguishability of quantum operations and thus provides new insight into this problem. Applying this characterization to specific quantum operations, we can directly obtain many interesting results on the perfect distinguishability of quantum operations. In particular, a unitary operation U and a general quantum operation $\mathcal{E}$ are perfectly distinguishable if and only if U is not a Kraus operator of $\mathcal{E}$. As a potential application, we show that the classical data hiding is possible by encoding the data into quantum devices instead of quantum states [10].

With the help of the notion of the maximal fidelity, we further design an optimal protocol which can distinguish two quantum operations with a minimal number of queries. This number can be determined using numerical iteration techniques. When distinguishing between two isometries (generalization of unitary operations), the calculation becomes quite efficient and an optimal discrimination can always be achieved without auxiliary systems or entanglement by using the theory of q-numerical range. This generalizes our previous work on unitary operations [6].

Consider a d-dimensional Hilbert space $\mathcal{H}_d$. The set of linear operators on $\mathcal{H}_d$ is denoted by $\mathcal{B}(\mathcal{H}_d)$. A general quantum state ρ on $\mathcal{H}_d$ is given by a positive operator in $\mathcal{B}(\mathcal{H}_d)$ with trace one. A pure state $|\psi\rangle$ is a unit vector in $\mathcal{H}_d$. For ease of notations, we will use ψ to denote the density operator form $|\psi\rangle\langle\psi|$ of $|\psi\rangle$. Let ρ be with the spectral decomposition $\rho = \sum_{k=1}^{d} p_k|\psi_k\rangle\langle\psi_k|$. The support of ρ is given by $\mathrm{supp}(\rho) = \mathrm{span}\{|\psi_k\rangle: p_k > 0\}$. A quantum operation $\mathcal{E}$ from $\mathcal{B}(\mathcal{H}_d)$ to $\mathcal{B}(\mathcal{H}_{d'})$ is a trace-preserving completely positive map with the form $\mathcal{E}(\rho) = \sum_{i=1}^{m} E_i\rho E_i^\dagger$, where $\{E_i\}_{i=1\cdots m}$ are the Kraus operators of $\mathcal{E}$ satisfying $\sum_i E_i^\dagger E_i = I_d$. Note that an isometry is a linear operator U from $\mathcal{H}_d$ to $\mathcal{H}_{d'}$ such that $U^\dagger U = I_d$.

ρ_0 and ρ_1 are said to be disjoint if $\mathrm{supp}(\rho_0) \cap \mathrm{supp}(\rho_1) = \{0\}$. The maximal fidelity quantitatively characterizes the disjointedness between two quantum states (actually two subspaces) and is defined as follows:

$$\tilde{F}(\rho_0, \rho_1) = \max\{|\langle\psi_0|\psi_1\rangle|: |\psi_k\rangle \in \mathrm{supp}(\rho_k), k = 0, 1\}$$

Clearly, $0 \le \tilde{F}(\rho_0, \rho_1) \le 1$. $\tilde{F}$ is vanishing iff ρ_0 and ρ_1 are orthogonal, and attains 1 iff ρ_0 and ρ_1 are not disjoint. The most important property of the maximal fidelity is the following operational interpretation, which is a key tool in our later discussion. See [11] for a similar property of ordinary fidelity.

Lemma 1.—For two pairs of quantum states $\{\rho_0, \rho_1\}$ and $\{|\psi_0\rangle, |\psi_1\rangle\}$, there is a quantum operation $\mathcal{T}$ such $\mathcal{T}(\rho_k) = \psi_k$ for $k = 0, 1$ iff $\tilde{F}(\rho_0, \rho_1) \le \tilde{F}(\psi_0, \psi_1) = |\langle\psi_0|\psi_1\rangle|$. Thus we have $\tilde{F}(\rho_0, \rho_1) = \min\{|\langle\psi_0|\psi_1\rangle|: \exists\mathcal{T}, \mathcal{T}(\rho_k) = \psi_k\}$.

