Locally Indistinguishable Subspaces Spanned by Three-Qubit Unextendible Product Bases

Runyao Duan[1],* Yu Xin[1,2],† 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,*
[2]*Department of Physics, Tsinghua University, Beijing 100084, China*
(Dated: June 13, 2013)

We study the local distinguishability of general multi-qubit states and show that local projective measurements and classical communication are as powerful as the most general local measurements and classical communication. Remarkably, this indicates that the local distinguishability of multi-qubit states can be decided efficiently. Another useful consequence is that a set of orthogonal n-qubit states is locally distinguishable only if the summation of their orthogonal Schmidt numbers is less than the total dimension 2^n. When $n = 2$ such a condition is also sufficient. Employing these results, we show that any orthonormal basis of a subspace spanned by arbitrary three-qubit orthogonal unextendible product bases (UPB) cannot be exactly distinguishable by local operations and classical communication. This not only reveals another intrinsic property of three-qubit orthogonal UPB, but also provides a class of locally indistinguishable subspaces with dimension 4. We also explicitly construct locally indistinguishable subspaces with dimensions 3 and 5, respectively. In particular, 3 is the minimal possible dimension of locally indistinguishable subspaces. Combining with the previous results, we conclude that any positive integer between 3 and 7 is the possible dimension of some three-qubit locally indistinguishable subspace.

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

I. INTRODUCTION

An interesting problem in quantum information theory is to distinguish a finite set of orthogonal multipartite quantum states using local operations and classical communication (LOCC). This problem has been extensively studied in the last two decades and numerous exciting results have been reported, see Ref. [1] and references therein for details. In spite of these considerable efforts, a complete solution to this problem is still out of reach due to the complicated nature of LOCC operations. Nevertheless, several objects with rich mathematical structure such as unextendible product bases (UPB) and locally indistinguishable subspaces were introduced during this process.

The notion of UPB was originally introduced by Bennett and coworkers [2], and has been thoroughly studied in the literatures [3, 4, 5]. Notably, the members of a UPB cannot be perfectly distinguishable by LOCC.

Recently Watrous introduced a class of interesting bipartite subspaces having no orthonormal bases distinguishable by LOCC [6]. Such subspaces can be intuitively named locally indistinguishable subspaces. The minimal dimension of locally indistinguishable subspaces obtained by Watrous is 8. In Ref. [1] we generalized his result to multipartite setting ans showed that any orthogonal complement of a multipartite pure state with orthogonal Schmidt number at least 3 is locally indistinguishable. Furthermore, a $3 \otimes 3$ subspace of dimension 7 and a $2 \otimes 2 \otimes 2$ subspace of dimension 6 were constructed. All these subspaces are actually indistinguishable by a wider class of quantum operations, say separable operations. However, it still remains unknown how low can the dimension of indistinguishable subspaces go. In general, there is no simple and feasible way to show a given subspace is locally indistinguishable.

In this paper we try to connect the above two notions together. The problem we attempt to solve can be described as follows. Let S be an orthogonal UPB, and let $span(S)$ be the subspace spanned by the members of S. Our ultimate goal is to show that $span(S)$ is locally indistinguishable. Unfortunately, we fail to present a complete solution at present. We can only partially accomplish this goal by showing that any subspace spanned by the members of a $2 \otimes 2 \otimes 2$ UPB is locally indistinguishable. These subspaces also have the interesting property that they are indistinguishable by LOCC but have at least an orthonormal basis distinguishable by separable operations. As a direct consequence, we obtain a class of locally indistinguishable subspaces with dimension 4.

It should be noted that unextendibility itself is not the crucial property for local indistinguishability. To see this, we present an explicit $2 \otimes 2 \otimes 2$ subspace which is spanned by a set locally distinguishable quantum states. As an interesting byproduct, we show the state space of three-qubits can be decomposed into two orthogonal subspaces which both are entangled, thus are unextendible. That immediately yields an instance of two orthogonal mixed states that are locally indistinguishable, even probabilistically, which is strikingly different from the perfect local

*Electronic address: dry@tsinghua.edu.cn
†Electronic address: xiny05@mails.tsinghua.edu.cn
‡Electronic address: yingmsh@tsinghua.edu.cn

distinguishability of any two orthogonal pure states [7]. To the best of our knowledge, no such instance was previously known.

Since any two orthogonal pure states are perfectly distinguishable by LOCC [7], the dimension of locally indistinguishable subspace is at least 3. However, it seems a formidable task to find such a subspace. Actually for $3\otimes 3$ state space it was conjectured that such 3-dimensional subspace does not exist at all [13]. Interestingly, for three-qubit system we do find a class of three-dimensional subspaces that are locally indistinguishable. This is the first locally indistinguishable subspace with minimal dimension.

It remains unknown whether there is a locally indistinguishable subspace with dimension 5. We provide an affirmative answer to this question by explicitly constructing a five-dimensional three-qubit subspace containing a unique product state. Then this subspace is locally indistinguishable follows from the Schmidt-number-summation criterion about the local distinguishability for multi-qubit system.

The rest of this paper is organized as follows. In Section II we review basic definitions and notions that are useful in studying LOCC discrimination. Then in Section III a criterion for the local distinguishability of general $2 \otimes n$ orthogonal quantum states is given, which slightly generalizes the work of Walgate and Hardy [8]. We apply this criterion in Section IV to show that local projective measurements and classical measurements are sufficient to perfectly distinguish multi-qubit orthogonal quantum states. As a direct consequence, we show that a set of multi-qubit orthogonal quantum states is locally distinguishable only if the total summation of their orthogonal Schmidt numbers is not more than the dimension of the state space under consideration. In particular, in Section V we further prove that the summation of orthogonal Schmidt numbers less than 4 gives exactly the necessary and sufficient condition of the local distinguishability of $2 \otimes 2$ orthogonal quantum states. With above preparations, we are ready to present our main result in Section VI. That is, any subspace spanned by a three-qubit UPB is locally indistinguishable. Section VII clarifies the relation between indistinguishablity and unextendibility. In particular, two $2\otimes 2\otimes 2$ orthogonal mixed states that are indistinguishable by probabilistic LOCC are presented. Locally indistinguishable subspaces with dimensions 3 and 5 are presented in Sections VIII and IX, respectively. We conclude the paper in Section X. Several unsolved problems are also proposed for further study.

II. PRELIMINARIES

We consider a multipartite quantum system consisting of K parts, say $A_1, \cdots, A_K$. We assume part A_k has a state space $\mathcal{H}_k$ with dimension d_k. The whole state space is given by $\mathcal{H} = \otimes_{k=1}^{K} \mathcal{H}_k$ with total dimension $D = d_1 \cdots d_K$. The notation $d_1 \otimes \cdots \otimes d_K$ is an abbreviation for $\mathcal{H}$.

We first recall some useful definitions introduced by Walgate and Hardy [8]. When discriminating a set of states, we need to perform suitable measurements $\{M_m\}$ on the system to obtain useful information about the real identity of the states. If $M_m^\dagger M_m$ is proportional to the identity, then the measurement operator M_m is simply a unitary operation on the state and it cannot provide any useful information for discrimination. This kind of measurement operator is said to be trivial. A measurement is said to be non-trivial if at least one of its measurement operators is not trivial.

