**Locally indistinguishable subspaces spanned by three-qubit unextendible product bases**

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

| Citation       | Duan, Runyao, Yu Xin, and Mingsheng Ying. “Locally indistinguishable subspaces spanned by three-qubit unextendible product bases.” Physical Review A 81.3 (2010): 032329. © 2010 The American Physical Society |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| As Published   | http://dx.doi.org/10.1103/PhysRevA.81.032329                                                                                                                                                     |
| Publisher      | American Physical Society                                                                                                                                                                        |
| Version        | Final published version                                                                                                                                                                         |
| Citable link   | http://hdl.handle.net/1721.1/58596                                                                                                                                                               |
| Terms of Use   | Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.                                    |
Locally indistinguishable subspaces spanned by three-qubit unextendible product bases

Runyao Duan,†‡ Yu Xin, †‡‡ and Mingsheng Ying†‡,†‡

1Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology, Sydney, New South Wales 2007, Australia
2State 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, People’s Republic of China
3Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
4Department of Physics, Tsinghua University, Beijing 100084, People’s Republic of China

(Received 17 January 2010; published 29 March 2010)

We study the local distinguishability of general multiqubit 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 multiqubit states can be decided efficiently. Another useful consequence is that a set of orthogonal qubit states is locally distinguishable only if the summation of their orthogonal Schmidt numbers is less than the total dimension 2^n. 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. Similar to the bipartite case, these results on multipartite locally indistinguishable subspaces can be used to estimate the one-shot environment-assisted classical capacity of a class of quantum broadcast channels.

DOI: 10.1103/PhysRevA.81.032329 PACS number(s): 03.67.Hk, 03.65.Ud

1. 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 past 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. 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 co-workers [2] and has been thoroughly studied in the literature [3–5]. This notion plays an important role in quantum information theory. Most notably, the orthogonal complement of any UPB can be used to construct bound entangled states. It was also well known that the members of any UPB cannot be perfectly distinguishable by LOCC and thus provide alternative instances for the weird phenomenon “quantum nonlocality without entanglement” [6].

Recently, Watrous introduced a class of interesting bipartite subspaces having no orthonormal bases distinguishable by LOCC [7]. Such subspaces can be intuitively named locally indistinguishable subspaces (LIS). The notion of LIS is not only interesting in their own right but also has an important application in environment-assisted communication, where a friendly environment of a noisy quantum channel can help the receiver to decode the classical messages by performing local measurement and communicating the outcome to the receiver [8,9]. The allowable decoding operations can be further relaxed to general LOCC operations. It was shown that in this model any noisy quantum channel can send at least two messages [10], which is essentially because any two orthogonal pure states can be locally distinguishable [11]. When the dimension of the input state space is 2 the environment-assisted capacity becomes optimum. However, it was unclear whether this is always the case [10]. If so it would imply that the help of environment is really powerful as it makes any channel noiseless in transmitting classical information. Otherwise, it means the existence of a quantum channel which is too noisy to be corrected even with the help of the environment. In the latter case we say the channel has suboptimal capacity.

Watrous employed this notion of LIS to explicitly construct a class of quantum channels with suboptimal environment-assisted classical capacity and thus answered this question in the negative. Winter employed a very different approach to provide some nice lower and upper bounds to the environment-assisted classical capacity [12]. Remarkably, Winter proved that there exists a class of quantum channels with environment-assisted classical capacity approximately 0.5 log_2 d, where d is the dimension of the input state space. This result actually implies the existence of d-dimensional bipartite subspaces with only about √d states locally distinguishable and thus provides stronger instances of LIS. It should be noted that both these results are one-shot, that is, valid only for one use of the quantum channel (Watrous’s case) or for multiple uses but with product input states (Winter’s case). In Ref. [12] the general asymptotic setting has been considered but the arguments there were based on a special form of the famous strong superadditivity of entanglement of formation, which has
been disproved by Hastings very recently [13]. Consequently, we still do not know whether there is a quantum channel with suboptimal environment-assisted classical capacity in an asymptotic setting (allowing multiple uses of the channels and entangled input states). For simplicity, in the following we only consider the one-shot case.

In practice we also need to use quantum channels which have several senders and/or receivers. As a reasonable constraint, these senders (or receivers) can only exchange classical but not quantum messages. When the channel has only one sender but more than one receiver, we call it a quantum broadcast channel. The notion of multipartite LIS is unavoidable if we study the environment-assisted classical capacity of quantum broadcast channels. Actually, for any multipartite LIS, we can construct a broadcast quantum channel which has (one-shot) suboptimal environment-assisted classical capacity. The generalization of LIS from bipartite to multipartite plays a significant role in determining the environment-assisted classical capacity of a class of quantum broadcast channels.

The minimal dimension of locally indistinguishable subspace obtained by Watrous is 8. In Ref. [1] we generalized this result to a multipartite setting and showed that any orthogonal complement of a multipartite pure state with orthogonal Schmidt number of 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 the dimension of indistinguishable subspaces can go. In general, there is no feasible way known to determine whether a given subspace is locally indistinguishable.

In this paper we further develop the theory of local distinguishability of quantum states by combining the notions of UPB and LIS. Let $S$ be an orthogonal UPB, and let $\text{span}(S)$ be the subspace spanned by the members of $S$. We would like to know whether $\text{span}(S)$ is locally indistinguishable. The complete answer to this question is unknown so far mainly because for general multipartite state spaces the structures of UPB and the conditions for local distinguishability remain unsolved. Fortunately, for $2 \otimes 2 \otimes 2$ UPB, we can provide an affirmative answer. These subspaces also have the interesting property that they are indistinguishable by LOCC but have at least an orthonormal basis distinguishable by separable operations. These results give us a class of LIS with dimension 4.