Proof.—The necessity can be easily proven by the results from Ref. [11]. Here we only focus on the sufficiency. Assume that $\tilde{F}(\rho_0, \rho_1) \le |\langle\psi_0|\psi_1\rangle|$. We will construct a quantum operation $\mathcal{T}$ such that $\mathcal{T}(\rho_k) = \psi_k$ for $k = 0, 1$. We exclude the trivial cases and assume $0 < \tilde{F}(\rho_0, \rho_1) < 1$. Let P and Q be the projectors onto $\mathrm{supp}(\rho_0)$ and $\mathrm{supp}(\rho_1)$, respectively. Applying the singular-valued decomposition theorem to PQ, we have

$$PQ = \sum_{k=1}^{r} \lambda_k|\psi_0^{(k)}\rangle\langle\psi_1^{(k)}|,$$

where $\lambda_k > 0$ for $1 \le k \le r$. One can verify that $\langle\psi_0^{(i)}|\psi_1^{(j)}\rangle = \delta_{ij}\lambda_i$. So $\{|\psi_0^{(k)}\rangle, |\psi_1^{(k)}\rangle\}_{k=1\ldots r}$ are mutually orthogonal. Let P_k be the projector onto $\mathrm{span}\{|\psi_0^{(k)}\rangle, |\psi_1^{(k)}\rangle\}$ for each $k = 1\cdots r$. Let $P_0 = P - \sum_{k=1}^{r}|\psi_0^{(k)}\rangle\langle\psi_0^{(k)}|$ and $P_{r+1} = Q - \sum_{k=1}^{r}|\psi_1^{(k)}\rangle\langle\psi_1^{(k)}|$. One can see that $\{P_0, P_1, \cdots, P_r, P_{r+1}\}$ forms a complete projective measurement on $\mathrm{supp}(P + Q)$. We then apply this measurement to $\{\rho_0, \rho_1\}$. If the outcome is 0 or $r + 1$ then the original state is ρ_0 or ρ_1, respectively, and we can directly prepare the target as ψ_0 or ψ_1. Otherwise the outcome is $1 \le k \le r$ and the left state should be $|\psi_0^{(k)}\rangle$ or $|\psi_1^{(k)}\rangle$, depending on the original state is ρ_0 or ρ_1, respectively. Noticing that $|\langle\psi_0^{(k)}|\psi_1^{(k)}\rangle| \le \tilde{F}(\rho_0, \rho_1) \le |\langle\psi_0|\psi_1\rangle|$, we can further transform $\{|\psi_0^{(k)}\rangle, |\psi_1^{(k)}\rangle\}$ into $\{|\psi_0\rangle, |\psi_1\rangle\}$. ■

It is straightforward to define that two quantum operations $\mathcal{E}_0$ and $\mathcal{E}_1$ are (entanglement-assisted) disjoint if there is an input state $|\psi\rangle^{RQ}$ such that $(I^R \otimes \mathcal{E}_0^Q)(\psi^{RQ})$ and $(I^R \otimes \mathcal{E}_1^Q)(\psi^{RQ})$ are disjoint, where R and Q denote auxiliary and principal systems, respectively, and I^R is the identity operation on R. The use of auxiliary system is not always necessary for the disjointedness between some special quantum operations including unitary operations, but is unavoidable for general quantum operations.

There is an efficient procedure to determine whether $\mathcal{E}_0$ and $\mathcal{E}_1$ are disjoint. Suppose that $\mathcal{S}_k = \mathrm{span}\{E_{ki}\}_{i=1\cdots n_k}$, $k = 0, 1$. If $\mathcal{S}_0 \cap \mathcal{S}_1 = \{0\}$ then $\mathcal{E}_0$ and $\mathcal{E}_1$ are entanglement-assisted disjoint and the input state can be chosen as $|\alpha\rangle^{RQ} = 1/\sqrt{d}\sum_{k=1}^{d}|k\rangle^R|k\rangle^Q$. Otherwise, select a basis $\{D_i\}_{i=1\cdots p}$ for $\mathcal{S}_0 \cap \mathcal{S}_1$, and construct an operator $X = \sum_{k=1}^{p} D_k^\dagger D_k$. Let P_1 be the projector onto $\mathrm{supp}(X)$, and consider two new quantum operations $\mathcal{E}_0'$ and $\mathcal{E}_1'$ with respective Kraus operators $\{E_{0i}P_1^\perp\}$ and $\{E_{1j}P_1^\perp\}$, where $P_1^\perp = I_d - P_1$. The original problem is now reduced to decide whether $\mathcal{E}_0'$ and $\mathcal{E}_1'$ are disjoint. Repeating this process $n \le d$ times we can efficiently construct a sequence of mutually orthogonal projectors $P_1, \ldots, P_n$ such that $P_n = 0$ and $P_i \ne 0$ for any $i < n$. Let $P = I_d - \sum_{i=1}^{n-1} P_i$. Then $\mathcal{E}_0$ and $\mathcal{E}_1$ are entanglement-assisted disjoint iff $P \ne 0$. If satisfied, $|\psi\rangle = (I \otimes P)|\alpha\rangle$ is an eligible input state.