Any finite LOCC protocol that discriminates a set of orthogonal multipartite states $\{\rho_1, \cdots, \rho_N\}$ consists of finitely many *measuring and broadcasting* rounds as follows: Some party performs a measurement and then broadcasts the outcome through the classical channels to the others. The protocol will not terminate until a definite decision about the identity of the state can be made. Clearly, there should be some person who performs the first non-trivial measurement. This simple observation leads us to the following definition:

Definition 1. Suppose Alice, Bob, $\cdots$, try to discriminate a set of states among them by local operations and classical communication only. We say Alice goes first if Alice is the one who performs the first non-trivial measurement.

After performing a non-trivial measurement, Alice, Bob, $\cdots$, need to discriminate a new set of (unnormalized) states $\{M_m \rho_k M_m^\dagger : k = 1, \cdots, N\}$ if the outcome is m. To ensure a perfect discrimination can be achieved, the resulting states should be orthogonal and some states may be vanishing. This puts a strong constraint on the measurement operators.

Definition 2. Let $\{\rho_1, \cdots, \rho_N\}$ be a set of orthogonal states. A measurement operator M_m is called orthogonality-keeping if states in the set $\{M_m \rho_k M_m^\dagger : k = 1, \cdots, N\}$ remain to be orthogonal. A complete measurement $\{M_m\}$ is said to be orthogonality-keeping if for each M_m is orthogonality-keeping.

For a positive operator ρ, Supp(ρ) represents the support of ρ. In other words, Supp(ρ) is the subspace spanned by the eigenvectors of ρ corresponding to the positive eigenvalues. We shall need the following technical lemma:

Lemma 1. Let ρ be a density operator, and $|\psi\rangle$ be a normalized state. Then $|\psi\rangle \in Supp(\rho)$ if and only if there exists $0 < p \leq 1$ and a density operator ρ' such that $\rho = p|\psi\rangle\langle\psi| + (1-p)\rho'$.

The physical meaning of the above lemma can be interpreted as follows: A pure state $|\psi\rangle$ is in the support of ρ if and only if it appears in some ensemble that realizes ρ. A useful consequence is as follows:

Corollary 1. A measurement $\{M_m\}$ is orthogonality-keeping for a set of orthogonal states $\{\rho_k\}$ if and only if for each m, $M_m|\psi_1\rangle, \cdots, M_m|\psi_N\rangle$ are pairwise orthogonal, where $|\psi_k\rangle \in \mathrm{Supp}(\rho_k)$.

In what follows we shall frequently employ the notion of orthogonal Schmidt number. Here we simply state a definition, for details we refer to Ref. [1]. Let ρ be a general quantum state. The orthogonal Schmidt number of ρ, denoted as $\mathrm{Sch}_\perp(\rho)$, is the minimal number orthogonal product states needed to span the support of ρ. When only bipartite pure states are involved, the orthogonal Schmidt number is exactly the ordinary Schmidt number, i.e., the number of nonzero Schmidt coefficients.

III. A CRITERION FOR THE LOCAL DISTINGUISHABILITY OF GENERAL ORTHOGONAL $2 \otimes n$ STATES

Now we turn to study the local distinguishability of $2 \otimes n$ quantum system. Without loss of generality, we assume Alice is the person who holds the qubit. In Ref. [8], Walgate and Hardy gave a necessary and sufficient condition for the local distinguishability of a finite set of $2 \otimes n$ pure states when Alice goes first. Interestingly, their result is also valid for mixed states.

Theorem 1. Let Alice and Bob share an unknown state which is secretely chosen from N orthogonal $2 \otimes n$ states, say $\rho_1, \cdots, \rho_N$, and let Alice be the one holding the qubit. If Alice goes first, then Alice and Bob can perfectly identify their state using LOCC if and only if there exists an orthogonal basis $\{|0\rangle, |1\rangle\}_A$ such that for any $|\psi_k\rangle \in Supp(\rho_k)$, we have

$$|\psi_k\rangle = |0\rangle_A|\psi_0^{(k)}\rangle_B + |1\rangle_A|\psi_1^{(k)}\rangle_B, \tag{1}$$

where $\langle\psi_0^{(k)}|\psi_0^{(l)}\rangle = \langle\psi_1^{(k)}|\psi_1^{(l)}\rangle = 0$ for any $1 \le k < l \le N$.

Proof. Many proof techniques are borrowed from Ref. [8]. The sufficiency is obvious. If there exists an orthonormal basis $\{|0\rangle, |1\rangle\}_A$ such that the above equation holds, then each ρ_k should be of the following form:

$$\rho_k = \sum_{m,n=0}^{1} |m\rangle\langle n| \otimes \rho_{mn}^{(k)},$$

where $\{\rho_{mm}^{(k)}\}$ is a set of orthogonal states and $m = 0, 1$. A perfect discrimination protocol is as follows:

(1) Alice measures her qubit according to the basis $\{|0\rangle, |1\rangle\}_A$ and sends the outcome m to Bob.

(2) If $m = 0$ then Bob's state is one of $\{\rho_{00}^{(k)}\}$. He can perfectly discriminate them by a projective measurement since they are orthogonal. The case when $m = 1$ can be analyzed similarly.

Now we turn to show the necessity. Suppose that $\rho_1, \cdots, \rho_N$ can be discriminated with certainty when Alice goes first. Let us assume that Alice's nontrivial and orthogonality-keeping measurement operator be M_m. Then for any $|\psi_k\rangle \in Supp(\rho_k)$ and $|\psi_l\rangle \in Supp(\rho_l)$, we have

$$\langle\psi_k|M_m^\dagger M_m \otimes I|\psi_l\rangle = 0, \tag{2}$$
$$\langle\psi_k|\psi_l\rangle = 0, \tag{3}$$

where the second equation is due to the fact that ρ_k and ρ_l are orthogonal. Let

$$M_m^\dagger M_m = \alpha|0\rangle\langle 0| + \beta|1\rangle\langle 1| \tag{4}$$

be the spectral decomposition, where $\alpha > \beta \ge 0$ by the non-triviality. Rewrite

$$|\psi_k\rangle = |0\rangle|\psi_0^{(k)}\rangle + |1\rangle|\psi_1^{(k)}\rangle, \tag{5}$$
$$|\psi_l\rangle = |0\rangle|\psi_0^{(l)}\rangle + |1\rangle|\psi_1^{(l)}\rangle. \tag{6}$$

Then we have

$$\alpha\langle\psi_0^{(k)}|\psi_0^{(l)}\rangle + \beta\langle\psi_1^{(k)}|\psi_1^{(l)}\rangle = 0, \tag{7}$$
$$\langle\psi_0^{(k)}|\psi_0^{(l)}\rangle + \langle\psi_1^{(k)}|\psi_1^{(l)}\rangle = 0. \tag{8}$$

Since $\alpha \neq \beta$, the above system of equations has a unique solution $\langle\psi_0^{(k)}|\psi_0^{(l)}\rangle = \langle\psi_1^{(k)}|\psi_1^{(l)}\rangle = 0$. With that we complete the proof of the necessity. ■

Intuitively speaking, the above theorem shows that a set of $2 \otimes n$ states are locally distinguishable when Alice goes first if and only after Alice performs some suitable projective measurement, the post-measurement states remain orthogonal. Actually, we have proven the following

Corollary 2. If Alice goes first, then $\rho_1, \cdots, \rho_N$ can be perfectly discriminated by LOCC if and only if there exists an orthogonal basis $\{|0\rangle, |1\rangle\}_A$ such that each ρ_k has the form:

$$\rho_k = \sum_{m,n=0}^{1} |m\rangle\langle n| \otimes \rho_{mn}^{(k)}, \tag{9}$$

where $\rho_{mm}^{(1)}, \cdots, \rho_{mm}^{(N)}$ are pairwise orthogonal for each $m = 0, 1$.

