Local Unambiguous Discrimination with Remaining Entanglement

Yangjia Li,[1, *] Runyao Duan,[1, †] and Mingsheng Ying[1, ‡]

[1]*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, NSW 2007, Australia

(Dated: December 28, 2009)

A bipartite state which is secretly chosen from a finite set of known entangled pure states cannot be immediately useful in standard quantum information processing tasks. To effectively make use of the entanglement contained in this unknown state, we introduce a new way to locally manipulate the original quantum system: either identify the state successfully or distill some pure entanglement. Remarkably, if many copies are available, we show that any finite set of entangled pure states, whatever orthogonal or not, can be locally distinguished in this way, which further implies that pure entanglement can be deterministically extracted from unknown pure entanglement. These results make it clear why a large class of entangled bipartite quantum operations including unitary operations and measurements that are globally distinguishable can also be locally distinguishable: they can generate pure entanglement consistently.

PACS numbers: 03.67.Ac, 03.67.Hk, 03.65.Ta

I. INTRODUCTION AND MAIN RESULTS

How to identify an unknown system which is secretely chosen from a finite set of pre-specified states is one of the basic problems in information theory. In quantum mechanics, it becomes more interesting since perfect discrimination can't be achieved for nonorthogonal states. In most cases, unambiguous discrimination is generally effective, unless these states are linearly dependent [1]. The problem is also considered when the unknown system is shared by some physically separated parties and only local operations on each party and classical communication between them (LOCC) is allowed during the process [2]. Things get quite different in the local discrimination. When there are only two different states, the results are simple: the successful probability can be always achieved optimally for both of orthogonal case [3] and nonorthogonal case [4]. However, for more than two states, the problem becomes very complicated. One surprising example is that some orthogonal product states can't be perfect distinguished locally [5]. Another one is that any orthogonal basis which is unambiguously distinguishable by LOCC must be a product basis [6]. On the other hand, there are also some positive results discovered such as Ref. [7] and Ref. [8]

Up to now, all things considered in the above researches is how to get classical information from the unknown system. When the process is finished, the original system would be simply discard. Thus, if the discrimination is failed, nothing can be obtained from it. It is actually assumed that the only useful thing contained in this system is distinguishability. However, this assumption doesn't conform to the fact when people distinguish between entangled states using only LOCC. In this scenario, the entanglement contained in the system becomes a kind of nonclassical information, which plays indispensable roles in standard quantum information processing tasks such as superdense coding [9] and teleportation [10]. In fact, discrimination of different states is often employed as some steps of complicated physical tasks. Preserving as much entanglement as possible in each of these steps will bring a lot of convenience for the whole tasks in practice. Thus, a right choice here is to optimally make use of the entanglement contained in the original quantum system, instead of ignoring it.

One possible strategy of doing this is to directly extract the entanglement before discrimination and to treat it as an independent quantum task. In this case, such a quantum task is equivalent to distill pure entanglement from a arbitrarily given entangled mixed state, which is known as entanglement distillation [11] in standard quantum information processing tasks. Unfortunately, this task is very difficult in general and most of the existing distillation protocols which are effective for mixed states only work in the asymptotic regime [11, 12, 13, 14]. It means that the

*Electronic address: liyangjia@gmail.com
†Electronic address: Runyao.Duan@uts.edu.au
‡Electronic address: yingmsh@tsinghua.edu.cn

target entanglement won't become exactly pure unless the source entanglement goes to infinite. It is still unclear how to do this in finite regime.

What we proposed in this paper is actually another strategy which seems more effective than the above one: we perform the entanglement distillation as a part of our new discrimination. The idea is that when discrimination is failed, we make the different states become the same in the output. More important, entanglement will remain in this outcome state while it would normally be destroyed in traditional discrimination protocols. We noticed that some preliminary works on preserving entanglement in the local discrimination of orthogonal entangled states have been discussed [15]. However, these works are not applicable for nonorthogonal states. Another advantage of our method is that the original quantum system is always useful whether it is successfully identified or not. Formally, we propose the following:

Definition 1. A set of bipartite pure states $\{|\psi_1\rangle, \cdots, |\psi_n\rangle\}$ is said to be *unambiguously distinguishable with remaining entanglement*(UDRE) via LOCC if there is a local measurement $\{M_s, M_f\}$ such that i) $\{M_s|\psi_k\rangle\}$ are locally distinguishable with certainty; ii) $M_f|\psi_k\rangle \equiv |\eta\rangle$ for some bipartite entangled state $|\eta\rangle$, where the subscripts "s" and "f" represent the successful and the failed outcomes of discrimination, respectively. Note that we write $|\alpha\rangle \equiv |\beta\rangle$ if there is scalar λ such that $|\alpha\rangle = \lambda|\beta\rangle$.

Clearly, any two orthogonal pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ are locally UDRE [3]. However, if nonorthogonal or more than two states are involved, the situation becomes quite complicated. For instance, it is not difficult to show that any two nonorthogonal or three orthogonal $2 \otimes 2$ pure entangled states cannot be distinguishable in this way. It is also easy to see that two nonorthogonal pure states containing at least one product state cannot be UDRE (Actually from the remaining entangled state we can infer that the original state should be entangled and thus achieve a perfect discrimination, which is a contradiction with the nonorthogonality).