We are now ready to present a complete characterization of the perfect distinguishability of quantum operations.

Theorem 1.—Let $\mathcal{E}_0$ and $\mathcal{E}_1$ be two quantum operations from $\mathcal{B}(\mathcal{H}_d)$ to $\mathcal{B}(\mathcal{H}_{d'})$ with Kraus operators $\{E_{0i}: i = 1\cdots n_0\}$ and $\{E_{1j}: j = 1\cdots n_1\}$, respectively. Then $\mathcal{E}_0$ and $\mathcal{E}_1$ are perfectly distinguishable by a finite number of uses iff (i) $\mathcal{E}_0$ and $\mathcal{E}_1$ are disjoint and (ii) $I_d \notin \mathrm{span}\{E_{0i}^\dagger E_{1j}\}$.

Proof.—The necessity of (i) and (ii) will be evident from the remarks after Theorem 2. The sufficiency follows from the following protocol to distinguish between $\mathcal{E}_0$ and $\mathcal{E}_1$ (R is an auxiliary system with dimension d):

Step 1. Calculate $|\psi_0\rangle^{RQ}$ and $|\psi_1\rangle^{RQ}$ such that $\langle\psi_0|\psi_1\rangle \ne 0$ and $(I \otimes \mathcal{E}_0)(\psi_0) \perp (I \otimes \mathcal{E}_1)(\psi_1)$. This can be done due to condition (ii). More precisely, let $|\psi_0\rangle = |\alpha\rangle^{RQ}$ and $|\psi_1\rangle = (I \otimes M)|\alpha\rangle^{RQ}$, where $M \in \mathrm{span}^\perp\{E_{0i}^\dagger E_{1j}\}$ and $\mathrm{tr}(M^\dagger M) = d$.

Step 2. Choose $|\phi\rangle^{RQ}$ such that $\rho_0 = (I \otimes \mathcal{E}_0)(\phi)$ and $\rho_1 = (I \otimes \mathcal{E}_1)(\phi)$ are disjoint. This can be done due to condition (i).

Prepare N copies of $|\phi\rangle^{RQ}$ and apply the unknown device N times to Q in parallel. Then we are left with a state from $\{\rho_0^{\otimes N}, \rho_1^{\otimes N}\}$. Choose N such that $\tilde{F}(\rho_0^{\otimes N}, \rho_1^{\otimes N}) = \tilde{F}(\rho_0, \rho_1)^N \leq |\langle\psi_0|\psi_1\rangle|$. We can choose $N = \lceil \ln|\langle\psi_0|\psi_1\rangle| / \ln\tilde{F}(\rho_0, \rho_1)\rceil$.

Step 3. Transform $(\rho_0^{\otimes N}, \rho_1^{\otimes N})$ into $(|\psi_0\rangle, |\psi_1\rangle)$ by some quantum operation $\mathcal{T}$, which can be done due to our choice of N and Lemma 1. Then applying the unknown device to $(|\psi_0\rangle, |\psi_1\rangle)$ will yield two orthogonal states, which allows us to perfectly identify the unknown device with $N + 1$ queries. ■

A potential application of Theorem 1 is to design a classical data hiding protocol using devices instead of states [10]: A boss, say Charlie, encodes a secret bit b into two pairs of quantum operations (devices) $(\mathcal{E}_b, \mathcal{E}'_b)_{b=0,1}$, and allocates $\mathcal{E}_b$ and $\mathcal{E}'_b$ to Alice and Bob, respectively. Alice and Bob cannot individually infer b with certainty. However, they can reveal the bit if they perform joint quantum operations or receive shared entanglement from Charlie. Theorem 1 allows us to construct these kind of instances by imposing that $\{\mathcal{E}_0, \mathcal{E}_1\}$ satisfies only condition (i) while $\{\mathcal{E}'_0, \mathcal{E}'_1\}$ satisfies only condition (ii). For example, $\mathcal{E}_0$ and $\mathcal{E}_1$ are quantum operations that prepare quantum states $|\psi_0\rangle = (|0\rangle + \sqrt{2}|1\rangle)/\sqrt{3}$ and $|\psi_1\rangle = (|0\rangle - \sqrt{2}|1\rangle)/\sqrt{3}$, respectively, while $\mathcal{E}'_0 = (|0\rangle\langle 0| + 1/\sqrt{2}|1\rangle\langle 1|, 1/\sqrt{2}|1\rangle\langle 1|, 0)$ and $\mathcal{E}'_1 = (|0\rangle \times \langle 0| + 1/\sqrt{2}|1\rangle\langle 1|, 0, 1/\sqrt{2}|1\rangle\langle 1|)$ are two one-qubit measurements. One can easily verify that $\mathcal{E}'_0$ and $\mathcal{E}'_1$ are perfectly distinguishable upon the respective input states $|\psi_0\rangle$ and $|\psi_1\rangle$ as $\mathrm{tr}((|0\rangle\langle 0| + 1/2|1\rangle\langle 1|)|\psi_0\rangle\langle\psi_1|) = 0$. The new feature of hiding classical data using quantum devices is that the identified device can be reused in the future information processing tasks.