The decomposition in the Eq. (1) can be analytically determined.

IV. LOCAL PROJECTIVE MEASUREMENTS AND CLASSICAL COMMUNICATION ARE SUFFICIENT FOR LOCALLY DISTINGUISHING MULTI-QUBIT STATES

A simple but remarkable consequence of Theorem 1 is that local projective measurement and classical communication is powerful enough to locally distinguish a set of multi-qubit orthogonal quantum states. Due to its significance, we formally state it as follows:

Theorem 2. Local projective measurements and classical communications are sufficient for deciding the local distinguishability of any set of multi-qubit orthogonal quantum states.

The above theorem simplifies the local distinguishability of multi-qubit considerably and makes it almost feasible to locally distinguish a set of multi-qubit orthogonal states. A procedure can be described as follows. Suppose n qubits are held by $Alice_1, \cdots, Alice_n$, respectively. Then any set of n-qubit orthogonal states can be perfectly distinguishable by LOCC if and only if they can be distinguishable by local projective measurements and classical communication (LPMCC). Let σ be a permutation on n qubits which is used to specify the order of the projective measurement performed by each party. That is, $Alice_{\sigma(1)}$ is the first person who performs a nontrivial measurement, $Alice_{\sigma(2)}$ is the second one who performs a conditional non-trivial measurement depending on $Alice_{\sigma(2)}$'s outcome, $\cdots$, and $Alice_{\sigma(n)}$ is the last one who performs conditional projective measurement depending on the previous $n-1$ party's outcome. The projective measurement performed by $Alice_{\sigma(1)}$ is given by an orthogonal basis $P_{\sigma(1)}(x_1) = \{|\psi_{\sigma(1)}(x_1)\rangle : x_1 = 0, 1\}$, where x_1 represents the outcome. According to the outcome of $Alice_{\sigma_1}$, $Alice_{\sigma(2)}$ performs a projective measurement $P_{\sigma(2)}(x_1x_2) = \{|\psi_{\sigma(2)}(x_1x_2)\rangle : x_2 = 0, 1\}$ with outcome x_2. Finally, depending on the previous outcomes $x_1, \cdots, x_{n-1}$, $Alice_{\sigma(n)}$ performs a conditional projective measurement $P_{\sigma(n)}(x_1x_2\cdots x_n) = \{|\psi_{\sigma(n)}(x_1x_2\cdots x_n)\rangle : x_n = 0, 1\}$. The above procedure induces a projective measurement on n qubits represented by an orthogonal product basis $\{|\psi(x)\rangle : x \in \{0,1\}^n\}$, where

$$|\psi(x)\rangle = |\psi_{\sigma(1)}(x_1)\rangle \otimes \cdots \otimes |\psi_{\sigma(n)}(x_1x_2\cdots x_n)\rangle. \quad (10)$$

It is clear that $\rho_1, \cdots, \rho_N$ are perfectly distinguishable by $Alice_1, \cdots, Alice_n$ if and only if they lead to different (non-overlap) measurement outcomes. That is, there exists a permutation σ, and a disjoint partition of $\{0,1\}^n$, say $O_1, \cdots, O_N$ such that

$$\mathrm{Supp}(\rho_k) \subseteq \mathrm{Span}\{|\psi(x)\rangle : x \in O_k\}. \quad (11)$$

For each σ, the sequence of projective measurement, say, $P_{\sigma(1)(x_1)}, \cdots, P_{\sigma(n)}(x_1\cdots x_n)$ can be analytically determined. Repeating the above process for all the $n!$ permutations, we can completely determine the local distinguishability of $\{\rho_1, \cdots, \rho_N\}$.

Eq. (11) implies a simple but highly nontrivial criterion for local distinguishability of a set of multi-qbut states.

Theorem 3. Let $S = \{\rho_1, \cdots, \rho_N\}$ be a collection of orthogonal states on n qubits. Then S is perfectly distinguishable by LOCC only if the sum of the orthogonal Schmidt numbers of ρ_k is not more than the total dimension of state space, i.e.,

$$\sum_{k=1}^{N} \mathrm{Sch}_\perp(\rho_k) \leq 2^n. \quad (12)$$

A few remarks come as follows. Eq. (12) reflects the fact that local projective measurements and classical communication are sufficient for locally distinguishing multi-qubit quantum states. In general, only projective measurements are not able to distinguish quantum states locally. For such peculiar states the summations of the orthogonal Schmidt numbers may exceed the total dimension of the state space. An explicit instance of such peculiar states has been found by Cohen very recently [10]. We would also like to point out that Eq. (12) is not sufficient when the number of qubits under consideration are more than 2: There do exist four $2\otimes 2\otimes 2$ orthogonal product pure states that are indistinguishable by LOCC [2].

To appreciate the power of Theorems 2 and 3, we shall present two examples concerning with the local distinguishability of GHZ-type and W-type states, which are respectively defined as

$$\alpha|00\cdots 0\rangle + \beta|11\cdots 1\rangle \quad (13)$$

and

$$\alpha_1|00\cdots 1\rangle + \alpha_2|0\cdots 01\rangle + \cdots + \alpha_n|10\cdots 0\rangle, \quad (14)$$

where each α_k is nonzero complex number and $n \geq 2$. It has been shown that any n-qubit W-type state has orthogonal Schmidt number n. By Theorem 3, there are at most $2^n/n$ W-type states can be locally distinguishable. In particular, any three 3-qubit W-type states are locally indistinguishable.

For GHZ-type states we shall show that any three n-qubit states containing at least two GHZ-type states of the form Eq. (13) are locally indistinguishable ($n \geq 2$). The proof is by mathematical induction. First, the base case when $n = 2$ directly follows from Theorem 3 as the summation of the orthogonal Schmidt numbers is at least $2 + 2 + 1 = 5 > 4$. Second, suppose the result is valid for $n - 1$, we will show the result is also valid for n. By Theorem 2, we only need to consider local projective measurements. Assume some party performs a projective measurement $\{|\psi\rangle, |\psi^\perp\rangle\}$. If $|\psi\rangle \in \{|0\rangle, |1\rangle\}$ (up to some phase factor), then after the measurement two GHZ-type states will reduce to identical states such as $|0\rangle^{\otimes n-1}$ or $|1\rangle^{\otimes n-1}$ thus cannot be further distinguished. If $|\psi\rangle \notin \{|0\rangle, |1\rangle\}$, then at least for one measurement outcome (0 or 1) the possible remaining states are three $n-1$-qubit states containing at least two-GHZ type state. The proof is completed by applying induction hypothesis. We notice the case of $n = 3$ has been solved by Ye *et al.* using a different but much more complicated method [9].

V. LOCAL DISTINGUISHABILITY OF $2 \otimes 2$ STATES

When only $2 \otimes 2$ states are under consideration, Eq. (12) is also sufficient for the local distinguishability.

Theorem 4. Let $S = \{\rho_1, \cdots, \rho_N\}$ be a set of $2 \otimes 2$ orthogonal states. Then S is locally distinguishable if and only if $\sum_{k=1}^{N} \mathrm{Sch}_\perp(\rho_k) \leq 4$.