For $2\otimes 3$ states there do exist nonorthogonal pure states which can be distinguished via UDRE. An explicit example is given as follows:

$$\begin{aligned}|\psi_0\rangle &= (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |0\rangle_A|2\rangle_B)/\sqrt{3},\\ |\psi_1\rangle &= (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |1\rangle_A|2\rangle_B)/\sqrt{3}.\end{aligned}$$

A simple protocol is as follows: Bob performs a measurement $\{|0\rangle\langle 0| + |1\rangle\langle 1|, |2\rangle\langle 2|\}$. If the outcome is 2 then Alice only needs to perform the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ to complete the discrimination. Otherwise the discrimination is failed and they are left with an entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$.

It is still unknown when a set of states can be locally UDRE. Interestingly, if multiple copies are available, we find that any finite number of bipartite pure entangled states can be distinguished in this way.

Theorem 1. Let $|\psi_1\rangle, \cdots, |\psi_n\rangle$ be any n bipartite entangled pure states in $\mathcal{H}_A \otimes \mathcal{H}_B$. Then there is always an integer N such that $|\psi_1\rangle^{\otimes N}, \cdots, |\psi_n\rangle^{\otimes N}$ are UDRE.

As a direct consequence, we have the following

Theorem 2. Let $|\psi_1\rangle, \cdots, |\psi_n\rangle$ be any n bipartite entangled pure states on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then there is always an integer N and an LOCC protocol $\mathcal{E}$ such that $\mathcal{E}(\psi_k^{\otimes N}) = |\Phi_0\rangle\langle\Phi_0|$ for any $1 \le k \le N$, where $|\Phi_0\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$.

The above theorem has a clear physical meaning: one can use LOCC to deterministically distill an Einstein-Podolsky-Rosen (EPR) state [16] of form $|\Phi_0\rangle$ from the following of mixed state

$$\rho(N) = \sum_{i=1}^{n} p_i[|\psi_i\rangle\langle\psi_i|]^{\otimes N},$$

where $p_i \ge 0$ and $\sum_{i=1}^n p_i = 1$. For $n = 1$, it is a special case of the fundamental result in entanglement transformation [17]. However, our generalization here brings it to a essentially different level since the source entanglement becomes mixed. This distillation protocol for mixed states works in finite regime and succeed with probability one. Compared with traditional distillation protocols, it has two remarkable advantages: first, both of the amount of source entanglement and the number of runs of LOCC can be bounded before execution; second, without statistical fluctuation, the result is more faithful and reliable. Although only states of form $\rho(N)$ is given in our distillation protocol, it works for all UDRE states.

II. PROOF OF THEOREM 1

We will now provide a complete proof to Theorem 1. To make our arguments more readable, we first consider the case of $n = 2$ and then generalize the result to the case where $n > 2$.

Suppose the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ are d' and d, respectively, and $d' \geq d \geq 2$. Let us assume one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is of full Schmidt number at Bob's side. Later in Appendix 1 we will show this assumption can be removed. To be specific, suppose that $|\psi_2\rangle$ is with the Schmidt decomposition as follows:

$$|\psi_2\rangle = \sum_{i=0}^{d-1} \sqrt{\lambda_i}|i_A i_B\rangle, \text{ where } \lambda_i > 0, 0 \leq i \leq d-1. \tag{1}$$

Let us emphasize that $\{|i\rangle_B : 0 \leq i \leq d-1\}$ is an orthonormal basis of $\mathcal{H}_B$ and $\{|i\rangle_A : 0 \leq i \leq d-1\}$ is a set of orthonormal vectors of $\mathcal{H}_A$. Let $\lambda_{\min} = \min\{\lambda_i : 0 \leq i \leq d-1\}$. A key property of full Schmidt rank state is the following:

Lemma 1. Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two bipartite pure states on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $|\psi_2\rangle$ is of full Schmidt rank at Bob's side. Then there is a linear operator M_A such that $(M_A \otimes I_B)|\psi_2\rangle = |\psi_1\rangle$ and $M_A^\dagger M_A \leq \lambda_{\min}^{-1} I_A$.

Proof. Note that $|\psi_1\rangle$ can be uniquely decomposed as $|\psi_1\rangle = \sum_{i=0}^{d-1} |\alpha_i\rangle|i\rangle_B$, where $\{|i\rangle_B : 0 \leq i \leq d-1\}$ is the same as in Eq. (1) and $\{|\alpha_i\rangle : 0 \leq i \leq d-1\}$ is a set of (unnormalized) vectors on $\mathcal{H}_A$. Let $M_A = \sum_{i=0}^{d-1} \lambda_i^{-1/2}|\alpha_i\rangle\langle i_A|$. One can readily verify that M satisfies our requirements. ■

The following lemma provides a sufficient condition for UDRE.

Lemma 2. Let $|\alpha\rangle$ and $|\beta\rangle$ be two states on an auxiliary system $\mathcal{H}_{A'}$ of Alice. Then $|\alpha\rangle_{A'}|\psi_1\rangle_{AB}$ and $|\beta\rangle_{A'}|\psi_2\rangle_{AB}$ are locally unambiguously distinguishable with remaining entanglement $|\alpha\rangle_{A'}|\psi_1\rangle_{AB}$ if $|\langle\alpha|\beta\rangle| \leq \sqrt{\lambda_{\min}/(1+\lambda_{\min})}$.