The protocol we presented in Theorem 1 is not optimal in general. To describe an optimal one, we need the notion of q-maximal fidelity, which is naturally induced from the maximal fidelity between quantum states, to quantitatively describe the disjointedness between quantum operations. For quantum operations $\mathcal{E}_0$ and $\mathcal{E}_1$, and $0 \leq q \leq 1$, the (unassisted) q-maximal fidelity is defined as follows:

$$\tilde{F}_q(\mathcal{E}_0, \mathcal{E}_1) = \min\{\tilde{F}(\mathcal{E}_0(\psi_0), \mathcal{E}_1(\psi_1)) \colon \langle\psi_0|\psi_1\rangle = q\}.$$

The entanglement-assisted q-maximal fidelity is defined as follows:

$$\tilde{F}_q^{ea}(\mathcal{E}_0, \mathcal{E}_1) = \tilde{F}_q(\mathcal{I}^R \otimes \mathcal{E}_0^Q, \mathcal{I}^R \otimes \mathcal{E}_1^Q),$$

where R is an auxiliary system with the same dimension as Q (larger cannot make difference). When $q = 1$, $\tilde{F}_1(\mathcal{E}_0, \mathcal{E}_1)$ and $\tilde{F}_1^{ea}(\mathcal{E}_0, \mathcal{E}_1)$ are said to be the maximal fidelity and the entanglement-assisted maximal fidelity between $\mathcal{E}_0$ and $\mathcal{E}_1$, respectively.

$\tilde{F}_q^{ea}(\mathcal{E}_0, \mathcal{E}_1)$ plays a crucial role in designing the optimal perfect discrimination protocol mainly due to the following desirable property:

$$\tilde{F}_q^{ea}(\mathcal{E}_0, \mathcal{E}_1) \leq \frac{q}{q'}\tilde{F}_{q'}^{ea}(\mathcal{E}_0, \mathcal{E}_1), \qquad 0 \leq q < q' \leq 1. \quad (1)$$

This property can be understood as "more distinguishable input states will yield more distinguishable output states." It is true due to the fact that by appending an auxiliary qubit we can divide the input states for $\tilde{F}_q^{(ea)}$ into two parts: a pair of qubit states with inner product q/q' and a pair of optimal input states for $\tilde{F}_{q'}^{ea}$.

Let $N_{\min}$ be the minimal number of uses of the unknown quantum operation required to perfectly distinguish between $\mathcal{E}_0$ and $\mathcal{E}_1$, and let $\{q_k\}$ be a sequence of q-maximal fidelities recursively defined as follows:

$$q_0 = 1, \qquad q_k = \tilde{F}_{q_{k-1}}^{ea}(\mathcal{E}_0, \mathcal{E}_1), \qquad k \geq 1.$$

Notice that $q_1 = \tilde{F}_1^{(ea)}(\mathcal{E}_0, \mathcal{E}_1)$ is just the maximal fidelity between $\mathcal{E}_0$ and $\mathcal{E}_1$. Let us further introduce $q_{\max}$ by $q_{\max} = \max\{q \colon \tilde{F}_q^{(ea)}(\mathcal{E}_0, \mathcal{E}_1) = 0\}$. Then the following theorem shows that $N_{\min}$ is completely determined by the sequence of $\{q_k\}$ and $q_{\max}$ (indirectly).