Proof. If each ρ_k is a pure state, then the above theorem is reduced to the one given by Walgate and Hardy [8]. Here we need to consider the case when some state may be mixed. We consider three cases according the number of states. First we consider the case of $N = 2$. By Theorem 12, we only need to consider the sufficiency. If both ρ_1 and ρ_2 are mixed states. Then we should have $\mathrm{Sch}_\perp(\rho_1) = Sch_\perp(\rho_2) = 2$. That means there exists a set of orthogonal product states $\{|\Psi_k\rangle : 1 \leq k \leq 4\}$ such that

$$\mathrm{Supp}(\rho_1) = \mathrm{Span}\{|\Psi_1\rangle, |\Psi_2\rangle\}, \quad (15)$$
$$\mathrm{Supp}(\rho_3) = \mathrm{Span}\{|\Psi_3\rangle, |\Psi_4\rangle\}. \quad (16)$$

Applying the result of Walgate and Hardy [8], we know that Alice and Bob can perfectly distinguish $\{|\Psi_k\rangle : 1 \leq k \leq 4\}$. If the outcome is 1 or 2, then the state is ρ_1; otherwise is ρ_2. Using similar arguments, we can prove the case when only one of ρ_1 and ρ_2 is mixed.

The case of three or four states is rather simple. Actually, we can show that three $2 \otimes 2$ orthogonal states are locally distinguishable if and only if there are two product states, and four $2 \otimes 2$ orthogonal states are locally distinguishable if and only if they are all product pure states. These results are completely in accordance with Ref. [8] ■

Theorem 4 indicates the local distinguishability of a set of $2 \otimes 2$ orthogonal states is completely characterized by their orthogonal Schmidt numbers. More precisely, a set of states $\{\rho_1, \cdots, \rho_N\}$ $(2 \leq N \leq 4)$ is locally distinguishable the set orthogonal Schmidt numbers belongs to one of the following case: $\{2, 2\}$, $\{2, 1, 1\}$, $\{1, 1, 1, 1\}$, $\{2, 1\}$, $\{1, 1, 1\}$, $\{1, 1\}$.

Employing Theorem 4, we can show there exists pairs of orthogonal $2 \otimes 2$ quantum states that are locally indistinguishable. Let ρ_1 be a uniform mixture of $|00\rangle$ and $|{+}{+}\rangle$, and let ρ_2 be a uniform mixture of $|1{-}\rangle$ and $|{-}1\rangle$. It is clear that both ρ_1 and ρ_2 are separable. However, we have

$$\mathrm{Sch}_\perp(\rho_1) = \mathrm{Sch}_\perp(\rho_2) = 3,$$

which immediately implies that ρ_1 and ρ_2 are locally indistinguishable as the sum exceeds 4. The indistinguishability between ρ_1 and ρ_2 has already been proven in Ref. [17], and was thoroughly studied in the scenario of quantum data hiding [18]. But here we supply a rather different approach which is of independent interest. Similarly, let $\rho_3 = |\psi\rangle\langle\psi|$ such that $|\psi\rangle = \alpha|1{-}\rangle + \beta|{-}1\rangle$ and $\alpha\beta \neq 0$, then ρ_1 and ρ_3 are indistinguishable as $\mathrm{Sch}_\perp(\rho_1) + \mathrm{Sch}_\perp(\rho_3) = 5 > 4$.

VI. LOCALLY INDISTINGUISHABLE SUBSPACES SPANNED BY $2 \otimes 2 \otimes 2$ UNEXTENDIBLE PRODUCT BASES

Now we begin to study three-qubit quantum systems. First we present a formal definition of locally indistinguishable subspace.

Definition 3. Let S be a subspace of $\mathcal{H} = \otimes_{k=1}^{m} \mathcal{H}_k$. S is said to be locally indistinguishable if any orthogonal basis of S cannot be perfectly distinguishable by LOCC.

The first instance of locally indistinguishable subspace was given by Watrous [6]. For completeness, we give a short review here. Let $|\Phi\rangle$ be a $d \otimes d$ maximally entangled state, then it was proven that $\{|\Phi\rangle\}^\perp$ is locally indistinguishable whenever $d > 2$. Actually, what was shown in Ref. [6] is that $\{|\Phi\rangle\}^\perp$ has no orthonormal basis perfectly distinguishable by separable operations rather than LOCC. With this subspace, Watrous constructed a class of quantum channels which have sub-optimal environment-assisted capacity thus solved an open problem suggested by Hayden and King [12]. Clearly, the minimal dimension of indistinguishable subspaces obtained by Watrous is $3^2 - 1 = 8$. In Ref. [1] we generalized this result to arbitrary multipartite pure state $|\Psi\rangle$ with orthogonal Schmidt number not less than 3. Furthermore, we explicitly constructed an indistinguishable bipartite subspaces with dimension $3^2 - 2 = 7$. Our method also gave a $2 \otimes 2 \otimes 2$ indistinguishable subspace with dimension $2^3 - 2 = 6$. How to further reduce the dimension of indistinguishable subspaces remains a difficult problem. In particular, we still don't know whether there are locally indistinguishable subspaces with dimensions 3, 4, 5, respectively.

All the known indistinguishable subspaces up to now are not only indistinguishable by LOCC, but also indistinguishable by separable operations. So a question of interest naturally arises: Does there exist some indistinguishable subspace which is locally indistinguishable but has some orthonormal basis distinguishable by separable operations? If such subspace does exist, we would expect it has a smaller dimension.

In what follows we show that locally indistinguishable subspaces with dimensions 3, 4, and 5 do exist. Moreover, subspaces with dimension 4 can be constructed from $2 \otimes 2 \otimes 2$ orthogonal UPB and have bases distinguishable by separable operations. We discuss the case of dimension 4 here, and the other two cases will be discussed in next section.

Note that any UPB for three-qubits should have four members, and can be uniquely written into the following from (up to some local unitary) [11]:

$$\begin{aligned} |S_1\rangle &= |0\rangle \otimes |0\rangle \otimes |0\rangle, \\ |S_2\rangle &= |1\rangle \otimes |B\rangle \otimes |C\rangle, \\ |S_3\rangle &= |A\rangle \otimes |1\rangle \otimes |C^\perp\rangle, \\ |S_4\rangle &= |A^\perp\rangle \otimes |B^\perp\rangle \otimes |1\rangle, \end{aligned} \quad (17)$$

where $|A\rangle = \cos\theta_1|0\rangle + \sin\theta_1|1\rangle$, $|B\rangle = \cos\theta_2|0\rangle + \sin\theta_2|1\rangle$, $|C\rangle = \cos\theta_3|0\rangle + \sin\theta_3|1\rangle$, and $\theta_1, \theta_2, \theta_3 \in (0, \pi/2)$. Our main result is the following

Theorem 5. Let S be the subspace spanned by the UPB defined in Eq. (17). Then S is locally indistinguishable, but has an orthogonal basis distinguishable by separable operations.

Proof. Applying the results in Ref. [3] or Ref. [1], we can easily see that the set of $\{S_k : 1 \le k \le 4\}$ is perfectly distinguishable by separable operations. That completes the proof that S has a basis distinguishable by separable operations.

Now we show that any basis of S is locally indistinguishable. It is easy to see that any orthonormal basis $\{|\Phi_k\rangle : 1 \le k \le 4\}$ of S is uniquely determined by a 4×4 unitary matrix U as follows:

$$|\Phi_k\rangle = u_{k1}|S_1\rangle + u_{k2}|S_2\rangle + u_{k3}|S_3\rangle + u_{k4}|S_4\rangle, \quad 1 \le k \le 4. \tag{18}$$

We shall consider five cases to complete the proof. By the symmetry, we may assume that Alice is the one who goes first. The basic idea is to show after Alice performs a projective measurements $\{|\psi\rangle, |\psi^\perp\rangle\}$, the post-measurement states are indistinguishable. It is worth noting that we shall employ an interesting property about S: There are only four product states in S. A proof of this fact was given in Ref. [11]. One can also prove it by a direct calculation.