It should be noted that unextendibility itself is not the crucial property for local indistinguishability of a subspace. To see this, we present an explicit $2 \otimes 2 \otimes 2$ subspace which is spanned by a set of locally distinguishable quantum states. As an interesting byproduct, we show that the state space of three qubits can be decomposed into two orthogonal subspaces, both of which are entangled and 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 distinguishability of any two orthogonal pure states [11]. To the best of our knowledge, no such instance was previously known.

Since any two orthogonal pure states are perfectly distinguishable by LOCC [11], the dimension of locally indistinguishable subspace is at least 3. However, it seems a formidable task to find such a subspace. Actually for a $3 \otimes 3$ state space it was conjectured that such a three-dimensional subspace does not exist at all [14]. Fortunately, for a 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 that this subspace is locally indistinguishable follows from the Schmidt-number-summation criterion about the local distinguishability for multiqubit system.

The rest of this paper is organized as follows. In Sec. II we review basic definitions and notions that are useful in studying LOCC discrimination. Then in Sec. 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 [15]. We apply this criterion in Sec. IV to show that local projective measurements and classical communication are sufficient to perfectly distinguish multiqubit orthogonal quantum states. As a direct consequence, we show that a set of multiqubit 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 Sec. 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 these preparations, we are ready to present our main result in Sec. VI: that any subspace spanned by a three-qubit UPB is locally indistinguishable. In this section we also describe the connection between tripartite LIS and environment-assisted classical capacity of quantum broadcast channels with two receivers. Section VII clarifies the relation between indistinguishability 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 Secs. VIII and IX, respectively. We conclude the paper in Sec. X. Several unsolved problems are also proposed for further study.

II. PRELIMINARIES

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

We first recall some useful definitions introduced by Walgate and Hardy [15]. When discriminating a set of states, we need to perform suitable measurements $M_{mn}$ on the system to obtain useful information about the real identity of the states. If $M^a_m$ 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 nontrivial if at least one of its measurement operators is not trivial.
Any finite LOCC protocol that discriminates a set of orthogonal multiparticle states, \( \{\rho_1, \ldots, \rho_N\} \) 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 nontrivial measurement. This simple observation leads us to the following definition:

**Definition 1.** Suppose Alice, Bob, \ldots 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 nontrivial measurement.

After performing a nontrivial measurement, Alice, Bob, \ldots need to discriminate a new set of (unnormalized) states \( \{M_n\rho_kM_n^\dagger : k = 1, \ldots, N\} \) 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 \( \{\rho_1, \ldots, \rho_N\} \) be a set of orthogonal states. A measurement operator \( M_n \) is called orthogonality-keeping if states in the set \( \{M_n\rho_kM_n^\dagger : k = 1, \ldots, N\} \) remain orthogonal. A complete measurement \( \{M_n\} \) is said to be orthogonality-keeping if each \( M_n \) is orthogonality-keeping.

For a positive operator \( \rho \), \( \text{Supp}(\rho) \) represents the support of \( \rho \). In other words, \( \text{Supp}(\rho) \) is the subspace spanned by the eigenvectors of \( \rho \) corresponding to the positive eigenvalues.

We shall need the following technical lemma:

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

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

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

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 \( \rho \) be a general quantum state. The orthogonal Schmidt number of \( \rho \), denoted as \( \text{Sch}_\perp(\rho) \), is the minimal number orthogonal product states needed to span the support of \( \rho \). 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. [15], 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 secretly chosen from \( N \) orthogonal 2 \( \otimes n \) states, say \( \rho_1, \ldots, \rho_N \), 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 \( \{0\rangle, \{1\rangle\} \) such that, for any \( |\psi_l\rangle \in \text{Supp}(\rho_k) \), we have

\[
|\psi_l\rangle = |0\rangle_A |\psi_0^{(k)}\rangle_B + |1\rangle_A |\psi_1^{(k)}\rangle_B,
\]

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

**Proof.** Many proof techniques are borrowed from Ref. [15]. The sufficiency is obvious. If there exists an orthonormal basis \( \{0\rangle, \{1\rangle\} \) such that Eq. (1) holds, then each \( \rho_k \) should be of the following form:

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

where \( \rho_{mn}^{(k)} \) 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 \( \{0\rangle, \{1\rangle\} \) and sends the outcome \( m \) to Bob.
2. **Bob** performs a nontrivial measurement and then broadcasts the outcome \( l \).
3. **Alice** measures her qubit according to the basis \( \{0\rangle, \{1\rangle\} \) if and only after Alice performs some suitable projective measurement.