Theorem 2.—Let $\mathcal{N}^{(k)}$ be an arbitrary quantum discrimination network containing k uses of the unknown quantum operation from $\{\mathcal{E}_0, \mathcal{E}_1\}$. Then

$$q_k \leq \tilde{F}_1^{ea}(\mathcal{N}^{(k)}(\mathcal{E}_0), \mathcal{N}^{(k)}(\mathcal{E}_1)).$$

Hence $\mathcal{E}_0$ and $\mathcal{E}_1$ are perfectly distinguishable iff $q_k = 0$ for some $k \geq 1$. If so, $N_{\min} = \min\{k \colon q_k = 0, k \geq 1\} = \min\{k \colon q_{k-1} \leq q_{\max}\}$, and $q_k = 0$ for any $k > N_{\min}$.

Proof.—By definition q_1 is the optimal maximal fidelity one can achieve by a single use. Assume that q_k is optimal by k uses of the unknown device. Consider now any quantum discrimination protocol $\mathcal{N}^{(k+1)}$ containing $k + 1$ uses of the unknown device. By the induction assumption, we have $q'_k = \tilde{F}(\rho_0^{(k)}, \rho_1^{(k)}) \geq q_k$, where $\rho_0^{(k)}$ and $\rho_1^{(k)}$ are the output states of $\mathcal{N}^{(k+1)}$ except the last use of the unknown device. Clearly, $\rho_0^{(k)}$ and $\rho_1^{(k)}$ are the output states of a quantum discrimination network containing k uses of the unknown device, and also the input states for the last query in $\mathcal{N}^{(k+1)}$. Let $\rho_0^{(k+1)}$ and $\rho_1^{(k+1)}$ be the final output states of $\mathcal{N}^{(k+1)}$. By Eq. (1), we have

$$\tilde{F}(\rho_0^{(k+1)}, \rho_1^{(k+1)}) \geq \tilde{F}_{q'_k}^{ea}(\mathcal{E}_0, \mathcal{E}_1) \geq \frac{q'_k}{q_k}\tilde{F}_{q_k}^{ea}(\mathcal{E}_0, \mathcal{E}_1) \geq q_{k+1},$$

where we have employed the assumption $q'_k \geq q_k$ and the definition of q_{k+1}. The expression of $N_{\min}$ follows immediately. ■

It is clear from the above proof that $\mathcal{E}_0$ and $\mathcal{E}_1$ are perfectly distinguishable iff $q_1 < 1$ and $q_{\max} > 0$, which is based on the following two simple observations: (1) $q_1 = 1$ implies $q_k = 1$ for any $k \geq 1$; or (2) $q_{\max} = 0$ implies $q_k > 0$ for any $k \geq 1$. One can readily verify that $q_1 < 1$ and $q_{\max} > 0$ correspond to conditions (i) and (ii) in Theorem 1, respectively.

The sequence of $\{q_k\}$ and $q_{\max}$ can be calculated with arbitrary high precision using numerical iteration techniques as it is evident that $F_q^{(ea)}(\mathcal{E}_0, \mathcal{E}_1)$ can be formulated into an optimization problem on a compact set. Hence we can estimate $N_{\min}$ for any two quantum operations $\mathcal{E}_0$ and $\mathcal{E}_1$ according to the above theorem.

If both $\mathcal{E}_0$ and $\mathcal{E}_1$ are isometries, the calculation of $\{q_k\}$ and $q_{\max}$ becomes quite tractable. For isometries U_0 and U_1, we have

$$\tilde{F}_q(U_0, U_1) = \tilde{r}_q(A) = \min\{|z|: z \in W_q(A)\},$$

where $A = U_0^\dagger U_1$ [12] and $W_q(A) = \{\langle\psi_0|A|\psi_1\rangle: \langle\psi_0|\psi_1\rangle = q\}$. Similarly, $\tilde{F}_q^{ea}(U_0, U_1) = \tilde{r}_q(I_d \otimes A)$. For $0 \leq q \leq 1$, $W_q(A)$ is said to be the q-numerical range of A with $\tilde{r}_q(A)$ the inner radius [13–15]. A somewhat surprising fact is that the optimal perfect discrimination of isometries can be achieved without auxiliary systems or entanglement. That is, for any isometries U_0 and U_1 and $0 \leq q \leq 1$,

$$\tilde{F}_q^{ea}(U_0, U_1) = \tilde{F}_q(U_0, U_1).$$

Previously we have shown the same result for unitary operations [6]. The above result follows from an interesting property about the q-numerical range, say $W_q(I_d \otimes A) = W_q(A)$ for any linear operator A and $0 \leq q \leq 1$. A detailed proof of property is provided in [16].