Proof. Let us write $|\alpha\rangle = |0\rangle$ and $|\beta\rangle = u|0\rangle + v|1\rangle$, where $u = \langle\alpha|\beta\rangle$. By a simple algebraic calculation we have $|u/v| \leq \sqrt{\lambda_{\min}}$. We are now seeking for a linear operator $O_{A'A}$ such that i) $O^\dagger O \leq I_{A'A}$; ii) $O|0\rangle_{A'}|i\rangle_A = |0\rangle_{A'}|i\rangle_A/\sqrt{2}$, $0 \leq i \leq d-1$; and iii) $(O_{A'A} \otimes I_B)|1\rangle_{A'}|\psi_2\rangle = 1/\sqrt{2}(u/v)|0\rangle_{A'}(2\langle\psi_1|\psi_2\rangle|\psi_1\rangle - |\psi_2\rangle)$.

If such a linear operator $O_{A'A}$ exists, we can construct a local measurement $\{M_s, M_f\}$ such that $M_f = O_{A'A} \otimes I_B$ and $M_s = \sqrt{I_{A'A} - O^\dagger O} \otimes I_B$. It is quite straightforward to verify that such a local measurement can achieve a UDRE.

Consider the following linear operator

$$O = 1/\sqrt{2}|0\rangle\langle 0|_{A'} \otimes I_A + 1/\sqrt{2}|0\rangle\langle 1|_{A'} \otimes (u/v)M_A,$$

where M is a linear operator such that $(M_A \otimes I_B)|\psi_2\rangle = (2\langle\psi_1|\psi_2\rangle|\psi_1\rangle - |\psi_2\rangle)$ and $M_A M_A^\dagger \leq \lambda_{\min}^{-1} I_A$. The existence of M follows directly from Lemma 1. Clearly, by construction conditions ii) and iii) are automatically satisfied. The validity of condition i) follows from the observation $OO^\dagger = 1/2|0\rangle\langle 0|\otimes I_A + 1/2|0\rangle\langle 0|\otimes(u/v)^2 MM^\dagger \leq |0\rangle\langle 0|\otimes I_A$. ■

What is missing in Lemma 2 is how to construct the auxiliary system A' used on the Alice's part when the given state is $\rho(N)$. Our idea is to transform the state $|\psi_1\rangle^{\otimes N_0}$ (resp. $|\psi_2\rangle^{\otimes N_0}$) to $|\alpha\rangle$ (resp. $|\beta\rangle$) for some N_0, and then system A' can be constructed from these N_0 copies. The following lemma plays a key role.

Lemma 3. There exists an orthonormal basis $\{|e_i\rangle : 0 \leq i \leq d-1\}$ of $\mathcal{H}_B$ such that

$$\begin{aligned} |\psi_1\rangle_{AB} &= \sum_{i=0}^{d-1} a_i|\alpha_i\rangle_A|e_i\rangle_B, \ \langle\alpha_i|\alpha_i\rangle = 1, \\ |\psi_2\rangle_{AB} &= \sum_{i=0}^{d-1} b_i|\beta_i\rangle_A|e_i\rangle_B, \ \langle\beta_i|\beta_i\rangle = 1, \end{aligned}$$

and $|\langle\alpha_i|\beta_i\rangle| < 1$ for each $0 \leq i \leq d-1$. In particular, $(|\psi_1\rangle_{AB}, |\psi_2\rangle_{AB})$ can be transformed into $(|\alpha\rangle_A, |\beta\rangle_A)$ by a local operation, where $\langle\alpha|\beta\rangle = \max\{|\langle\alpha_i|\beta_i\rangle| : 0 \leq i \leq d-1\} < 1$.

Proof. For the case of $d = 2$, we can choose $\{|e_0\rangle, |e_1\rangle\}$ to be one of the following three bases: $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$, and $\{\frac{4}{5}|0\rangle + \frac{3}{5}|1\rangle, \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle\}$.

Now we start to consider the general case $d > 2$. Let us start with the basis $|e_i\rangle = |i\rangle_B$ which gives the Schmidt decomposition of $|\psi_2\rangle$. That is, $\langle\alpha_i|\alpha_j\rangle = \delta_{ij}$. Let $I_1 = \{0 \leq i \leq d-1 : |\alpha_i\rangle \equiv |\beta_i\rangle\}$. If $I_1 = \emptyset$ then we have done. Otherwise we have the following two cases:

Case 1. $I_1 = \{0, \cdots, d-1\}$. In this case $|\psi_1\rangle$ and $|\psi_2\rangle$ are simultaneously Schmidt decomposable. Let us define a new basis $|e'_i\rangle_B = 1/\sqrt{d}\sum_{j=0}^{d-1} \omega^{ij}|e_j\rangle_B$, where $\omega = e^{2\pi i/d}$ is the d-th root of unity. Then we have $|\alpha'_i\rangle_A = \sum_{i=0}^{d-1} \omega^{ij} a_i|\alpha_i\rangle_A$ and $|\beta'_i\rangle_A = \sum_{i=0}^{d-1} \omega^{ij} b_i|\beta_i\rangle_A$. One can readily verify that $\langle\alpha'_i|\beta'_i\rangle = \langle\psi_1|\psi_2\rangle$. That completes our proof in this case.

