Local Distinguishability of Multipartite Unitary Operations

Runyao Duan,* Yuan Feng,† and Mingsheng Ying‡
State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084

(Dated: February 11, 2013)

We show that any two different unitary operations acting on an arbitrary multipartite quantum system can be perfectly distinguishable by local operations and classical communication when a finite number of runs is allowed. We then directly extend this result into the case when the number of unitary operations to be discriminated is more than two. Intuitively, our result means that the lost identity of a nonlocal (entangled) unitary operation can be recovered locally, without any use of entanglement or joint quantum operations.

PACS numbers: 03.65.Ta, 03.65.Ud, 03.67.-a

Unitary operation is one of the most fundamental ingredients of quantum mechanics. The study of various properties of unitary operations lies at the heart of many quantum information processing tasks. Recently the discrimination of unitary operations has received many attentions [1, 2, 3, 4]. As a matter of fact, the well-known effect of quantum super-dense coding [5] can be treated as an instance of the discrimination of unitary operations [1, 6, 7]. Although two nonorthogonal quantum states cannot be perfectly distinguishable whenever only a finite number of copies are available[8, 9], it was shown that any two different unitary operations, no matter orthogonal or not, can always be perfectly distinguishable by taking a suitable entangled state as input and then applying only a finite number of runs of the unknown unitary operation [2, 3]. This result was further refined by showing that the entangled input state is not necessary [4]. The probabilistic discrimination of unitary operations as well as general quantum operations has also been studied extensively [10, 11, 12, 13, 14].

Up to now all the above discrimination schemes of quantum operations assume that the unknown quantum operation to be discriminated is under the completely control of a single party who can prepare any entangled states or perform any unconstrained quantum measurements in order to achieve an optimal discrimination. However, any reasonable quantum system in practice generally consists of several subsystems. Nonlocal unitary operations are a valuable resource to interact different subsystems together [15, 16, 17, 18]. The problem of distinguishing multipartite unitary operations naturally arises when several parties share a unitary operation but forget the real identity of the operation. Fortunately, they do remember that the unknown unitary operation belongs to a finite set of pre-specified unitary operations. As in this scenario different parties may be far from each other, a reasonable constraint on the discrimination is that each party is only allowed to perform local operations and classical communication (LOCC). Moreover, we assume that there is no pre-shared entanglement between any two distant parties. Here we may have two kinds of entanglement: One is shared between distant parties and the other is existing between different subsystems of a same party. The most expensive entanglement we are concerned with is the former and the latter can be used in order to achieve an optimal discrimination. A general scheme for LOCC discrimination of unitary operations is intuitively depicted as Fig. 1. Two special kinds of schemes are of particular interests. A scheme is said to be *parallel* if the computational network in Fig. 1 is reduced to the form of $U^{\otimes N}$ for some finite N. While it is said to be *sequential* if no auxiliary quantum systems are involved. In other words, in a sequential scheme every party cannot employ local entanglement and can only perform local unitary operations and projective measurements on a single quantum system. Clearly, a sequential scheme represents the most economic strategy for discrimination.

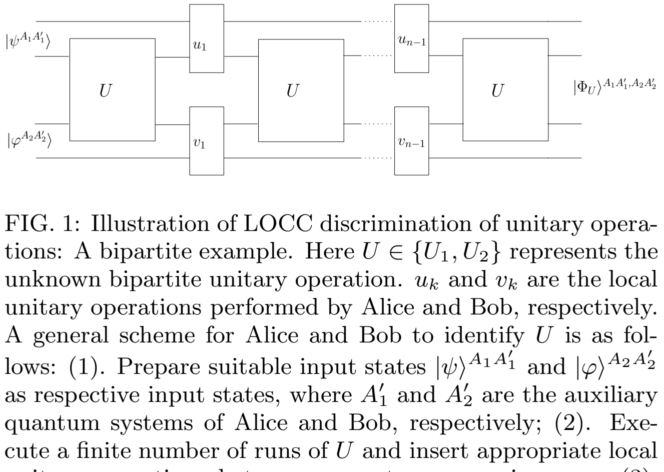
$|\psi^{A_1A_1'}\rangle$
$|\varphi^{A_2A_2'}\rangle$
U
u_1
v_1
U
u_{n-1}
v_{n-1}
U
$|\Phi_U\rangle^{A_1A_1',A_2A_2'}$