Now we turn to show the necessity. Suppose that \( \rho_1, \ldots, \rho_N \) 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 \( |\psi_l\rangle \in \text{Supp}(\rho_k) \) and \( |\psi_l\rangle \in \text{Supp}(\rho_l) \), we have

\[
\langle\psi_l| M_m^\dagger M_m \otimes I |\psi_l\rangle = 0,
\]

\[
\langle\psi_l|\psi_l\rangle = 0,
\]

where the second equation follows from the fact that \( \rho_k \) and \( \rho_l \) are orthogonal. Let

\[
M_m^\dagger M_m = \alpha |0\rangle\langle 0| + \beta |1\rangle\langle 1|
\]

be the spectral decomposition, where \( \alpha > \beta \geq 0 \) by the non triviality. Rewriting

\[
|\psi_l\rangle = |0\rangle |\psi_0^{(k)}\rangle + |1\rangle |\psi_1^{(k)}\rangle,
\]

\[
|\psi_l\rangle = |0\rangle |\psi_l^{(k)}\rangle + |1\rangle |\psi_1^{(k)}\rangle.
\]

we then have

\[
\alpha |\psi_0^{(k)}\rangle_{\psi_1^{(k)}}\rangle + \beta |\psi_1^{(k)}\rangle_{\psi_1^{(k)}\rangle} = 0,
\]

\[
|\psi_0^{(k)}\rangle_{\psi_0^{(k)}}\rangle + |\psi_1^{(k)}\rangle_{\psi_1^{(k)}\rangle} = 0.
\]

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

Intuitively speaking, this 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 \( \rho_1, \ldots, \rho_N \) can be perfectly discriminated by LOCC if and only if there exists an
orthogonal basis \(\{|0\rangle, |1\rangle\}_A\) such that each \(\rho_k\) has the form
\[
\rho_k = \sum_{m,n=0}^{1} |m\rangle\langle n| \otimes \rho_{mn}^{(k)},
\]
where \(\rho_{mn}^{(1)}, \ldots, \rho_{mn}^{(N)}\) 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 MULTIQUBIT STATES

A simple but remarkable consequence of Theorem 1 is that local projective measurements and classical communication are powerful enough to locally distinguish a set of multiqubit orthogonal quantum states. Due to its importance, 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 multiqubit orthogonal quantum states. The theorem simplifies the local distinguishability of multiqubit considerably and makes it almost feasible to locally distinguish a set of multiqubit orthogonal states. Procedure can be described as follows. Suppose \(n\) qubits are held by Alice\(1, \ldots, Alice_n\), respectively. Then any set of \(n\)-qubit orthogonal states can be perfectly distinguishable by LOCC if and only if they can be distinguished by local projective measurements and classical communication (LPMCC). Let \(\sigma\) 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 nontrivial measurement depending on \(Alice_{\sigma(1)}\)'s outcome, \(\ldots, Alice_{\sigma(n)}\) is the last one who performs conditional projective measurement depending on the previous \(n - 1\) party's outcomes. The projective measurement performed by \(Alice_{\sigma(1)}\) is given by an orthogonal basis \(\{\psi_{\sigma(1)}(x_1)\} : x_1 = 0, 1\) for outcomes. \(Alice_{\sigma(2)}\) performs a projective measurement \(\{\psi_{\sigma(2)}(x_1 x_2)\} : x_2 = 0, 1\) with outcome \(x_2\). Finally, depending on the previous outcomes \(x_1, \ldots, x_{n-1}\), \(Alice_{\sigma(n)}\) performs a conditional projective measurement \(\{\psi_{\sigma(n)}(x_1 x_2 \ldots x_n)\} : x_n = 0, 1\). This procedure induces a projective measurement on \(n\) qubits represented by an orthogonal product basis \(\{\psi(x)\} : x \in \{0, 1\}^n\),

\[
\psi(x) = \|\psi_{\sigma(1)}(x_1)\rangle \otimes \cdots \otimes |\psi_{\sigma(n)}(x_1 x_2 \ldots x_n)\rangle.
\]

It is clear that \(\rho_1, \ldots, \rho_N\) are perfectly distinguishable by \(Alice_{1, \ldots, Alice_n}\) if and only if they lead to different (nonoverlap) measurement outcomes. That is, there exists a permutation \(\sigma\), and a disjoint partition of \(\{0, 1\}^n\), say \(O_1, \ldots, O_N\), such that
\[
\text{Supp}(\rho_k) \subseteq \text{span}\{\psi(x) : x \in O_k\}.
\]

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

Equation (11) implies a simple but highly nontrivial criterion for local distinguishability of a set of multiqubit states.

**Theorem 3.** Let \(S = \{\rho_1, \ldots, \rho_N\}\) 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 \(\rho_k\) is not more than the total dimension of state space, that is,
\[
\sum_{k=1}^{N} \text{Sch}_\perp(\rho_k) < 2^n.
\]

A few remarks are in order. Equation (12) reflects the fact that local projective measurements and classical communication are sufficient for locally distinguishing multiqubit quantum states. In general, only projective measurements are usable 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 [16]. We would also like to point out that Eq. (12) is not sufficient when the number of qubits under consideration is more than 2. There do exist four \(2 \otimes 2 \otimes 2\) orthogonal 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
\[
\alpha|00 \cdots 0\rangle + \beta|11 \cdots 1\rangle
\]
and
\[
\alpha_1|00 \cdots 1\rangle + \alpha_2|0 \cdots 01\rangle + \cdots + \alpha_n|10 \cdots 0\rangle,
\]
where each \(\alpha_k\) is a 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 least \(2^n/n\) W-type states that can be locally distinguishable. In particular, any three 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 in 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 \(\{\psi, |\psi^\perp\rangle\}\). If \(|\psi\rangle \notin \{0, 1\}\) (up to some phase factor), then after the measurement two GHZ-type states will reduce to identical states such as \(|0^0 n-1\rangle\) or \(|1^0 n-1\rangle\) and thus cannot be further distinguished. If \(|\psi\rangle \notin \{0, 1\}\), 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 the induction hypothesis.
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 $S = \{\rho_1, \ldots, \rho_N\}$ be a set of 2 $\otimes$ 2 orthogonal states. Then $S$ is locally distinguishable if and only if
$$\sum_{k=1}^N \text{SCH}_⊥(\rho_k) \leq 4.$$