Case 2. $I_1 \subsetneqq \{0,\cdots,d-1\}$. To be specific, assume that $|\alpha_0\rangle \equiv |\beta_0\rangle$ and $|\alpha_1\rangle \not\equiv |\beta_1\rangle$. Then consider the following two sub-vectors of $|\psi_1\rangle$ and $|\psi_2\rangle$:

$$\begin{aligned} |\psi_1'\rangle &= a_0|\alpha_0\rangle_A|e_0\rangle_B + a_1|\alpha_1\rangle_A|e_1\rangle_B, \\ |\psi_2'\rangle &= b_0|\beta_0\rangle_A|e_0\rangle_B + b_1|\beta_1\rangle_A|e_1\rangle_B. \end{aligned}$$

Applying the result for $d=2$ we know that there is an orthonormal basis $\{|e_0'\rangle_B, |e_1'\rangle_B\}$ of $span\{|e_0\rangle_B, |e_1\rangle_B\}$ such that $\langle e_0'|\psi_1'\rangle \not\equiv \langle e_0'|\psi_2'\rangle$ and $\langle e_1'|\psi_1'\rangle \not\equiv \langle e_1'|\psi_2'\rangle$. Thus under the new basis $\{|e_0'\rangle_B, |e_1'\rangle_B, |e_2\rangle_B, \cdots, |e_{d-1}\rangle_B\}$, we have $I_1' = I_1 - \{0\} \subsetneqq I_1$. Repeating this process at most $d-1$ times we can finally have $I_1 = \emptyset$. ■

For $|\alpha\rangle$ and $|\beta\rangle$ in the above lemma, we can choose a positive integer N_0 such that

$$|\langle\alpha|\beta\rangle|^{N_0} \leq \sqrt{\frac{\lambda_{\min}}{1+\lambda_{\min}}}.$$

Then it follows from Lemma 2 that

Corollary 1. $|\psi_1\rangle^{\otimes(N_0+1)}$ and $|\psi_2\rangle^{\otimes(N_0+2)}$ are locally unambiguously distinguishable with remaining entangled state $|\psi_2\rangle$.

This completes the proof of Theorem 1 for the case where $k=2$ and one of $|\psi_1\rangle$ and $|\psi_2\rangle$ has full Schmidt number. The proof for the most general case is somewhat involved and is given in Appendix 1.

III. APPLICATIONS TO THE LOCAL IDENTIFICATION OF QUANTUM MEASUREMENTS

We will employ Theorem 2 to study the local identification of quantum operations, which formalize all physically realizable operations in quantum mechanics [19]. Recently the problem of distinguishing quantum operations has attracted a lot of attentions. Many interesting results have been reported [20, 21, 22, 23, 24]. It was shown that perfect identification can be achieved for unitary operations [20] and projective measurements [21]. A necessary and sufficient condition for the perfect distinguishability of quantum operations has been discovered quite recently [24]. An important generalization of this problem is to consider the identification of a bipartite unknown quantum operation using LOCC only, which seems much more complicated than the global setting. Surprisingly, it has been shown that the perfect discrimination between unitary operations is always possible even under LOCC [25]. However, the local distinguishability of general quantum operations remains unknown so far.

Here we consider the identification of bipartite quantum measurements. We will employ a new strategy different from that in [25], i.e., we will reduce the LOCC discrimination problem to the global case by generating pure bipartite entanglement using the known apparatus. Applying our result about deterministic distillation, we can generate a sufficiently large number of EPR pairs between Alice and Bob, and thus accomplish the local perfect discrimination by teleportation and global protocol. This motivates us to introduce the following

Definition 2. Two quantum measurements $\mathcal{M}_0 = (M_{01},\cdots,M_{0n_0})$ and $\mathcal{M}_1 = (M_{11},\cdots,M_{1n_1})$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ are said to be *consistently entangled*, if there exists $|\alpha\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_A$ and $|\beta\rangle \in \mathcal{H}_{B'} \otimes \mathcal{H}_B$ such that $(I_{A'} \otimes I_{B'} \otimes M_{ik})|\alpha\rangle_{A'A}|\beta\rangle_{B'B}$ is entangled or vanished for $1 \leq i \leq n_k$ and $k=0,1$, where A' and B' are auxiliary systems.

It follows immediately from Theorem 2 that bipartite pure entanglement can be extracted by a finite number of runs of an unknown operation $\mathcal{M}$ which is secretely chosen from two consistently entangled measurements $\mathcal{M}_0$ and $\mathcal{M}_1$. So if $\mathcal{M}_0$ and $\mathcal{M}_1$ are perfectly distinguishable by global quantum operations, then they are also perfectly distinguishable by LOCC.

If we focus our attention on the identification of two bipartite projective measurements $\mathcal{M}_0 = \sum_{i=1}^{l} iP_i$ and $\mathcal{M}_1 = \sum_{j=1}^{l} jQ_j$ and apply the fact that any two projective measurements are identifiable by global operations [21], we have the following results about the local distinguishability of consistently entangled projective measurements.

Lemma 4. If $\mathcal{M}_0$ and $\mathcal{M}_1$ are consistently entangled bipartite projective measurements, then they are perfectly distinguishably by LOCC.

Unfortunately, for $\mathcal{M}_0$ and $\mathcal{M}_1$ that may not be consistently entangled, the local distinguishability remains unknown. Nevertheless, we still have the following sufficient condition. The proof of this result is somewhat tricky and is put in Appendix 2.

Lemma 5. Two projective measurements $\mathcal{M}_0$ and $\mathcal{M}_1$ can be perfectly distinguished by LOCC if for some $k \in \{1,2,\cdots,l\}$ there is a product state in the supports of P_k or Q_k but not in their intersection.