Case 1. There are four product states in $\{|\Phi_k\rangle : 1 \le k \le 4\}$. They are just the UPB $\{S_k : 1 \le k \le 4\}$, thus are locally indistinguishable [2]. A direct proof is as follows. If $|\psi\rangle \notin \{|0\rangle, |A\rangle\}$, then the left states are four nonorthogonal product states, which is indistinguishable. Even if $|\psi\rangle \in \{|0\rangle, |A\rangle\}$, the left states are not orthogonal.

Case 2. There are three product states in $\{|\Phi_k\rangle : 1 \le k \le 4\}$. This case cannot happen.

Case 3. There are two product states. Without loss of generality, assume that $\{|\Phi_k\rangle : 1 \le k \le 4\}$ is of the following form:

$$|S_1\rangle, \quad |S_2\rangle, \tag{19}$$
$$u_1|S_3\rangle + u_2|S_4\rangle, \tag{20}$$
$$u_2^*|S_3\rangle - u_1^*|S_4\rangle \tag{21}$$

where $|u_1|^2 + |u_2|^2 = 1$ and $u_1 u_2 \ne 0$. If $|\psi\rangle = |0\rangle$ then the left (unnormalized) states are

$$|00\rangle, \tag{22}$$
$$u_1\langle 0|A\rangle|1C^\perp\rangle + u_2\langle 0|A^\perp\rangle|B^\perp 1\rangle, \tag{23}$$
$$u_2^*\langle 0|A\rangle|1C^\perp\rangle - u_1^*\langle 0|A^\perp\rangle|B^\perp 1\rangle, \tag{24}$$

which contains two entangled states and one product state. It follows from Ref. [8] that they cannot be perfectly distinguishable by LOCC. If $|\psi\rangle = |A\rangle$ then the left states are not orthogonal to each other. If $|\psi\rangle \notin \{|0\rangle, |1\rangle, |A\rangle, |A^\perp\rangle\}$, then the left states are not orthogonal to each other.

Case 4. There is a unique product state. Similar to Case 3. The orthogonality was ruined.

Case 5. There is no product states. This is the most nontrivial case we need to discuss. After Alice performs a projective measurement, we have four left states. They should constitute an orthogonal product basis. That immediately implies $\{|\Phi_k\rangle\}$ should be of the following form:

$$|\Phi_k\rangle = \alpha_k|\psi\rangle \otimes |ab_k\rangle + \beta_k|\psi^\perp\rangle \otimes |cd_k\rangle, \ 1 \le k \le 4, \tag{25}$$

where α_k and β_k are nonzero complex numbers such that $|\alpha_k|^2 + |\beta_k|^2 = 1$, and $\{|ab\rangle_k\}$ and $\{|cd\rangle_k\}$ are two orthogonal product bases. However, we shall show that such a representation is not possible.

First we derive a relation between $\{|ab_k\rangle\}$ and $\{|cd_k\rangle\}$. Consider the set of product states $\{|00\rangle, |BC\rangle, |1C^\perp 1\rangle, |B^\perp 1\rangle\}$. Let $\{|\widetilde{00}\rangle, |\widetilde{BC}\rangle, |\widetilde{1C^\perp}\rangle, |\widetilde{B^\perp 1}\rangle\}$ be its reciprocal basis. First we have

$$\begin{aligned} \alpha_k|ab_k\rangle &= u_{k1}\langle\psi|0\rangle|00\rangle + u_{k2}\langle\psi|1\rangle|BC\rangle \\ &+ u_{k3}\langle\psi|A\rangle|1C^\perp\rangle + u_{k4}\langle\psi|A^\perp\rangle|B^\perp 1\rangle, \end{aligned} \tag{26}$$
$$\begin{aligned} \beta_k|cd_k\rangle &= u_{k1}\langle\psi^\perp|0\rangle|00\rangle + u_{k2}\langle\psi^\perp|1\rangle|BC\rangle \\ &+ u_{k3}\langle\psi^\perp|A\rangle|1C^\perp\rangle + u_{k4}\langle\psi^\perp|A^\perp\rangle|B^\perp 1\rangle. \end{aligned} \tag{27}$$

From the equation about $|ab_k\rangle$ we have:

$$u_{k1} = \frac{\alpha_k}{\langle\psi|0\rangle}\frac{\langle\widetilde{00}|ab_k\rangle}{\langle\widetilde{00}|00\rangle}, \tag{28}$$
$$u_{k2} = \frac{\alpha_k}{\langle\psi|1\rangle}\frac{\langle\widetilde{BC}|ab_k\rangle}{\langle\widetilde{BC}|BC\rangle}, \tag{29}$$
$$u_{k3} = \frac{\alpha_k}{\langle\psi|A\rangle}\frac{\langle\widetilde{1C^\perp}|ab_k\rangle}{\langle\widetilde{1C^\perp}|1C^\perp\rangle}, \tag{30}$$
$$u_{k4} = \frac{\alpha_k}{\langle\psi|A^\perp\rangle}\frac{\langle\widetilde{B^\perp 1}|ab_k\rangle}{\langle\widetilde{B^\perp 1}|B^\perp 1\rangle}. \tag{31}$$

Substituting these equations into the equation about $|cd_k\rangle$, we have

$$M|ab_k\rangle = \frac{\beta_k}{\alpha_k}|cd_k\rangle, \ 1 \le k \le 4, \tag{32}$$

where

$$\begin{aligned} M &= r\frac{|00\rangle\langle\widetilde{00}|}{\langle\widetilde{00}|00\rangle} - \frac{1}{r^*}\frac{|BC\rangle\langle\widetilde{BC}|}{\langle\widetilde{BC}|BC\rangle} \\ &+ s\frac{|1C^\perp\rangle\langle\widetilde{1C^\perp}|}{\langle\widetilde{1C^\perp}|1C^\perp\rangle} - \frac{1}{s^*}\frac{|B^\perp 1\rangle\langle\widetilde{B^\perp 1}|}{\langle\widetilde{B^\perp 1}|B^\perp 1\rangle}, \end{aligned} \tag{33}$$

and $r = \frac{\langle\psi^\perp|0\rangle}{\langle\psi|0\rangle}$ and $s = \frac{\langle\psi^\perp|A\rangle}{\langle\psi|A^\perp\rangle}$. A key observation here is that from Eq. (32) we can obtain a very useful form of M as follows:

$$M|00\rangle = r|00\rangle, \tag{34}$$
$$M|BC\rangle = -1/r^*|BC\rangle, \tag{35}$$
$$M|1C^\perp\rangle = s|1C^\perp\rangle, \tag{36}$$
$$M|B^\perp 1\rangle = -1/s^*|B^\perp 1\rangle. \tag{37}$$

Second we turn to show how to determine $|ab_k\rangle$ and $|cd_k\rangle$. Let P be the projector on S, then

$$P = \sum_{k=1}^{4} |S_k\rangle\langle S_k| = \sum_{k=1}^{4} |\Phi_k\rangle\langle\Phi_k|. \quad (38)$$