FIG. 1: Illustration of LOCC discrimination of unitary operations: A bipartite example. Here $U \in \{U_1, U_2\}$ represents the unknown bipartite unitary operation. u_k and v_k are the local unitary operations performed by Alice and Bob, respectively. A general scheme for Alice and Bob to identify U is as follows: (1). Prepare suitable input states $|\psi\rangle^{A_1A_1'}$ and $|\varphi\rangle^{A_2A_2'}$ as respective input states, where A_1' and A_2' are the auxiliary quantum systems of Alice and Bob, respectively; (2). Execute a finite number of runs of U and insert appropriate local unitary operations between every two successive runs; (3). Distinguish the final output states $|\Phi_U\rangle^{A_1A_1',A_2A_2'}$ by LOCC. U_1 and U_2 can be perfectly distinguishable if and only if the final output states $|\Phi_{U_1}\rangle$ and $|\Phi_{U_2}\rangle$ can be orthogonal [21].

The purpose of this Letter is to show that any two multipartite unitary operations can be perfectly distinguishable even under the constraint of LOCC. Our scheme for discrimination is rather simple as it only involves with parallel scheme and sequential scheme and only requires one party to prepare local entanglement. By similar arguments as that in Refs. [2, 4], we can directly extend this result into 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 our knowledge, this is the first result about the local distinguishability of multipartite quantum operations. An immediate application is as follows. Suppose several parties share an unknown unitary operation which is secretly chosen from a finite set of unitary operations, each of which is assumed to be capable of creating entanglement locally. Then these parties can always produce pure multipartite entanglement with certainty by employing the unknown operation shared among them. On the other hand, the same task is not possible if we consider the distillation of nonorthogonal entangled states instead of unitary operations.

Obviously, the proof presented in this Letter automatically provides an alternative way to show the perfect distinguishability between unitary operations in the global scenario [2, 3, 4]. However, due to the nonlocal nature of general multipartite unitary operations, the proof for the local distinguishability is rather complicated and needs lots of new techniques. For instance, the notion of numerical range for a linear operation has been generalized to multipartite setting and many interesting properties are presented. We hope these tools would also be useful in studying other problems in quantum information theory.

Let us begin to introduce the notion of numerical range. Consider a quantum system associated with a finite dimensional state space $\mathcal{H}$. The set of linear operations acting on $\mathcal{H}$ is denoted by $\mathcal{B}(\mathcal{H})$. In particular, $\mathcal{U}(\mathcal{H})$ is the set of unitary operations acting on $\mathcal{H}$. Two unitary operations $U, V \in \mathcal{U}(\mathcal{H})$ are said to be different if $U = e^{i\theta}V$ cannot hold for any real number θ. For $A \in \mathcal{B}(\mathcal{H})$. The numerical range (or the field of values) of A is a subset of complex numbers defined as follows:

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

When A is a normal operation, i.e., $AA^\dagger = A^\dagger A$. By spectral decomposition theorem it is easy to verify that $W(A) = Co(\sigma(A))$, where $\sigma(A)$ represents the set of eigenvalues of A and $Co(S)$ denotes the convex hull of S for $S \subseteq \mathcal{C}$. In other words, the numerical range of a normal operation is a convex polygon. Unfortunately, no similar analytical characterization of numerical range is known for general linear operations. Nevertheless, a celebrated theorem due to Toeplitz and Hausdorff states that the numerical range of a bounded linear operator is always convex. For our purpose here, a finite dimensional version of this theorem is sufficient [19].

Lemma 1. For any $A \in \mathcal{B}(\mathcal{H})$, $W(A)$ is convex. Moreover, let $\{|\psi_k\rangle\}$ be a finite set of normalized states, and let $\{p_k\}$ be a probability distribution, then the state $|\psi\rangle$ such that $\langle\psi|A|\psi\rangle = \sum_k p_k\langle\psi_k|A|\psi_k\rangle$ can be chosen as a linear combination of $|\psi_k\rangle$, i.e, $|\psi\rangle \in \text{span}\{|\psi_k\rangle\}$.