To describe the above two identifiable cases in a more unified way, we will employ the notion of Unextendible Product Bases (UPB) [26]. A UPB is a set of orthogonal product pure states which cannot be further extended by adding any additional orthogonal product state. The notion of UPB is very important as it can be used to construct bound entanglement or to demonstrate the weird phenomenon "quantum nonlocality without entanglement" [8]. It can also be used to construct interesting examples in quantum information theory [27]. In addition, we need to introduce the notion of *Unextendible Product Part* (UPP). Let W be a set of product states $|\alpha\beta\rangle$ such that $|\alpha\beta\rangle$ is in the intersection of the supports of P_k and Q_k for some k. That is,

$$W = \{|\alpha\beta\rangle : |\alpha\beta\rangle \in supp(P_k) \cap supp(Q_k) \text{ for some } k\}.$$

A subset X of W is said to be a (orthogonal) *Product Part* (PP) of $\mathcal{M}_0$ and $\mathcal{M}_1$, if any two states in X are orthogonal. A PP is called a UPP if it can be a proper subset of any other PP.

Theorem 3. $\mathcal{M}_0$ and $\mathcal{M}_1$ are perfectly distinguishable if they have a UPP which is not a UPB.

Proof. Let Y be such a UPP. Notice that $|Y| < dim(\mathcal{H}_A \otimes \mathcal{H}_B)$ as $\mathcal{M}_0$ and $\mathcal{M}_1$ are different. Since Y is not a UPB, there is a product state $|\alpha\beta\rangle$ in the orthogonal complement of Y. If for every k, both $P_k|\alpha\beta\rangle$ and $Q_k|\alpha\beta\rangle$ are not product states, then we can identify $\mathcal{M}$ according to Corollary 4. Otherwise, without loss of generality, we can assume that $P_k|\alpha\beta\rangle = \lambda|\gamma\eta\rangle(\lambda \neq 0)$ is a product state. Then $|\gamma\eta\rangle$ is in the support of P_k as $P_k|\gamma\eta\rangle = P_kP_k|\alpha\beta\rangle = P_k|\alpha\beta\rangle = |\gamma\eta\rangle$. We claim that $|\gamma\eta\rangle$ is not in the support of Q_k, and then the identifiability of $\mathcal{M}$ follows immediately from Lemma 5. In fact, if it is not the case, then $|\gamma\eta\rangle$ is in the both supports of P_k and Q_k. Thus, $Y \cup \{|\gamma\eta\rangle\}$ is a PP which strictly includes Y. This contradicts our assumption that Y is a UPP. ■

If the dimension of one part of a bipartite system is 2, then any UPP of $\mathcal{M}_0$ and $\mathcal{M}_1$ cannot be a UPB as there is no UPB for $2 \otimes n$ quantum system [26]. So we have:

Theorem 4. Any two projective measurements acting on $2 \otimes n$ are perfectly distinguishable by LOCC.

However, there does exists two locally indistinguishable bipartite projective measurements if the dimension of each subsystem is not less than 3. This is essentially due to the existence of UPB for these quantum systems [26]. Let $\{|\alpha_i\rangle_A|\beta_i\rangle_B\}_{i=1}^l$ be a UPB and $P = \sum_{i=1}^l |\alpha_i\beta_i\rangle\langle\alpha_i\beta_i|$. Partition $I_{AB} - P$ into two nontrivial orthogonal projectors Q_1 and Q_2. Then we claim that the following two bipartite projective measurements

$$\begin{aligned}
\mathcal{M}_0 &= \sum_{i=1}^l i|\alpha_i\beta_i\rangle\langle\alpha_i\beta_i| + (l+1)(I-P),\\
\mathcal{M}_1 &= \sum_{i=1}^l i|\alpha_i\beta_i\rangle\langle\alpha_i\beta_i| + (l+1)Q_1 + (l+2)Q_2
\end{aligned}$$

cannot be perfectly distinguishable using LOCC. Actually, due to the property of UPB, $\mathcal{M}_0$ and $\mathcal{M}_1$ will yield an outcome $r \in \{1, \cdots, l\}$ with nonzero probability on any product input state. This makes further perfect discrimination impossible as both output states are $|\alpha_r\beta_r\rangle$.

IV. CONCLUSION

In this paper, we have considered the problem of how to effectively manipulate a quantum system whose state is secretely chosen from a set of nonorthogonal bipartite pure entangled states. Our idea is to distill some pure entanglement when the discrimination is failed. Then the notion of *Unambiguous Discrimination with Remaining Entanglement* has been introduced to describe such a discrimination protocol. We have shown that an unknown state which belongs to a finite set of bipartite pure entangled states $\{|\psi_i\rangle^{\otimes N}\}$ can be locally distinguished via UDRE for some sufficiently large N. This discrimination protocol is then used to construct exact and deterministic entanglement distillation protocols. Most interestingly, a mixed state $\rho(N)$ produced by randomly chosen from a finite set of N-copy entangled states $\{|\psi_i\rangle^{\otimes N}\}$, can be locally transformed to an EPR pair $|\Phi_0\rangle$, for some sufficiently large N.

We apply our distillation to identify an unknown bipartite quantum measurement locally. It provides us a way to obtain EPR pairs by a finite number of runs of this unknown measurement. The local identification has been reduced to global identification in these cases. In particular, we have discussed the local identification from two bipartite projective measurements and have found a computable sufficient condition of identifiable measurements. Surprisingly, even in this simple case, we have found an example of two bipartite measurements which are locally undistinguishable. It exposes the difference between global identification and local identification, for quantum measurements.