For simplicity, denote $p = |\langle\psi|0\rangle|^2$, $q = |\langle\psi|A\rangle|^2$, and

$$\rho_1 = p|00\rangle\langle 00| + (1-p)|BC\rangle\langle BC|, \quad (39)$$
$$\rho_2 = q|1C^\perp\rangle\langle 1C^\perp| + (1-q)|B^\perp 1\rangle\langle B^\perp 1|. \quad (40)$$

Then we have

$$\langle\psi|P|\psi\rangle = \sum_{k=1}^{4} |\alpha_k|^2 |ab_k\rangle\langle ab_k| = \rho_1 + \rho_2, \quad (41)$$

which implies that $|ab_k\rangle$ is the eigenvector of $\langle\psi|P|\psi\rangle$ associated with the eigenvalue $|\alpha_k|^2$. The problem left is to find the spectral decomposition of $\langle\psi|P|\psi\rangle$. It is clear that $\rho_1 \perp \rho_2$. So the spectral decomposition of $\langle\psi|P|\psi\rangle$ is just the summation of the spectral decompositions of ρ_1 and ρ_2. Suppose the spectral decompositions of ρ_1 and ρ_2 are given as follows:

$$\rho_1 = \lambda(p)|\Psi_1\rangle\langle\Psi_1| + (1-\lambda(p))|\Psi_2\rangle\langle\Psi_2|,$$
$$\rho_2 = \lambda(q)|\Psi_3\rangle\langle\Psi_3| + (1-\lambda(q))|\Psi_4\rangle\langle\Psi_4|, \quad (42)$$

where

$$\lambda(p) = \frac{1+\sqrt{1-4p(1-p)(1-c_2^2c_3^2)}}{2}. \quad (43)$$

If $\lambda(p) \neq \lambda(q)$ or $1-\lambda(q)$, then $\rho_1+\rho_2$ will have four distinct eigenvalues, namely $\lambda(p)$, $\lambda(q)$, $1-\lambda(p)$, $1-\lambda(q)$, and four unique entangled eigenvectors $\{|\Psi_k\rangle\}$. That means $\langle\psi|P|\psi\rangle$ cannot have product states as its eigenvectors, which contradicts Eq. (41). So we should have $p = q$ or $p = 1-q$. Without loss of generality, let us assume $p = q$ and simply write $\lambda(p)$ as λ. By Eqs. (41) and (42), it should hold that

$$|\Psi_1\rangle\langle\Psi_1| + |\Psi_3\rangle\langle\Psi_3| = |ab_1\rangle\langle ab_1| + |ab_2\rangle\langle ab_2|, \quad (44)$$
$$|\Psi_2\rangle\langle\Psi_2| + |\Psi_4\rangle\langle\Psi_4| = |ab_3\rangle\langle ab_3| + |ab_4\rangle\langle ab_4|. \quad (45)$$

In other words, $|ab_1\rangle$ and $|ab_2\rangle$ are just the two unique orthogonal product states in $span\{|\Psi_1\rangle, |\Psi_3\rangle\}$, and similarly, $|ab_3\rangle$ and $|ab_4\rangle$ are the other two unique orthogonal product states in $span\{|\Psi_2\rangle, |\Psi_4\rangle\}$. So if we can determine $\{|\Psi_k\rangle\}$ then we can also determine $|ab_k\rangle$. To be specific, we only show how to determine $|ab_1\rangle$ (assume the corresponding eigenvalue is λ).

Let $|\Psi_1\rangle = \mu|00\rangle + |BC\rangle$ (unnormalized) be the eigenvector of ρ_1 associated with eigenvalue λ, where μ is some nonzero complex number. Then from $\rho_1|\Psi_1\rangle = \lambda|\Psi_1\rangle$ we have

$$p(\mu + \langle 00|BC\rangle) = \lambda\mu, \quad (46)$$
$$(1-p)(\mu\langle BC|00\rangle + 1) = \lambda, \quad (47)$$

from which we know that both λ and μ are nonzero real numbers. More precisely, μ should satisfy the following equation:

$$\mu^2 - \mu\frac{1-r^2}{r^2c_2c_3} - \frac{1}{r^2} = 0, \quad (48)$$

where we c_k and s_k as abbreviations for $\cos\theta_k$ and $\sin\theta_k$, respectively. Similarly, $|\Psi_3\rangle$ should also be of the form $\mu|1C^\perp\rangle + |B^\perp 1\rangle$, where μ is the same as that in $|\Psi_1\rangle$. This is simply due to the fact that $\langle 1C^\perp|B^\perp 1\rangle = \langle 00|BC\rangle$. So we can write $|ab_1\rangle$ (unnormalized) as

$$|ab_1\rangle = x(\mu|00\rangle + |BC\rangle) + (\mu|1C^\perp\rangle + |B^\perp 1\rangle), \quad (49)$$

where x is a complex number needed to be determined. Substituting $|B\rangle$, $|C\rangle$, $|B^\perp\rangle$, and $|C^\perp\rangle$ into the above equation we have:

$$|ab_1\rangle = x(\mu + c_2c_3)|00\rangle + (xc_2s_3 + s_2)|01\rangle + (xs_2c_3 + \mu s_3)|10\rangle + (xs_2s_3 - \mu c_3 - c_2)|11\rangle. \quad (50)$$

To guarantee that $|ab_1\rangle$ is a product state, x should satisty the following equation:

$$x^2 - x\frac{(1+\mu^2)c_3 + 2\mu c_2}{\mu s_2 s_3} - 1 = 0, \quad (51)$$

which immediately implies that x is a real number. The procedure for determining $|cd_1\rangle$ is almost the same. Employing the spectral decomposition of $\langle\psi^\perp|P|\psi^\perp\rangle$, we can see that $|cd_1\rangle$ is an eigenvector of $\langle\psi^\perp|P|\psi^\perp\rangle$ associated with eigenvalue $1-\lambda$. (Here we have employed the fact that $|\alpha_1|^2 + |\beta_1|^2 = 1$ and $|\alpha_1|^2 = \lambda$.) Furthermore, we can similarly show that $|cd_1\rangle$ should be of the following form:

$$|cd_1\rangle = y(\mu'|00\rangle + |BC\rangle) + (\mu'|1C^\perp\rangle + |B^\perp 1\rangle), \quad (52)$$

where y is chosen in such a way so that the right hand side of the above equation is a product vector. That means y and μ' should satisfy

$$y^2 - y\frac{(1+\mu'^2)c_3 + 2\mu' c_2}{\mu' s_2 s_3} - 1 = 0. \quad (53)$$

Applying Eqs. (32) and (34) (assume $\xi = \frac{\beta_1}{\alpha_1}$) to Eqs. (49) and (52) we have

$$rx\mu = \xi y\mu', \ -x/r^* = \xi y, \ s\mu = \xi\mu', \ -1/s^* = \xi, \quad (54)$$

which follows that

$$\mu' = -|r|^2\mu = -|s|^2\mu, \ (r/s)^* = x/y. \quad (55)$$

Noticing that x, y, and r are all real, we have $s = \pm r$. Assume

$$|\psi\rangle = \sqrt{p}|0\rangle + e^{i\alpha}\sqrt{1-p}|1\rangle,$$
$$|\psi^\perp\rangle = \sqrt{1-p}|0\rangle - e^{i\alpha}\sqrt{p}|1\rangle, \quad (56)$$

where $0 \leq \alpha < 2\pi$. Then by a direct calculation we have

$$r = \sqrt{\frac{1-p}{p}},\ s = \frac{\sqrt{1-p}c_1 - \sqrt{p}s_1 e^{-i\alpha}}{\sqrt{p}c_1 + \sqrt{1-p}s_1 e^{-i\alpha}}. \quad (57)$$

s also can be rewritten into the following form:

$$s = \frac{r - t_1 e^{-i\alpha}}{1 + r t_1 e^{-i\alpha}}.$$

If $r = s$, then it follows that $r^2 = -1$, a contradiction. So $r = -s$. We have

$$e^{i\alpha} = \frac{1-r^2}{2r} t_1.$$

$e^{i\alpha} = \pm 1$, then $(1-r^2)t_1 = \pm 2r$. We also have $y = -x$ and $\mu' = -r^2\mu$. Substituting these two equations into Eq. (53) we have

$$x^2 - x\frac{(1+r^4\mu^2)c_3 - 2\mu r^2 c_2}{r^2 \mu s_2 s_3} - 1 = 0. \quad (58)$$