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

$$W_a(A) = \cup_{\mathcal{H}'} W(A \otimes I_{\mathcal{H}'}), \tag{2}$$

where $\mathcal{H}'$ ranges over all finite dimensional state spaces. One can verify by a direct calculation that

$$W_a(A) = \{\text{tr}(A\rho) : \rho \geq 0, \text{tr}(\rho) = 1\}.$$

It follows from Lemma 1 that $W_a(A) = Co(W(A)) = W(A)$ for any $A \in \mathcal{B}(\mathcal{H})$.

Suppose now we are concerned with a multipartite quantum system consisting of m parties, say, $M = \{A_1, \cdots, A_m\}$. Assume that the party A_k has a state space $\mathcal{H}_k$ with dimension d_k. Then the whole state space is given by $\mathcal{H} = \otimes_{k=1}^m \mathcal{H}_k$ with total dimension $d = d_1 \cdots d_m$. We often use $d_1 \otimes \cdots \otimes d_m$ as an abbreviation for $\mathcal{H}$. $U \in \mathcal{U}(\mathcal{H})$ is said to be local or decomposable if $U = \otimes_{k=1}^m u_k$ such that $u_k \in \mathcal{U}(\mathcal{H}_k)$. Otherwise U is nonlocal or entangled. 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,

$$W^{local}(A) = \{\langle\psi|A|\psi\rangle : |\psi\rangle = \otimes_{k=1}^m|\psi_k\rangle\}, \tag{3}$$

where $|\psi_k\rangle \in \mathcal{H}_k$ and $\langle\psi_k|\psi_k\rangle = 1$. The local entanglement-assisted numerical range $W_a^{local}(A)$ can be defined similar to $W_a(A)$. A simple observation is as follows:

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

where ρ_k is a density operator on $\mathcal{H}_k$. A rather surprising result is that local entanglement cannot broaden the local numerical range even in the multipartite scenario.

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

Proof. The proof is a simple application of Lemma 1. For simplicity, we only consider 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 $|\psi_2\rangle\langle\psi_2|$ (resp. $|\psi_1\rangle\langle\psi_1|$) 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* [21] to study the local distinguishability of nonlocal unitary operations.

Lemma 3. (Walgate *et al*, [21]): Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two multipartite orthogonal pure state on $\mathcal{H}$. Then $|\psi_1\rangle$ and $|\psi_2\rangle$ are perfectly distinguishable by LOCC.

The relation between local distinguishability of unitary operations and local numerical range now is clear. Actually, if $0 \in W^{local}(U_2^\dagger U_1)$ then there exists a product state $|\psi\rangle$ such that $U_1|\psi\rangle$ and $U_2|\psi\rangle$ are orthogonal. It follows from the above lemma that U_1 and U_2 can be perfectly distinguishable by LOCC. Conversely, suppose that U_1 and U_2 can be discriminated by LOCC, then there exists a product state $|\psi\rangle^{MM'} = \otimes_{k=1}^m |\psi_k\rangle^{A_k A_k'}$ such that $(U_1^M \otimes I^{M'})|\psi\rangle^{MM'}$ and $(U_2^M \otimes I^{M'})|\psi\rangle^{MM'}$ are orthogonal, where A_k' is a local auxiliary system of A_k. That is equivalent to $0 \in W_a^{local}(U_1^\dagger U_2)$. By Lemma 2, this is also equivalent to $0 \in W^{local}(U_1^\dagger U_2)$. Interestingly, local entanglement is not necessary for the perfect local discrimination between two unitary operations.

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

For simplicity 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 a simple application of Lemma 2, we have $\mathrm{tr}(U_1^\dagger U_2) = 0$ implies that $U_1^\dagger U_2$ has an isotropic product state. Hence U_1 and U_2 are perfectly distinguishable by LOCC with a single run.

Unfortunately, how to determine when 0 is in the local numerical range remains unknown even for unitary operations. Consequently, it is generally difficult to decide the local distinguishability of nonlocal unitary operations in the single-run scenario. Since the set of LOCC operations is very restricted, it is not clear whether nonlocal unitary operations remain locally distinguishable. Indeed, the following example demonstrates that the LOCC discrimination and the global discrimination of unitary operations are very different when only the single-run scenario is considered.