We are grateful to Nengkun Yu for suggesting a different approach to deal with the general case of Theorem 1. We also thank Yuan Feng and Zhengfeng Ji for useful discussions. This work was partially supported by NSF of China (Grant Nos. 60621062, 60702080, 60736011) and QCIS, University of Technology, Sydney.

---

[1] A. Chefles, Phys. Lett. A **239**, 339 (1998); L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[2] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
[3] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[4] Z. F. Ji, H. E. Cao and M. S. Ying, Phys. Rev. A. **71**, 032323 (2005).
[5] C. H. Bennett, D. P. DiVincenzo, C. C. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A, **59**, 1070 (1999).
[6] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
[7] S. Bandyopadhyay and J. Walgate, J. Phys. A: Math. Theor. **42** 072002(2009).
[8] R. Duan, Y. Feng, Z. Ji, and M. Ying, Phys. Rev. Lett. **98**, 230502 (2007).
[9] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[11] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[12] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A, **54**, 3824 (1996).
[13] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[14] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A, **67**, 022310 (2003).
[15] S. M. Cohen, Phys. Rev. A, **75**, 052313 (2007)
[16] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[17] M. A. Nielsen. Phys. Rev. Lett. **83**, 436 (1999).
[18] I. D. Ivanovic, Phys. Lett. A, **123**, 257 (1987).
[19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[20] 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).
[21] Z. F. Ji, Y. Feng, R. Y. Duan and M. S. Ying, Phys. Rev. Lett. **96**, 200401 (2006).
[22] G. M. Wang and M. S. Ying, Phys. Rev. A. **73**, 042301 (2006); J. Watrous, arXiv:0710.0902; M. Piani and J. Watrous, Phys. Rev. Lett. **102**, 250501 (2009).
[23] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **98**, 100503 (2007).
[24] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **103**, 210501 (2009).
[25] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. **100**, 020503 (2008).
[26] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999); D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Comm. Math. Phys. **238**, 379 (2003).
[27] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001); R. Y. Duan, Y. Xin, and M. S. Ying, arXiv:0708.3559.

Appendix 1: Proof of the general case of Theorem 1

In this Appendix we turn to prove Theorem 1 for the general case $\{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_n\rangle\}$. Let us first complete the proof of $n = 2$ case. we will show that the full Schmidt rank assumption can be removed. In fact, we will show that for any two bipartite entangled pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, by performing a local projective measurement $\{P'_0, P'_1\}$ on Bob's side we can either i) with outcome "0" achieve a successful discrimination between these two states, or ii) with outcome "1" obtain another two entangled states $|\psi'_1\rangle$ and $|\psi'_2\rangle$ on a smaller state space $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, and one of them is of full Schmidt rank.

Let $\mathcal{H}_B(\psi_1)$ and $\mathcal{H}_B(\psi_2))$ denote the supports of $\mathrm{tr}_A(|\psi_1\rangle\langle\psi_1|)$ and $\mathrm{tr}_A(|\psi_2\rangle\langle\psi_2|))$, respectively. Let P_1 and P_2 be their respective projectors. We have $rank(P_1),\ rank(P_2) \geq 2$ as $|\psi_1\rangle$ and $|\psi_2\rangle$ are both entangled. The case of $\langle\psi_2|\psi_1\rangle = 0$ is trivial. In the following, we assume that $\langle\psi_2|\psi_1\rangle \neq 0$. Obviously, $P_2P_1 \neq 0$. Now we complete the proof for $n = 2$ by considering the following three cases:

- Case 1. $rank(P_2P_1) \geq 2$. It suffices to choose a measurement $\{P'_0 = I_B - P_2, P'_1 = P_2\}$ on Bob's part. Outcome "0" indicates the original state is $|\psi_1\rangle$ while outcome "1" yields a pair of entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B(\phi_2)$, namely $I_A \otimes P_2|\phi_1\rangle$ and the full Schmidt number state $I_A \otimes P_2|\phi_2\rangle = |\phi_2\rangle$, and the latter case has been proven.

- Case 2. $rank(P_2P_1) = 1$, and $P_1P_2 = P_2P_1$. Let $P_2P_1 = |x\rangle\langle x|$, where $|x\rangle$ and $|y\rangle$ are both normalized states in $\mathcal{H}_B$. $P_1|x\rangle = |x\rangle$, $P_2|x\rangle = |x\rangle$, $Q_1 := P_1 - |x\rangle\langle x| \perp P_2$, and $Q_2 := P_2 - |y\rangle\langle y| \perp P_1$, where Q_1 and Q_2 are projectors of rank at least 1. Let $|1\rangle$ and $|2\rangle$ be eigenstates of Q_1 and Q_2, respectively. Consider a measurement $\{P'_0 = I_B - P'_1, P'_1 = |x\rangle\langle x| + |1\rangle\langle 1| + |2\rangle\langle 2|\}$. It is easy to verify that outcome "0" results in two orthogonal states, and outcome "1" results in two new bipartite entangle pure states with projectors $P_1 = |1\rangle\langle 1| + |x\rangle\langle x|$ and $P_2 = |2\rangle\langle 2| + |x\rangle\langle x|$, respectively. Let $|z_\pm\rangle = (|1\rangle \pm |2\rangle)/\sqrt{2}$. By another local measurement $\{M_1 = |z_+\rangle\langle z_+| + |x\rangle\langle x|/\sqrt{2}, M_2 = |z_-\rangle\langle z_-| + |x\rangle\langle x|/\sqrt{2}\}$ we finally obtain two entangled states with the same supports $|z_+\rangle\langle z_+| + |x\rangle\langle x|$ or $|z_-\rangle\langle z_-| + |x\rangle\langle x|$, which is again a proven case.