Comparing Eqs. (51) and (58) we have

$$\frac{(1+r^4\mu^2)c_3 - 2\mu r^2 c_2}{r^2\mu s_2 s_3} = \frac{(1+\mu^2)c_3 + 2\mu c_2}{\mu s_2 s_3},$$

or

$$\mu^2 + \mu\frac{4c_2}{c_3(1-r^2)} - \frac{1}{r^2} = 0. \quad (59)$$

By comparing Eqs. (48) and (59) we have

$$\frac{4c_2}{c_3(1-r^2)} = -\frac{1-r^2}{r^2 c_2 c_3},$$

or

$$(\frac{1-r^2}{r})^2 = -4c_2^2,$$

which is impossible for real number r. With that we complete the proof. ■

VII. UNEXTENDIBILITY IS NOT SUFFICIENT FOR LOCAL INDISTINGUISHABILITY

The notion of unextendible bases (UB) is a generalization of UPB [16]. Let S be a set of linearly independent pure states such that $S^\perp$ contains no product state, then we say S is a UB. Furthermore, if S is a UB and any proper subset of S cannot be a UB, then we say S is a genuinely UB (GUB). It has been shown that the notion of UB is directly connected the local unambiguous distinguishability. That is, a UB S is distinguishable by probabilistic LOCC if and only if it is a GUB [16].

Since orthogonal UPB is a special case of GUB, a natural question is whether any GUB can be used to construct locally indistinguishable subspace. The answer is definitely no. Actually, the notion of UB is introduced to characterize the distinguishability of quantum states by probabilistic LOCC. So there is no direct relation between UB and local (perfect) indistinguishability. Let us consider the following four (unnormalized) states:

$$\begin{aligned} |\Phi_1\rangle &= |000\rangle + e^{i\theta_1}|111\rangle, \\ |\Phi_2\rangle &= |001\rangle + e^{i\theta_2}|110\rangle, \\ |\Phi_3\rangle &= |010\rangle + e^{i\theta_3}|101\rangle, \\ |\Phi_4\rangle &= |011\rangle + e^{i\theta_4}|100\rangle, \end{aligned} \quad (60)$$

where $0 \leq \theta_1 \leq \theta_2 \leq \theta_3 \leq \theta_4 < 2\pi$ and $\theta_4 - \theta_3 \neq \theta_2 - \theta_1$. By a direct calculation one can readily check that $\{|\Phi_k\rangle : 1 \leq k \leq 4\}$ is a UB. However, this set of states is clearly distinguishable by LOCC. Each party only needs to perform a projective measurements according to the standard basis $\{|0\rangle, |1\rangle\}$. Another interesting set of states which spans the orthogonal complement of $\{|\Phi_k\rangle\}$ is as follows:

$$\begin{aligned} |\Psi_1\rangle &= |000\rangle - e^{i\theta_1}|111\rangle, \\ |\Psi_2\rangle &= |001\rangle - e^{i\theta_2}|110\rangle, \\ |\Psi_3\rangle &= |010\rangle - e^{i\theta_3}|101\rangle, \\ |\Psi_4\rangle &= |011\rangle - e^{i\theta_4}|100\rangle, \end{aligned} \quad (61)$$

where $\{\theta_k\}$ is the same as the above equation. Then $\{|\Psi_k\rangle\}$ is also an unextendible bases. Furthermore, let ρ_1 and ρ_2 be two orthogonal mixed states with supports $span\{|\Phi_k\rangle\}$ and $span\{|\Psi_k\rangle\}$, respectively. Then it follows from Ref. [14] that ρ_1 and ρ_2 cannot be unambiguously distinguishable by LOCC. That is, we cannot locally discriminate one of $\{\rho_1, \rho_2\}$ from the other with a nonzero success probability without introducing error. Using the terminology introduced in Ref. [15], we can say that none of ρ_1 and ρ_2 is unambiguously identifiable by stochastic local operations and classical communication (SLOCC). This result is remarkable as it indicates that the local distinguishability of mixed states are rather different from pure states, for which it has been shown that any three linearly independent pure states are SLOCC distinguishable [15]. It would interesting to find similar instance in bipartite scenario.

VIII. LOCALLY INDISTINGUISHABLE SUBSPACE WITH DIMENSIONS 3

Another worthwhile problem is whether there is a locally indistinguishable subspace with dimension 3. Note that any two orthogonal pure states are locally distinguishable. Thus the dimension of a locally indistinguishable subspace is at least 3. For $3 \otimes 3$ quantum system it has been conjectured by King and Matysiak that any subspace with dimension 3 should contain a locally distinguishable orthonormal basis [13]. If this conjecture were true, it would immediately imply that the dimension of any $3 \otimes 3$ locally indistinguishable subspace should

at least be 4. However, for three-qubit system, it is possible to construct a locally indistinguishable subspace with dimension 3. An explicit instance is as follows:

$$\begin{aligned} |\psi_1\rangle &= |000\rangle, \\ |\psi_2\rangle &= |100\rangle - |010\rangle, \\ |\psi_3\rangle &= |100\rangle + |010\rangle + |001\rangle. \end{aligned} \tag{62}$$

Let $S_3 = span\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$. We have the following result.

Theorem 6. S_3 is a locally indistinguishable subspace.

Proof. Note that above states are not normalized, any basis of the subspace spanned by the above three orthogonal states can be expressed as $|\alpha\rangle = (\alpha_1, \alpha_2, \alpha_3)$, $|\beta\rangle = (\beta_1, \beta_2, \beta_3)$ and $|\gamma\rangle = (\gamma_1, \gamma_2, \gamma_3)$ under current basis. To distinguish orthogonal states, one of Alice, Bob, and Charlie can only perform a projective measurement to its own system and the orthogonality between post-measurement states should be preserved. We need to consider the following three cases corresponding to who will perform the first measurement.

Case 1: Alice perform the measurement first. Suppose Alice's measurement is given by the basis $\{|\psi\rangle, |\psi^\perp\rangle\}$, where $|\phi\rangle = a^*|0\rangle + b^*|1\rangle$ and $a \neq 0$. After the measurement, if outcome is 0, the post-measurement state for $|\alpha\rangle$ becomes $(a\alpha_1 + b\alpha_2 + b\alpha_3)|00\rangle + a(\alpha_3 - \alpha_2)|10\rangle + a\alpha_3|01\rangle$. Notice that the state is eliminated only if $|\alpha\rangle = 0$, thus for the same reason, no state is eliminated after Alice's measurement.