Example 1. Let U_1 and U_2 be $2 \otimes 2$ unitary operations 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 $0 < \theta_1, \theta_2 < \pi$.

On the one hand, by taking $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, we have $\langle\psi|U_1^\dagger U_2|\psi\rangle = 0$. That implies U_1 and U_2 are perfectly distinguishable by employing a maximally entangled state as input. On the other hand, we can easily verify that $U_1^\dagger U_2$ cannot have an isotropic product state, thus U_1 and U_2 are locally indistinguishable. □

The above example also demonstrates that the local numerical range is not convex in general. More precisely, we have $\pm 1 \in W^{local}(U_1^\dagger U_2)$ as one can choose $|\psi\rangle$ as $|00\rangle$ and $|11\rangle$, respectively. However, $0 = (-1+1)/2 \notin W^{local}(U_1^\dagger U_2)$. An interesting question is to ask for what kind of linear operations the local numerical range remains convex. The general answer to this question is unknown. Here we would like to point out that such a convex property does hold for Hermitian operations, for which the local numerical range is just a complex segment.

Remarkably, if we are allowed to use the unknown multipartite unitary repeatedly, then any two different multipartite unitary operations become locally distinguishable. In what follows we shall present a complete proof of this interesting fact. For the ease of presentation, the lengthy proof is divided into two parts: Theorem 2 and Theorem 3.

Some technical lemmas are necessary in order to present such a proof. The following useful lemma provides an alternative characterization of Hermitian operations.

Lemma 4. 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 $1 \le k \le d^2$.

There are many ways to choose a Hermitian basis. Here is a simple construction based on the idea of quantum process tomography [20]. Let $\{|k\rangle : 1 \le k \le d\}$ be an 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

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

is a Hermitian basis for $\mathcal{B}(\mathcal{H})$.

For a set of complex numbers $\{z_k\}$, z_ks are co-linear if there exists $0 \le \theta < 2\pi$ such that $z_k = r_k e^{i\theta}$ and $r_k \ge 0$ for any k. Geometrically, z_ks are co-linear if they lie on the same ray from the origin. The following lemma is crucial in proving our main result. Note that $\lceil x \rceil$ represents the minimum of the integers that are not less than x.

Lemma 5. For $A \in \mathcal{B}(\mathcal{H})$, let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two normalized vectors such that $\langle\psi_1|A|\psi_1\rangle = r_1 e^{i\theta_1}$ and $\langle\psi_2|A|\psi_2\rangle = r_2 e^{i\theta_2}$ are not co-linear, where $r_1, r_2 > 0$ and $0 \le \theta_1 < \theta_2 < 2\pi$. Define $\theta = \min\{\theta_2 - \theta_1, 2\pi + \theta_1 - \theta_2\}$ and $N = \lceil \frac{\pi}{\theta} \rceil$. 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. It is clear that $0 < \theta \le \pi$. To be specific, let us assume $\theta_1 = 0$ and $\theta_2 \le \pi$. Then $\theta = \theta_2$. We deal with the following two cases separately:

Case 1: $\theta = \pi$. In this case we have $N = 1$. Choose $0 \le p \le 1$ such that $pr_1 - (1-p)r_2 = 0$. Then we have $p\langle\psi_1|A|\psi_1\rangle + (1-p)\langle\psi_2|A|\psi_2\rangle = 0$. By Lemma 1, $0 \in W(A)$.

Case 2: $0 < \theta < \pi$. It is obvious that $N\theta < 2\pi$. Define $|\Phi_k\rangle = |\psi_1\rangle^{\otimes N-k}|\psi_2\rangle^{\otimes k}, 0 \le k \le N$ and $z_k =$

$\langle\Phi_k|A^{\otimes N}|\Phi_k\rangle$. We shall show that $0\in Co\{z_k : 0\leq k\leq N\}$. A routine calculation shows that

$$z_k = r_1^{N-k}r_2^k e^{ik\theta}. \tag{4}$$

To complete the proof in this case, it suffices to consider the following two subcases:

Case 2a: $N\theta=\pi$. Then we have $e^{iN\theta}=-1$. Similar to Case 1, we can choose $0\leq p\leq 1$ such that $pr_1^N-(1-p)r_2^N=0$, which immediately follows that $pz_0+(1-p)z_N=0$. By Lemma 1, $0\in W(A^{\otimes N})$.