- Case 3: $rank(P_2P_1) = 1$ and $P_2P_1 \neq P_1P_2$. Let $P_2P_1 = a|y\rangle\langle x|$, where $|x\rangle$ and $|y\rangle$ are both normalized states in $\mathcal{H}_B$ and $0 < |a| < 1$. It is easy to check that $\langle x|y\rangle \neq 0$, $P_1|x\rangle = |x\rangle$, $P_2|y\rangle = |y\rangle$, $Q_1 = P_1 - |x\rangle\langle x| \perp P_2$, and $Q_2 = P_2 - |y\rangle\langle y| \perp P_1$, where Q_1 and Q_2 are projectors of rank at least 1. Bob can perform a local measurement $\{P_0' = I_B - P_1', P_1' = Q_1 + Q_2 + |x\rangle\langle x|\}$. Then he can either determine the original state is $|\psi_1\rangle$ or yield another pair of entangled states $|\psi_1'\rangle = (I_A \otimes P_1')|\psi_1\rangle = |\psi_1\rangle$ and $|\psi_2'\rangle = (I_A \otimes P_1')|\psi_2\rangle$, which is reduced to Case 2 as $|x\rangle$ is in both supports.

Now we consider the case of $n > 2$. We shall first prove the result for the following three special states on two pairs of qubits: $|\psi_1\rangle_{AB} = |\Phi_0\rangle_{A_1B_1}|\Phi_0\rangle_{A_2B_2}$, $|\psi_2\rangle_{AB} = |\phi_1\rangle_{A_1B_1}|\Phi_0\rangle_{A_2B_2}$, $|\psi_3\rangle_{AB} = |\Phi_0\rangle_{A_1B_1}|\phi_2\rangle_{A_2B_2}$. If $|\phi_1\rangle$ is an entangled state, $\{|\Phi_0\rangle, |\phi_1\rangle\}$ is a proven case on pair 1, and the result is reduced to $n = 2$ case. So it suffices to consider that $|\phi_1\rangle$ is a product state. Similarly, we assume $|\phi_2\rangle$ to be a product state in the same way. Without loss of generality, let $|\phi_1\rangle = (a|0\rangle + b|1\rangle)_{A_1}|0\rangle_{B_1}$ and $|\phi_2\rangle = (c|0\rangle + d|1\rangle)_{A_2}|0\rangle_{B_2}$, where $|a|^2 + |b|^2$=1 and $|c|^2 + |d|^2 = 1$. (The reason that we can choose $|\phi_1\rangle$ (or $|\phi_2\rangle$) of this form is that we can perform $U_A \otimes {U_A}^*$ on pair 1 (pair 2) without change the state $|\Phi_0\rangle$) on both pairs).

Now let us introduce a linear operator $O_{B_1B_2}$ on Bob's system B_1B_2 as follows:

$$O_{B_1B_2} = |00\rangle(ac\langle 00| + ad\langle 01| + bc\langle 10|) + |11\rangle\langle 11|.$$

Then $\mathcal{M} = \{M_0, M_1\}$ is a local measurement, where $M_1 = I_{A_1A_2} \otimes O_{B_1B_2}, M_0 = I_{A_1A_2} \otimes \sqrt{I_{B_1B_2} - O^\dagger O}$. Notice that $\langle\psi_2|M_0^\dagger M_0|\psi_3\rangle = 0$. So after this measurement, $|\psi_2\rangle$ and $|\psi_3\rangle$ become orthogonal if the outcome is "0". and then, we can reduce the present case to $n = 2$ case by distinguishing between these two states. Thus, we only need to consider that when the outcome is always "1". In this setting, it's easy to check that $M_1|\psi_1\rangle$ is an entangled state $|\xi\rangle$ while $M_1|\psi_2\rangle, M_2|\psi_3\rangle$ become the same state $|\psi\rangle = |\alpha\rangle_{A_1A_2}|00\rangle_{B_1B_2}$. On the other hand, by the results in $n = 2$ case of Theorem 2, $|\psi_2\rangle^{\otimes N}$ and $|\psi_3\rangle^{\otimes N}$ can be transformed to $|\Phi_0\rangle$ at the same time by some local measurement $\mathcal{M}'$. Now, measure $\{|\psi_1\rangle^{\otimes(N+1)}, |\psi_2\rangle^{\otimes(N+1)}, |\psi_3\rangle^{\otimes(N+1)}\}$ by $\mathcal{M}$ on the first copy and $\mathcal{M}'$ on the other N copies. Suppose $\mathcal{M}'$ brings $|\psi_1\rangle^{\otimes N}$ into some $|\phi\rangle$. Then the whole state becomes a mixture of two entangled states $|\xi\rangle_{A_1B_1}|\phi\rangle_{A_2B_2}$ and $|\psi\rangle_{A_1B_1}|\Phi_0\rangle_{A_2B_2}$, which is a proven case.