**Proof.** If each $\rho_k$ is a pure state, then Theorem 4 is reduced to the one given by Walgate and Hardy [15]. Here we need to consider the case when some state may be mixed. We consider three cases according to the number of states. First we consider the case of $N = 2$. By Eq. (12) of Theorem 3, we only need to consider the sufficiency. If both $\rho_1$ and $\rho_2$ are mixed states. Then we should have $\text{SCH}_⊥(\rho_1) = \text{SCH}_⊥(\rho_2) = 2$. That means there exists a set of orthogonal product states \(\{|\Psi_k\rangle : 1 \leq k \leq 4\}\) such that
$$\text{Supp}(\rho_1) = \text{Supp}(\rho_2) = \text{Supp}(\rho_3) = \text{Supp}(\rho_4) = \text{span}\{|\Psi_1\rangle, |\Psi_2\rangle\},$$
$$\text{Supp}(\rho_5) = \text{span}\{|\Psi_3\rangle, |\Psi_4\rangle\}.$$ (15) (16)

Applying the result of Walgate and Hardy [15], 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 $\rho_1$; otherwise, it is $\rho_2$. Using similar arguments, we can prove the case when only one of $\rho_1$ and $\rho_2$ 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. [15].

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 orthogonal two-qubit states \(\{\rho_1, \ldots, \rho_N\} (2 \leq N \leq 4)\) is locally distinguishable if and only if their orthogonal Schmidt numbers belongs to one of the following cases: \(\{3, 1\}\), \(\{2, 2\}\), \(\{2, 1, 1\}\), \(\{1, 1, 1\}\), \(\{2, 2\}\), \(\{1, 1, 1\}\), or \(\{1, 1\}\).

Employing Theorem 4, we can show there exists pairs of orthogonal 2 $\otimes$ 2 quantum states that are locally indistinguishable. Let $\rho_1$ be a uniform mixture of \((|00\rangle + |11\rangle)\), and let $\rho_2$ be a uniform mixture of \((|−\rangle + |1−\rangle)\). It is clear that both $\rho_1$ and $\rho_2$ are separable. However, we have
$$\text{SCH}_⊥(\rho_1) = \text{SCH}_⊥(\rho_2) = 3,$$
which immediately implies that $\rho_1$ and $\rho_2$ are locally indistinguishable as the sum exceeds 4. The indistinguishability between $\rho_1$ and $\rho_2$ has already been proven in Ref. [6], and it 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 $|\psi\rangle = \alpha|−\rangle + \beta|1−\rangle$ and $\alpha\beta \neq 0$, then $\rho_1$ and $\rho_3$ are indistinguishable as $\text{SCH}_⊥(\rho_1) + \text{SCH}_⊥(\rho_3) = 5 > 4$.

VI. LOCALLY INDISTINGUISHABLE SUBSPACES SPANNED BY 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 a locally indistinguishable subspace was given by Watrous [7]. For completeness, we give a short review here. Let $|\Phi\rangle$ be a $d \otimes d$ maximally entangled state, then it was proven that $|\langle\Phi\rangle|^{\perp}$ is locally indistinguishable whenever $d > 2$. Actually, what was shown in Ref. [7] is that $|\langle\Phi\rangle|^{\perp}$ has no orthonormal basis perfectly distinguishable by separable operations rather than LOCC. With this subspace, Watrous constructed a class of quantum channels which have suboptimal environment-assisted classical capacity and thus solved an open problem suggested by Hayden and King [10]. 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 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 do not know whether there are locally indistinguishable subspaces with dimensions 3, 4, or 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 a 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 orthogonal UPB and have bases distinguishable by separable operations. We discuss the case of dimension 4 here; the other two cases will be discussed in the next section.

Before getting into the proof details, let us briefly mention how the notion of multipartite LHS can be used to estimate the environment-assisted classical capacity of quantum broadcast channels. For simplicity and without loss of generality, we only consider the tripartite case. Let $S = \text{span}\{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ be a $d$-dimensional tripartite subspace of $\mathcal{H}_{BCD} = \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$. For a $d$-dimensional state space $\mathcal{H}_A = \text{span}\{|1\rangle, \ldots, |d\rangle\}$, we can define an isometry $U$ from $\mathcal{H}_A$ to $\mathcal{H}_{BCD}$ as follows:
$$U = \sum_{i=1}^d |\psi_i^{BCD}\rangle\langle i^A|.$$ (17)

Then we can further construct a quantum broadcast channel $E$ with the sender $A$, the receivers $C$ and $D$, and the environment $B$ as follows:
$$E(\rho^A) = \text{Tr}_B(U\rho^A U^\dagger),$$
where the output state is in $\mathcal{B}(\mathcal{H}_{CD})$. The connection between $S$ and the environment-assisted classical capacity of $E$ is not difficult to see: $E$ can transmit $k$ classical messages exactly from $A$ to $C$ and $D$, with the help of $B$ if and only if there are $k$ states in $S$ that are locally distinguishable. In particular, $S$ is locally indistinguishable if and only if $E$ is
with suboptimal environment-assisted classical capacity. Due to this connection, we can define $\alpha(S)$ to be the maximal number of locally distinguishable states in $S$. Clearly, $\alpha(S)$ represents the one-shot environment-assisted capacity of $E$, or the one-shot zero-error local classical capacity of isometry $U$ [19]. In the following we shall construct a class of LIS $S$ and also compute the exact value for $\alpha(S)$.