Case 2b. $\pi<N\theta<2\pi$. By the assumption on N, we should have $N\geq 2$ and $N\theta-\pi<(N-1)\theta<\pi$. These conditions imply that for any positive real numbers s_1, s_2, s_3 we have $0\in Co\{s_1, s_2e^{i(N-1)\theta}, s_3e^{iN\theta}\}$. By Eq. (4), there exists p_1, p_2, p_3 such that

$$p_1z_0+p_2z_{N-1}+p_3z_N=0,$$

where $\sum_{k=1}^3 p_k=1$ and $p_k\geq 0$. Again, by Lemma 1, we have $0\in W(A^{\otimes N})$.

In all the above cases, by the second part of Lemma 1, the state $|\psi\rangle$ such that $\langle\psi|A^{\otimes N}|\psi\rangle=0$ can be chosen as a linear combination of $|\Phi_k\rangle$. □

With Lemma 5 in hand, we can show in the following theorem that perfect discrimination between two multipartite unitary operations U_1 and U_2 by a parallel scheme is always possible except for a special case.

Theorem 2. Let U_1 and U_2 be two multipartite unitary operations such that $U_1^\dagger U_2$ is non-Hermitian (up to some phase factor). Then there exists a finite N such that $0\in W^{local}((U_1^\dagger U_2)^{\otimes N})$. That is, $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable using LOCC.

Proof. We only need to seek a finite N and a product state $|\psi\rangle$ such that $\langle\psi|(U_1^\dagger U_2)^{\otimes N}|\psi\rangle=0$. To simplify the notations, we consider only the case when U_1 and U_2 both are bipartite unitary operations acting on $\mathcal{H}_1\otimes\mathcal{H}_2$. The general case can be proved similarly. Let $\{|\psi_k\rangle\langle\psi_k|\}$ and $\{|\varphi_l\rangle\langle\varphi_l|\}$ be Hermitian basis for $\mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B}(\mathcal{H}_2)$, respectively. Then $\{|\psi_k\varphi_l\rangle\langle\psi_k\varphi_l|$ is a Hermitian basis for $\mathcal{B}(\mathcal{H}_1\otimes\mathcal{H}_2)$, where $1\leq k\leq d_1^2$ and $1\leq l\leq d_2^2$.

Consider $d_1^2d_2^2$ complex numbers

$$z_{kl}=\langle\psi_k\varphi_l|U_1^\dagger U_2|\psi_k\varphi_l\rangle.$$

If all z_{kl} are co-linear, then $z_{kl}=r_{kl}e^{i\theta}$ for some $\theta\in\mathcal{R}$ and $r_{kl}\in\mathcal{R}$. Thus all $e^{-i\theta}z_{kl}$s are real. By Lemma 4, $e^{-i\theta}U^\dagger V$ is Hermitian. That contradicts our assumption. So there should exist $(k,l)\neq(p,q)$ such that z_{kl} and z_{pq} are not co-linear. More precisely, let $z_{kl}=r_{kl}e^{i\theta_{kl}}$ and $z_{pq}=r_{pq}e^{i\theta_{pq}}$, where $r_{kl}, r_{pq}>0$ and $0\leq\theta_{kl},\theta_{pq}<2\pi$. We should have $\theta_{kl}\neq\theta_{pq}$. Consider the value of z_{kq}. If $z_{kq}=0$ then we can choose $|\psi\rangle=|\psi_k\varphi_l\rangle$ and the proof is finished. Otherwise, write $z_{kq}=r_{kq}e^{i\theta_{kq}}$, where $r_{kq}>0$ and $0\leq\theta_{kq}<2\pi$. Since $\theta_{kl}\neq\theta_{pq}$, we should have either $\theta_{kq}\neq\theta_{kl}$ or $\theta_{kq}\neq\theta_{pq}$. Without loss of generality, let us assume $\theta_{kq}\neq\theta_{pq}$. By Lemma 5, there exists a finite N such that $0\in W((U_1^\dagger U_2)^{\otimes N})$. And the isotropic state $|\psi\rangle$ can be chosen as a linear combination of the states

$$|\Phi_n\rangle=|\psi_k\varphi_q\rangle^{\otimes N-n}|\psi_p\varphi_q\rangle^{\otimes n},\ 0\leq n\leq N.$$