The question is now reduced to distinguish three $2 \otimes 2$ orthogonal states. The condition for distinguishability is at least two states are product states. Suppose the two sates are $|\alpha\rangle$ and $|\beta\rangle$, and notice $|\alpha\rangle$ becomes a product state only when $\alpha_3 - \alpha_2 = 0$ or $\alpha_3 = 0$, so we also have $\beta_3 - \beta_2 = 0$ or $\beta_3 = 0$.

case 1.1: $\alpha_3 - \alpha_2 = 0$ and $\beta_3 - \beta_2 = 0$. After measurement, the two states become $|0\alpha'\rangle$ and $|0\beta'\rangle$. The only state orthogonal to them is $|1\gamma'\rangle$, that is $|\gamma\rangle$ also becomes a product state after measurement, thus $\gamma_3 = 0$. But for orthogonality between $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$, we require $\gamma_1 = 0$ and $3\gamma_3 = 2\gamma_2 \neq 0$.

case 1.2: $\alpha_3 = 0$ and $\beta_3 = 0$. After measurement, the states become $|\alpha' 0\rangle$ and $|\beta' 0\rangle$. So again $|\gamma\rangle$ becomes a product state, thus require $\gamma_3 - \gamma_2 = 0$. But only when $\gamma_3 \neq 0$ and $\gamma_1 = \gamma_2 = 0$, could the three states be orthogonal to each other.

case 1.3: $\alpha_3 = 0$ and $\beta_3 - \beta_2 = 0$. After measurement, the two states become $|\alpha' 0\rangle$ and $|0\beta'\rangle$. As they are orthogonal to each other, at leat one of $|\alpha'\rangle$ and $|\beta'\rangle$ equals to $|1\rangle$. So after measurement, $|\gamma\rangle$ should be orthogonal to either $|10\rangle$ or $|01\rangle$, thus $\gamma_3 = 0$ or $\gamma_3 - \gamma_2 = 0$ and we are back to above two subcases.

case 2: Bob does measurement first. In this case the theorem stands as we notice if we exchange the position of Alice and Bob, the three states stay the same.

case 3: Charles does measurement first. After measurement, $|\alpha\rangle$ becomes $(a\alpha_1 + b\alpha_3)|00\rangle + a(\alpha_3 - \alpha_2)|01\rangle + a(\alpha_3 + \alpha_2)|10\rangle$. Notice $|\alpha\rangle$ is eliminated only when $|\alpha\rangle = 0$, thus two states must become product states after measurement. Suppose they are $|\alpha\rangle$ and $|\beta\rangle$, then the following conditions should be satisfied: $\alpha_3 + \alpha_2 = 0$ or $\alpha_3 - \alpha_2 = 0$, and $\beta_3 + \beta_2 = 0$ or $\beta_3 - \beta_2 = 0$. There are three subcases and similar discussion in case 1 can be applied here. ■

IX. LOCALLY INDISTINGUISHABLE SUBSPACE WITH DIMENSIONS 5

It is relatively easier to construct a locally indistinguishable subspace with dimension 5. Consider the subspace $S_5 = span\{|\psi_k\rangle : 1 \leq |\psi_k\rangle \leq 5\}$ where

$$\begin{aligned} |\psi_1\rangle &= |000\rangle, \\ |\psi_2\rangle &= |001\rangle - |100\rangle, \\ |\psi_3\rangle &= |110\rangle - |011\rangle, \\ |\psi_4\rangle &= |001\rangle + |010\rangle + |100\rangle, \\ |\psi_5\rangle &= |110\rangle + |101\rangle + |011\rangle. \end{aligned} \tag{63}$$

Theorem 7. S_5 is locally indistinguishable.

Proof. The proof is rather straightforward. The key is to show the following claim: There is a unique product state $|\psi_1\rangle$ in S_5. We postpone the proof of this claim and see how it implies our result. Let $\{|\phi_k\rangle : 1 \leq k \leq 5\}$ be arbitrary orthonormal basis for S_5. Then there is at least four product states. So

$$\sum_{k=1} \mathrm{Sch}_\perp(|\phi_k\rangle) \geq 2 \times 4 + 1 = 9 > 8.$$

By Theorem 3, we know that $\{|\phi_k\rangle : 1 \leq k \leq 5\}$ cannot be distinguished by LOCC.

Now we prove the above claim. A general state $|\phi\rangle = \alpha_k|\psi_k\rangle$ is expressed as follows:

$$\begin{aligned} |\phi\rangle &= |0\rangle(\alpha_1|00\rangle + (\alpha_2 + \alpha_4)|01\rangle + \alpha_4|10\rangle + (\alpha_5 - \alpha_3)|11\rangle), \\ &+ |1\rangle((\alpha_4 - \alpha_2)|00\rangle + \alpha_5|01\rangle + (\alpha_3 + \alpha_5)|10\rangle), \end{aligned}$$

which is a product vector if and only if

$$\begin{aligned} \alpha_1(\alpha_5 - \alpha_3) &= \alpha_4(\alpha_2 + \alpha_4), \\ \alpha_5(\alpha_3 + \alpha_5) &= 0, \\ \lambda(\alpha_1, \alpha_2 + \alpha_4, \alpha_4, \alpha_5 - \alpha_3) &= (\alpha_4 - \alpha_2, \alpha_5, \alpha_3 + \alpha_5, 0). \end{aligned}$$

However, from the above equations we can easily verify that $\alpha_5 = \alpha_3 = \alpha_4 = \alpha_2 = \lambda = 0$. That is exactly $|\psi_1\rangle$. ■

X. CONCLUSION

The most challenging open problem is to prove (or disprove) that any orthogonal UPB spans a locally indistinguishable subspace. Another worthwhile problem is to

explore the applications of locally indistinguishable subspaces. It has been shown by Watrous that bipartite locally indistinguishable subspaces can be used to construct quantum channels with sub-optimal environment-assisted capacity [6]. However, for multipartite subspace little is known.

This work was partly supported by the National Natural Science Foundation of China (Grant Nos. 60702080, 60736011, and 60621062), the FANEDD under Grant No. 200755, the Hi-Tech Research and Development Program of China (863 project) (Grant No. 2006AA01Z102), and the National Basic Research Program of China (Grant No. 2007CB807901).

[1] R. Duan, Y. Feng, Y. Xin, and M. Ying, arXiv:0705.0795 [quant-ph].
[2] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B.M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[3] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B.M. Terhal, Comm. Math. Phys. **238**, 379 (2003).
[4] N. Alon and L. Lovasz, J. of Combinatorial Theory, Ser. A. **95**, 169 (2001).
[5] J. Niset and N. J. Cerf, Phys. Rev. A **74**, 052103 (2006).
[6] J. Watrous, Phys. Rev. Lett. **95**, 080505 (2005).
[7] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[8] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
[9] M.-Y. Ye, W. Jiang, P. X. Chen, Y. S. Zhang, Z. W. Zhou, G.-C. Guo, quant-ph/0608040.
[10] S. M. Cohen, Phys. Rev. A **75**, 052313 (2007).
[11] S. Bravyi, quant-ph/0310172v1.
[12] P. Hayden and C. King, Quantum Inf. Comput. **5**, 156 (2005).
[13] C. King and D. Matysiak, quant-ph/0510004.
[14] A. Chefles, Phys. Rev. A **69**, 050307(R) (2004).
[15] S. Bandyopadhyay and J. Walgate, quant-ph/0612013.
[16] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Phys. Rev. Lett. **98**, 230502 (2007).
[17] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[18] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).