Note that any UPB for three qubits should have four members, and it can be uniquely written into the following form (up to some local unitary) [20]:

\[
\begin{align*}
|S_1\rangle & = |0\rangle \otimes |0\rangle \otimes |0\rangle, \\
|S_2\rangle & = |1\rangle \otimes |B\rangle \otimes |C\rangle, \\
|S_3\rangle & = |A\rangle \otimes |1\rangle \otimes |C+\rangle, \\
|S_4\rangle & = |A+\rangle \otimes |B-\rangle \otimes |1\rangle,
\end{align*}
\]

(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 $\{S_k : 1 \leq k \leq 4\}$ 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 $\{\Phi_k\} : 1 \leq k \leq 4\}$ of $S$ is uniquely determined by a $4 \times 4$ unitary matrix $U$ as follows:

\[
|\Phi_k\rangle = u_{k1}|S_1\rangle + u_{k2}|S_2\rangle + u_{k3}|S_3\rangle + u_{k4}|S_4\rangle, \quad 1 \leq k \leq 4,
\]

(18)

We shall consider five cases to complete the proof. By symmetry, we may assume that Alice is the one who goes first. The basic idea is to show after Alice performs a projective measurement $|\psi\rangle$, $|\psi^\perp\rangle$; the post-measurement states are indistinguishable. We shall employ an interesting property about $S$: There are only four different product states in $S$. A proof of this fact was given in Ref. [20]. One can also prove it by a direct calculation.

Case 1. There are four product states in $\{|\Phi_k\rangle : 1 \leq k \leq 4\}$. They are just the UPB $\{S_k : 1 \leq k \leq 4\}$; thus they are locally indistinguishable [2]. A direct proof is as follows. If $|\psi\rangle \not\in \{|0\rangle, |A\rangle\}$, 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 $\{|\Phi_k\rangle : 1 \leq k \leq 4\}$. This case cannot happen.

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

\[
\begin{align*}
|S_1\rangle, |S_2\rangle, \\
u_1^1|S_1\rangle + u_2^1|S_4\rangle, \\
u_2^2|S_1\rangle - u_1^1|S_4\rangle,
\end{align*}
\]

(19)

(20)

(21)

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

\[
|00\rangle, \\
u_1^1|00\rangle|C^+\rangle + u_2^1|00\rangle|B^-1\rangle,
\]

(22)

(23)

which contains two entangled states and one product state. It follows from Ref. [15] that they cannot be perfectly distinguishable by LOCC. If $|\psi\rangle \not\in \{|0\rangle, |1\rangle, |A\rangle\}$, then the left states are not orthogonal to each other. If $|\psi\rangle \not\in \{|0\rangle, |1\rangle, |A\rangle\}$, then the left states are not orthogonal to each other.

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

Case 5. There are 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:

\[
|\Phi_k\rangle = \alpha_k|\psi\rangle \otimes |ab_k\rangle + \beta_k|\psi^\perp\rangle \otimes |cd_k\rangle, \quad 1 \leq k \leq 4,
\]

(25)

where $\alpha_k$ and $\beta_k$ are nonzero complex numbers such that $|\alpha_k|^2 + |\beta_k|^2 = 1$, and $|ab_k\rangle$ and $|cd_k\rangle$ 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 $\{|00\rangle, |BC\rangle, |C^+\rangle, |B^-1\rangle\}$. Let $\{|00\rangle, |BC\rangle, |C^+\rangle, |B^-1\rangle\}$ be its reciprocal basis.

First we have

\[
\begin{align*}
\alpha_k|ab_k\rangle & = u_{k1}|\psi\rangle|00\rangle + u_{k2}|\psi\rangle|BC\rangle, \\
\beta_k|cd_k\rangle & = u_{k1}|\psi^\perp\rangle|00\rangle + u_{k2}|\psi^\perp\rangle|BC\rangle,
\end{align*}
\]

(26)

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

\[
\begin{align*}
u_{k1} & = \frac{\alpha_k}{\langle \psi |00\rangle}, \\
u_{k2} & = \frac{\alpha_k}{\langle \psi |BC\rangle}, \\
u_{k3} & = \frac{\alpha_k}{\langle \psi |C^+\rangle}, \\
u_{k4} & = \frac{\alpha_k}{\langle \psi |B^-1\rangle}.
\end{align*}
\]

(28)

(29)

(30)

(31)

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

\[
M|ab_k\rangle = \frac{\beta_k}{\alpha_k}|cd_k\rangle, \quad 1 \leq k \leq 4,
\]

(32)

where

\[
M = r \frac{|00\rangle\langle 00|}{|00\rangle\langle 00|} + \frac{1}{r^*} \frac{|BC\rangle\langle BC|}{|BC\rangle\langle BC|} + \frac{1}{s^*} \frac{|C^+\rangle\langle C^+|}{|C^+\rangle\langle C^+|} - \frac{1}{s} \frac{|B^-1\rangle\langle B^-1|}{|B^-1\rangle\langle B^-1|},
\]