No explicit form of $\tilde{r}(A)$ is known in general. Hence it seems impossible to obtain the analytical formula of $N_{\min}(U_0, U_1)$ except some special cases such as A is normal. Fortunately, $W_q(A)$ is a convex compact set [14]. As a result, it is quite feasible to compute $\tilde{r}_q(A)$, and hence to determine the exact value of $N_{\min}$. In particular, the case that A is unitary has been completely solved [6]. For the case that A is positive definite, any parallel protocol cannot distinguish between U_0 and U_1. In sharp contrast, we know from the above discussions that there is a sequential protocol that can achieve an optimal perfect discrimination [17].

It would be highly desirable to identify the quantum Chernoff bound for quantum operations that are not perfectly distinguishable. Many of our techniques can be generalized to multipartite setting, where distant parties share an unknown quantum operation and they are only allowed to perform arbitrary local operations and communicate with each other classically (LOCC). Previously we have shown that the perfect distinguishability of unitary operations is preserved under LOCC [18], benefiting from the local distinguishability of two orthogonal multipartite pure states [19]. However, the condition for the perfect distinguishability of general multipartite quantum operations by LOCC remains open.

This work was partially supported by NSF of China (Grants No. 60702080, No. 60736011, No. 60621062), 863 project of China (Grant No. 2006AA01Z102), FANEDD (Grant No. 200755), and QCIS, University of Technology, Sydney.

*Runyao.Duan@uts.edu.au

[1] K. M. R. Audenaert *et al.*, Phys. Rev. Lett. **98**, 160501 (2007).

[2] A. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); D. Aharonov, A. Kitaev, and N. Nisan, in Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computation (STOC 97) (ACM, El Paso, 1997), pp. 20–30.

[3] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000).

[4] A. Acín, Phys. Rev. Lett. **87**, 177901 (2001); G. M. D'Ariano, P. LoPresti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).

[5] M. F. Sacchi, Phys. Rev. A **71**, 062340 (2005); D. Yang, arXiv:quant-ph/0504073; G. M. Wang and M. S. Ying, Phys. Rev. A **73**, 042301 (2006); A. Chefles *et al.*, J. Phys. A **40**, 10 183 (2007); J. Watrous, arXiv:0710.0902; M. Ziman, Phys. Rev. A **77**, 062112 (2008); M. Piani and J. Watrous, Phys. Rev. Lett. **102**, 250501 (2009).

[6] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **98**, 100503 (2007).

[7] X. D. Wu and R. Y. Duan, Phys. Rev. A **78**, 012303 (2008); G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008); J. X. Chen and M. S. Ying, arXiv:0809.0336.

[8] Z. F. Ji, Y. Feng, R. Y. Duan, and M. S. Ying, Phys. Rev. Lett. **96**, 200401 (2006).

[9] A. Laing, T. Rudolph, and J. L. O'Brien, Phys. Rev. Lett. **102**, 160502 (2009); P. Zhang *et al.*, J. Phys. B **41**, 195501 (2008).

[10] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001); T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).

[11] A. Uhlmann, Ann. Phys. (Leipzig) **497**, 524 (1985); see also A. Chefles, R. Jozsa, and A. Winter, arXiv:quant-ph/0307227; J. L. Dodd and M. A. Nielsen, Phys. Rev. A **66**, 044301 (2002).

[12] We can show that a linear operator $A \in \mathcal{B}(\mathcal{H}_d)$ can be written into the form $A = U_0^\dagger U_1$ for some isometries U_0 and U_1 from $\mathcal{B}(\mathcal{H}_d)$ to $\mathcal{B}(\mathcal{H}_{d'})$ iff $A^\dagger A \leq I_d$.

[13] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, Cambridge, 1991), Chap. 1.

[14] N. K. Tsing, Linear Algebra Appl. **56**, 195 (1984).

[15] C. K. Li and H. Nakazato, Linear Multilinear Algebra **43**, 385 (1998).

[16] See EPAPS Document No. E-PRLTAO-103-033949 for a detailed proof of property. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.

[17] Recently a pair of entanglement-breaking channels with similar properties has been found, see A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, arXiv:0909.0256.

[18] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **100**, 020503 (2008).

[19] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).