A key observation here is that any vector from $span\{|\Phi_n\rangle : 0\leq n\leq N\}$ is of the form $|\psi'\rangle\otimes|\varphi_q\rangle^{\otimes N}$, where $|\psi'\rangle\in\mathcal{H}_1^{\otimes N}$ and $|\varphi_q\rangle^{\otimes N}\in\mathcal{H}_2^{\otimes N}$. That is, $|\psi\rangle$ can be taken as a product state. □

It is worth noting that in the above proof only one party is required to prepare local entanglement.

However, the local discrimination between U_1 and U_2 such that $U_1^\dagger U_2$ is Hermitian has not been involved yet. Noticing that $U_1^\dagger U_2$ is Hermitian, we may write $U^\dagger V=I-2P$, where P is a projector satisfying $\mathrm{tr}(P)<\mathrm{tr}(I)/2$. The only left case for $2\otimes 2$ is that $U_1^\dagger U_2=I_{\mathcal{H}}-2|\Phi\rangle\langle\Phi|$ for some state $|\Phi\rangle\in\mathcal{H}$. Assume $|\Phi\rangle=\sqrt{\lambda}|00\rangle+\sqrt{1-\lambda}|11\rangle$ for some $1/2\leq\lambda\leq 1$. Then we have $\langle 00|U_1^\dagger U_2|00\rangle=1-2\lambda\leq 0$. On the other hand, we have that $\mathrm{tr}(U^\dagger V)=2>0$. By the convexity of $W^{local}(U_1^\dagger U_2)$, we have $0\in W^{local}(U_1^\dagger U_2)$. Combining this with Theorem 2 we obtain the following interesting result:

Corollary 1. Let U_1 and U_2 be two different $2\otimes 2$ unitary operations. Then there exists a finite N such that $0\in W^{local}((U_1^\dagger U_2)^{\otimes N})$.

In other words, any two $2\otimes 2$ unitary operations can be locally distinguishable by a parallel scheme.

In general, we can transform the case when $U_1^\dagger U_2$ is Hermitian to the non-Hermitian case by applying a sequential scheme. The following Lemma would be helpful in doing this transformation.

Lemma 6. Let A and B be two 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 be a function defined on the set of local unitary operations such that $f(u)=\mathrm{tr}(u^\dagger AuB)$. Then for Hermitian operations A and B, $f(u)\in\mathcal{R}$. 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 A and $uBu^\dagger$ are simultaneously diagonalizable under some unitary operation. Thus $f(u)=\mathrm{tr}(u^\dagger AuB)$ 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. Thus $f(u)$ can take at most $d!$ possible values and should be a constant C for any local unitary u. To calculate C explicitly, let us choose a set of local unitary operations $\{u_k : k=1,\cdots,d^2\}$ on $\mathcal{H}$ such that the following identity holds:

$$1/d^2\sum_{k=1}^{d^2}u_k^\dagger Au_k=\mathrm{tr}(A)I_{\mathcal{H}}/d, \tag{5}$$

where A is an arbitrary linear operation on $\mathcal{H}$. Intuitively, Eq. (5) represents the completely depolarizing channel on $\mathcal{B}(\mathcal{H})$. Such local unitary operations do exist. For instance, one may choose $\{u_k\}$ as the tensor products of the generalized Pauli matrices acting on $\mathcal{H}_l$. It follows that

$$1/d^2 \sum_{k=1}^{d^2} u_k^\dagger A u_k B = \mathrm{tr}(A)B/d. \qquad (6)$$

Taking trace and noticing that $\mathrm{tr}({u_k}^\dagger A u_k B) = C$ for any $1 \leq k \leq d^2$, we have $C = \mathrm{tr}(A)\mathrm{tr}(B)/d$. With that we complete the proof of Lemma 6. □

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 (up to some phase factor). Then there exists a finite $n > 1$ and a sequence of local unitary operations $u^{(1)}, \cdots, u^{(n-1)}$ such that $W_1^\dagger W_2$ is non-Hermitian, where $W_1 = U_1 u^{(1)} \cdots u^{(n-1)} U_1$ and $W_2 = U_2 u^{(1)} \cdots u^{(n-1)} U_2$.