(33)
and \( r = \frac{\langle \psi|0 \rangle}{|\psi|0 \rangle} \) and \( s = \frac{\langle \psi|A \rangle}{|\psi|A \rangle} \). A key observation here is that from Eq. (32) we can obtain a very useful form of \( M \) as follows:

\[
M(00) = r(00),
\]
\[
M|BC\rangle = -1/r^*|BC\rangle,
\]
\[
M|C\rangle = s|1\rangle + \lambda|1\rangle,
\]
\[
M|B^\perp\rangle = -1/s^*|B^\perp\rangle.
\]  

Second we show how to determine \(|ab_1\rangle\) and \(|cd_1\rangle\). Let \( P \) be the projector on \( S \), then

\[
P = \sum_{k=1}^{4} |S_k\rangle \langle S_k| = \sum_{k=1}^{4} |\Phi_2\rangle \langle \Phi_2|.
\]

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

\[
\rho_1 = p|00\rangle \langle 00| + (1 - p)|BC\rangle \langle BC|,
\]
\[
\rho_2 = q|1\rangle + |1\rangle + (1 - q)|B^\perp\rangle \langle B^\perp|.
\]

Then we have

\[
\langle \psi|P|\psi\rangle = \sum_{k=1}^{4} |\alpha_k|^2 \langle ab_1| \langle ab_1| = \rho_1 + \rho_2,
\]

which implies that \(|ab_1\rangle\) is the eigenvector of \( \langle \psi|P|\psi\rangle \) associated with the eigenvalue \(|\alpha_1|^2\). 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 respective spectral decompositions of \( \rho_1 \) and \( \rho_2 \). Suppose the spectral decompositions of \( \rho_1 \) and \( \rho_2 \) are given as follows:

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

where

\[
\lambda(p) = \frac{1 + \sqrt{-4p(1 - p)(1 - c^2_k c^2_s)}}{2}.
\]

If \( \lambda(p) \neq \lambda(q) \) or \( 1 - \lambda(p), \) then \( \rho_1 + \rho_2 \) will have four distinct eigenvalues, namely \( \lambda(p), \lambda(q), 1 - \lambda(p), \) and \( 1 - \lambda(q), \) and four unique entangled eigenvectors \(|\Psi_j\rangle\). 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 \( \lambda \). By Eqs. (41) and (42), it should hold that

\[
|\Psi_1\rangle \langle \Psi_1| + |\Psi_3\rangle \langle \Psi_3| = |ab_1\rangle \langle ab_1| + |ab_2\rangle \langle ab_2|,
\]
\[
|\Psi_2\rangle \langle \Psi_2| + |\Psi_4\rangle \langle \Psi_4| = |ab_3\rangle \langle ab_3| + |ab_4\rangle \langle ab_4|.
\]

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 \(|\Psi_3\rangle\) then we can also determine \(|ab_1\rangle\). To be specific, we only show how to determine \(|ab_1\rangle\) (assuming the corresponding eigenvalue is \( \lambda \)).

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

\[
p(\mu + |00\rangle \langle BC\rangle) = \lambda \mu,
\]
which implies that \(|ab_1\rangle\) is the eigenvector of \( \rho_1 \) associated with eigenvalue \( \lambda \), where \( \mu \) is some nonzero complex number. Then from \( \rho_1|\Psi_1\rangle = \lambda|\Psi_1\rangle \) we have

\[
 (1 - p)(\mu|BC\rangle|00\rangle + 1) = \lambda,
\]
from which we know that both \( \lambda \) and \( \mu \) are nonzero real numbers. More precisely, \( \mu \) should satisfy the following equation:

\[
\mu^2 - \mu \frac{1 - r^2}{r^2 c_2 s_2} - 1 = 0,
\]

where we use \( c_2 \) and \( s_1 \) as abbreviations for \( \cos \theta_2 \) and \( \sin \theta_2 \), respectively. Similarly, \( |\Psi_3\rangle \) should also be of the form \(|1\rangle + |B^\perp\rangle, \) where \( \mu \) is the same as that in \(|\Psi_1\rangle\). This is simply because \(|1\rangle + |B^\perp\rangle = (00)|BC\rangle \). So we can write \(|ab_1\rangle\) (unnormalized) as

\[
|ab_1\rangle = x(|00\rangle + |BC\rangle) + (\mu|1\rangle + |B^\perp\rangle),
\]

where \( x \) is a complex number needed to be determined. Substituting \(|B\rangle, |C\rangle, |B^\perp\rangle, |C^\perp\rangle \) into this equation we have

\[
|ab_1\rangle = x(\mu + c_3 c_5)|00\rangle + (c_3 s_3 + s_2)|01\rangle
\]
\[
+ (s_3 c_3 + \mu s_5)|10\rangle + (s_3 s_3 - \mu c_3 - c_2)|11\rangle.
\]

To guarantee that \(|ab_1\rangle\) is a product state, \( x \) should satisfy the following equation:

\[
x^2 - x(1 + \mu^2)c_3 + 2\mu c_2 = 1 = 0,
\]

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 \(|\psi^+\rangle |P|\psi^+\rangle\), we can see that \(|cd_1\rangle\) is an eigenvector of \(|\psi^+\rangle |P|\psi^+\rangle\) associated with eigenvalue \( 1 - \lambda \). 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:

\[
|cd_1\rangle = y(\mu^*|00\rangle + |BC\rangle) + (\mu^*|1\rangle + |B^\perp\rangle),
\]

where \( y \) is chosen in such a way so that the right-hand side of this equation is a product vector. That means \( y \) and \( \mu' \) should satisfy

\[
y^2 - y(1 + \mu^2)c_3 + 2\mu' c_2 = 1 = 0.
\]