Finally, let us complete the whole proof by induction on $n \geq 2$. By induction hypothesis and the result in Theorem 2, let local measurements $\mathcal{M}$ and $\mathcal{M}'$ transform $|\psi_1\rangle^{\otimes N_1}$, $|\psi_2\rangle^{\otimes N_1}$, $\cdots$, $|\psi_{n-1}\rangle^{\otimes N_1}$ and $|\psi_2\rangle^{\otimes N_2}$, $|\psi_2\rangle^{\otimes N_2}$, $\cdots$, $|\psi_n\rangle^{\otimes N_2}$ to $|\Phi_0\rangle$, respectively. Thus, $|\psi_1\rangle^{\otimes(N_1+N_2)}$, $|\psi_2\rangle^{\otimes(N_1+N_2)}$, $\cdots$, $|\psi_n\rangle^{\otimes(N_1+N_2)}$ can be reduced to a proven case. In fact, measure the first N_1 copies of this unknown state by $\mathcal{M}$ and measure the rest N_2 copies by $\mathcal{M}'$. Suppose M takes $|\psi_n\rangle^{\otimes N_1}$ to some $|\phi_1\rangle$ and $\mathcal{M}'$ takes $|\psi_1\rangle^{\otimes N_2}$ to some $|\phi_2\rangle$. Then these states become $|\Phi_0\rangle|\phi_2\rangle, |\Phi_0\rangle|\Phi_0\rangle, |\phi_1\rangle|\Phi_0\rangle$ for $|\psi_1\rangle, |\psi_i\rangle(i \neq 1, k), |\psi_k\rangle$ respectively. This is exactly the case we have just proven for $n = 3$. ■

Appendix 2: Proof of Lemma 5

Without loss of generality, we may assume that $|\alpha\beta\rangle$ is in the support of Q_k only. So we have $Q_k|\alpha\beta\rangle = |\alpha\beta\rangle$ and $P_k|\alpha\beta\rangle = \lambda|\Phi\rangle$, where $\lambda \neq 0$ (Otherwise $\mathcal{M}$ can be identified according the outcome of the measurement on $|\alpha\beta\rangle$) and $|\langle\alpha\beta|\Phi\rangle| < 1$. First, Alice and Bob apply $\mathcal{M}$ to input state $|\alpha\rangle|\beta\rangle$. If the outcome is not k, then $\mathcal{M} = \mathcal{M}_0$ and the identification is finished. Otherwise, the output state is $|\Phi\rangle$ and $|\alpha\beta\rangle$. To finish the proof, we need to consider the following two cases separately:

Case 1. $|\Phi\rangle = |\gamma\rangle_A|\delta\rangle_B$ is a product state. Clearly we have $|\langle\Phi|\alpha\beta\rangle| < 1$. If we further $|\langle\Phi|\alpha\beta\rangle| \leq 1/4$, then $|\langle\alpha|\gamma\rangle| \leq 1/2$ or $|\langle\beta|\delta\rangle| \leq 1/2$. Without loss of generality we may assume that $|\langle\gamma|\alpha\rangle| \leq 1/2$, then it follows from [**?**] there is a local isometry U acting on $\mathcal{H}_A$ satisfying $U|\gamma\rangle \perp |\gamma\rangle$ and $U|\alpha\rangle = |\alpha\rangle$. A perfect discrimination can be achieved by applying $(U \otimes I)$ to $(|\Phi\rangle, |\alpha\beta\rangle)$ and then applying $\mathcal{M}$ one more time. If $|\langle\alpha\beta|\Phi\rangle| > 1/4$, we can apply $\mathcal{M}$ in parallel to n copies of $|\alpha\beta\rangle$ yielding two output product states with inner product $|\langle\alpha\beta|\Phi\rangle|^n \leq 1/4$ for sufficiently large n.

Case 2. $|\Phi\rangle$ is entangled. Employing Lemma 3, we can transform $(|\Phi_{AB}\rangle, |\alpha_A\beta_B\rangle)$ locally into $(|\gamma_A 0_B\rangle, |\alpha_A 0_B\rangle)$ for some $|\gamma\rangle$ such that $|\langle\gamma|\alpha\rangle| < 1$. Similarly we can transform $(|\Phi_{AB}\rangle, |\alpha_A\beta_B\rangle)$ locally into $(|0_A\delta_B\rangle, |0_A\beta_B\rangle)$ for some $|\delta\rangle$ such that $|\langle\delta|\beta\rangle| < 1$. Combining these two transformations we can achieve the following transformation locally: $(|\Phi_{AB}\rangle^{\otimes 2}, |\alpha_A\beta_B\rangle^{\otimes 2})$ to $(|\gamma_A\delta_B\rangle, |\alpha_A\beta_B\rangle)$. It is clear by repeating this process sufficiently large times we can obtain two pairs of product states $|\gamma_A\delta_B\rangle$ and $|\alpha_A\beta_B\rangle$ such that $|\langle\gamma|\alpha\rangle|$ and $|\langle\delta|\gamma\rangle|$ can be arbitrarily small but not zero. Now we are trying to show that by choosing $|\gamma_A\delta_B\rangle$ carefully we can have $P_k|\gamma\delta\rangle \perp Q_k|\alpha\beta\rangle$, or equivalently, $P_k|\alpha\beta\rangle \perp |\gamma\delta\rangle$. This is obvious as the orthogonal complement of $P_k|\alpha\beta\rangle$ is spanned by a set of product states, and not all of these states are orthogonal to $|\alpha\beta\rangle$. Otherwise $P_k|\alpha\beta\rangle$ should coincide with $|\alpha\beta\rangle$, a contradiction with our assumption. ■