Proof. Without any loss of generality, we may assume that $U_1^\dagger U_2 = D$ for some Hermitian D. It is worth noting that $D = I - 2P$ for some projector P. Hence we can assume that $\mathrm{tr}(D)$ is a positive integer strictly less than d. By contradiction, suppose that for any $n > 1$ and any local unitary operations $u^{(1)}, \cdots, u^{(n-1)}$, we have that $W_1^\dagger W_2$ is Hermitian. Let $D^{(n)} = (U_1^n)^\dagger U_2^n$. We shall prove that

$$\mathrm{tr}(D^{(n)}) = (\mathrm{tr}(D)/d)^{n-1}\mathrm{tr}(D), \; n \geq 1. \qquad (7)$$

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

$$(U^{n-1} u U_1)^\dagger (U_2^{n-1} u U_2) = U_1^\dagger [u^\dagger D^{(n-1)} u U_1 D U_1^\dagger] U_1 \quad (8)$$

is Hermitian for any local unitary u. Applying Lemma 6 and setting $u = I_{\mathcal{H}}$ we have

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

More explicitly,

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

Solving this relation we complete the proof of Eq. (7).

However, Eq. (7) cannot be true for all $n > 1$. More precisely, since $\mathrm{tr}(D) < d$, it is obvious that $\mathrm{tr}(D^{(n)})$ is a strictly decreasing sequence with respect to n. Therefore for some suitable n we should have $0 < \mathrm{tr}(D^{(n)}) < 1$, which contradicts the fact that $\mathrm{tr}(D^{(n)})$ is a positive integer. □

In summary, we consider the discrimination between multipartite unitary operations by local quantum operations and classical communications only, and show that a perfect discrimination in this scenario is always possible. There are numerous open problems. For example, it remains unsolved whether a perfect discrimination can be achieved by merely a parallel scheme or a sequential scheme. Another challenging problem is to determine the minimal number of the runs needed for a perfect discrimination between two multipartite unitary operations in the LOCC scenario. Similar problems have been completely solved in the global scenario [2, 3, 4].

We thank Z.-F. Ji, G.-M. Wang, J.-X. Chen, Z.-H. Wei, and C. Zhang for helpful conversations. This work was partly supported by the Natural Science Foundation of China (Grant Nos. 60621062 and 60503001) and the Hi-Tech Research and Development Program of China (863 project) (Grant No. 2006AA01Z102).

* Electronic address: dry@tsinghua.edu.cn
† Electronic address: feng-y@tsinghua.edu.cn
‡ Electronic address: 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).
[3] G. M. D'Ariano, P. LoPresti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).
[4] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **98**, 100503 (2007).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] J. Oppenheim and B. Reznik, Phys. Rev. A **70**, 022312 (2004).
[7] S. Mozes, J. Oppenheim, and B. Reznik, Phys. Rev. A **71**, 012311 (2005).
[8] A. Chefles, Physical Review A **64**, 062305 (2001).
[9] K.M.R. Audenaert, J. Calsamiglia, Ll. Masanes, R. Munoz-Tapia, A. Acín, E. Bagan, and F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007).
[10] A. Chefles and M. Sasaki, Phys. Rev. A. 67 032112 (2003).
[11] A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley, quant-ph/0702245.
[12] M. F. Sacchi Phys. Rev. A 71, 062337 (2005).
[13] G. Wang and M. Ying, Phys. Rev. A 73 042301 (2006).
[14] Z. F. Ji, Y. Feng, R. Y. Duan, and M. S. Ying, Phys. Rev. Lett. **96**, 200401 (2006).
[15] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000).
[16] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[17] G. Vidal, K. Hammerer, and J. I. Cirac, Phys. Rev. Lett. **88**, 237902 (2002).
[18] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, and D. Mortimer, Phys. Rev. A **67**, 052301 (2003).
[19] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Combridge University Press, Cambridge, 1991.
[20] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997).

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