Applying Eqs. (32) and (34) (assuming \( \xi = \frac{\lambda}{\mu} \)) to Eqs. (49) and (52) we have

\[
rx\mu = \xi y \mu', \quad -x/r^* = \xi y, \quad s\mu = \xi \mu', \quad -1/s^* = \xi,
\]

from which it follows that

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

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

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

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

\[
r = \sqrt{1 - p \over p}, \quad s = \sqrt{1 - pc_1 - sp_1 e^{-i\alpha}} \over \sqrt{pc_1 + sp_1 e^{-i\alpha}}.
\]
s also can be rewritten in 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

\[ e^{i\alpha} = \frac{1 - r^2}{2r} \]

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

\[ x^2 - x \left( 1 + r^4 \mu^2 \right) c_3 - 2r \mu r^2 c_2 = 0. \]  

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

\[ r^2 \mu \epsilon^2 \epsilon \mu = \frac{1 + r^4 \mu^2 c_3 - 2r \mu r^2 c_2}{r^2 \mu \epsilon^2 \mu}, \]

or

\[ \mu^2 + \mu - \frac{4c_2}{c_1(1 - r^2)} - \frac{1}{r^2} = 0. \]  

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

\[ \frac{4c_2}{c_1(1 - r^2)} = \frac{1 - r^2}{r^2 c_2 c_3}, \]

or

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

which is impossible for real number \( r \). With that we complete the proof.

Noticing that any three orthogonal multipartite product states are locally distinguishable [3], we can actually determine that \( \alpha(S) = 3 \).

VII. UNEXTENDIBILITY IS NOT SUFFICIENT FOR LOCAL INDISTINGUISHABILITY

The notion of unextendible bases (UB) is a generalization of UPB [21]. Let \( S \) be a set of linearly independent pure states such that \( S \) 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 to the local unambiguous distinguishability. That is, a UB \( S \) is distinguishable by probabilistic LOCC if and only if it is a GUB [21].

Since orthogonal UPB is a special case of GUB, a natural question is whether any GUB can be used to construct a 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:

\[ |\Phi_1\rangle = |000\rangle + e^{i\theta_1}|111\rangle, \]

\[ |\Phi_2\rangle = |001\rangle + e^{i\theta_2}|110\rangle, \]

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 projective measurements according to the standard basis \([0, 1]\). Another interesting set of states which spans the orthogonal complement of \( \{|\Phi_k\rangle\} \) is as follows:

\[ |\Psi_1\rangle = |000\rangle - e^{i\theta_1}|111\rangle, \]

\[ |\Psi_2\rangle = |001\rangle - e^{i\theta_2}|110\rangle, \]

\[ |\Psi_3\rangle = |010\rangle - e^{i\theta_3}|101\rangle, \]

\[ |\Psi_4\rangle = |011\rangle - e^{i\theta_4}|100\rangle, \]

where \( \{|\Psi_k\rangle\} \) is also an unextendible bases. Furthermore, let \( \rho_1 \) and \( \rho_2 \) be two orthogonal mixed states with supports span\(\{|\Phi_k\rangle\}\) and span\(\{|\Psi_k\rangle\}\), respectively. Then it follows from Ref. [22] that \( \rho_1 \) and \( \rho_2 \) cannot be unambiguously distinguishable by LOCC. That is, we cannot locally discriminate one of \( \rho_1 \) and \( \rho_2 \) from the other with a nonzero success probability without introducing error. Using the terminology introduced in Ref. [23], we can say that none of \( \rho_1 \) and \( \rho_2 \) 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 is rather different from pure states, for which it has been shown that any three linearly independent pure states are SLOCC distinguishable [23]. It would be interesting to find similar instance in the bipartite scenario. Actually, just after the initial posting of this work (arXiv:0708.3559), an orthogonal bipartition of a bipartite state space 3 \( \otimes \) 4 has been found by Cubitt and collaborators [24].

VIII. LOCALLY INDISTINGUISHABLE SUBSPACE WITH DIMENSION 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 a 3 \( \otimes \) 3 quantum system it has been conjectured by King and Matsyuk that any subspace with dimension 3 should contain a locally distinguishable orthonormal basis [14]. 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 a three-qubit system, it is possible to construct a locally indistinguishable subspace with dimension 3. An explicit instance is as follows:

\[ |\psi_1\rangle = |000\rangle, \]

\[ |\psi_2\rangle = |100\rangle - |010\rangle, \]

\[ |\psi_3\rangle = |100\rangle + |010\rangle + |001\rangle. \]

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

Theorem 6. \( S_3 \) is a locally indistinguishable subspace. Thus \( \alpha(S_3) = 2 \).
Proof. Note that these states are not normalized, so any basis of the subspace spanned by these three orthogonal states can be expressed as $|\alpha\rangle = |\alpha_1, \alpha_2, \alpha_3\rangle$, $|\beta\rangle = |\beta_1, \beta_2, \beta_3\rangle$, and $|\gamma\rangle = |\gamma_1, \gamma_2, \gamma_3\rangle$ under the 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 performs the measurement first. Suppose Alice’s measurement is given by the basis $\{|\psi_+\rangle, |\psi_1\rangle\}$, where $|\alpha\rangle = a^*|0\rangle + b^*|1\rangle$ and $a \neq 0$. After the measurement, if the outcome is 0, the post-measurement state for $|\alpha\rangle$ becomes $(aa_1 + ba_2 + ba_3)|00\rangle + a(a_3 - a_2)|10\rangle + a(a_3 - a_2)|01\rangle$. 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 distinguishing three $2 \otimes 2$ orthogonal states. The condition for distinguishability is that at least two states are product states. Suppose the two states are $|\alpha\rangle$ and $|\beta\rangle$, and notice that $|\alpha\rangle$ becomes a product state only when $a_3 - a_2 = 0$ and $\alpha_3 = 0$, so we also have $\beta_3 - \beta_2 = 0$ or $\beta_3 = 0$.

Case 1.1: $a_3 - a_2 = 0$ and $\beta_3 - \beta_2 = 0$. After measurement, the two states become $|00\rangle$ and $|00\rangle$. The only state orthogonal to them is $|1y\rangle$; that is, $|\gamma\rangle$ also becomes a product state after measurement, and thus $\gamma_3 = 0$. For orthogonality among $|\alpha\rangle$, $|\beta\rangle$, and $|\gamma\rangle$, we require $\gamma_1 = 0$ and $3\beta_3 = 2\gamma_2 \neq 0$.

Case 1.2: $a_3 = 0$ and $\beta_3 = 0$. After measurement, the states become $|000\rangle$ and $|000\rangle$. So again $|\gamma\rangle$ becomes a product state, and this requires $\gamma_3 = 2\gamma_2 = 0$. But only when $\gamma_3 = 2\gamma_2 = 0$ could the three states be orthogonal to each other.

Case 1.3: $a_3 = 0$ and $\beta_3 - \beta_2 = 0$. After measurement, the two states become $|00\rangle$ and $|0\rangle$. As they are orthogonal to each other, at least one of $|\alpha\rangle$ and $|\beta\rangle$ equals $|1\rangle$. So after measurement, $|\gamma\rangle$ should be orthogonal to either $|10\rangle$ or $|01\rangle$, and thus $\gamma_3 = 0$ or $\gamma_3 = 2\gamma_2 = 0$, and we return to the two previous subcases.

Case 2: Bob does the 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 the measurement first. After measurement, $|\alpha\rangle$ becomes $(aa_1 + ba_2 + ba_3)|00\rangle + a(a_3 - a_2)|01\rangle + a(a_3 + a_2)|10\rangle$. Notice that $|\alpha\rangle$ is eliminated only when $|\alpha\rangle = 0$, and thus two states must become product states after measurement. Suppose they are $|\alpha\rangle$ and $|\beta\rangle$, then the following conditions should be satisfied: $a_3 + a_2 = 0$ or $a_3 - a_2 = 0$ and $\beta_3 + \beta_2 = 0$ or $\beta_3 - \beta_2 = 0$. There are three subcases and a similar discussion to that in Case 1 can be applied here.

IX. LOCALLY INDISTINGUISHABLE SUBSPACE WITH DIMENSION 5

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

$|\psi_1\rangle = |000\rangle$, $|\psi_2\rangle = |001\rangle - |100\rangle$, $|\psi_3\rangle = |110\rangle - |011\rangle$, $|\psi_4\rangle = |001\rangle + |101\rangle + |110\rangle$, $|\psi_5\rangle = |110\rangle + |101\rangle + |011\rangle$. (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 $S_5$ (up to a scalar). We postpone the proof of this claim and show how it implies our result. Let $\{|\phi_k\rangle : 1 \leq k \leq 5\}$ be an arbitrary orthonormal basis for $S_5$. Then there is at least four entangled states. So

$$\sum_{k=1}^{5}\text{Sch}_\perp(|\phi_k\rangle) \geq 2 \times 4 + 1 = 9 > 8.$$  

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

Now we prove this claim. A general state $|\phi\rangle = \sum_{k=1}^{5}a_k|\psi_k\rangle$ is expressed as follows:

$|\phi\rangle = |0\rangle(a_1|00\rangle + (a_2 + a_4)|01\rangle + a_5|10\rangle + (a_5 - a_3)|11\rangle)$

$+ |1\rangle(a_4 - a_2)|00\rangle + a_5|01\rangle + (a_3 + a_5)|10\rangle)$,

which is a product vector if and only if

$$a_1(a_5 - a_3) = a_4(a_2 + a_3),$$

$$a_5(a_3 + a_5) = 0,$$

$$\lambda(a_1, a_2 + a_4, a_5 - a_3) = (a_4 - a_2, a_5, a_3 + a_5, 0).$$

However, from these equations we can easily verify that $a_5 = a_3 = a_4 = a_2 = \lambda = 0$. That is exactly $|\psi_1\rangle$.

For $S_5$, we can only determine that $3 \leq \text{d}(S_5) \leq 4$. The exact value remains unknown.

X. CONCLUSION

The most challenging open problem is to prove (or disprove) that any orthogonal UPB spans a locally indistinguishable subspace. As the structure of a $3 \otimes 3$ UPB has been thoroughly studied and fully characterized in Ref. [3], perhaps it might be feasible to solve the general problem in this special case. However, even this special case seems extremely difficult for the following two reasons. First, the subspace spanned by UPB contains one additional product state [20]. Second, local projective measurements and classical communication are no longer sufficient to decide the local distinguishability of a multipartite subspace. To do this, a criterion similar to Theorem 3 would be highly desirable. Finally, we hope to explore more applications of locally indistinguishable subspaces in quantum information theory.

ACKNOWLEDGMENTS

The material in this work was presented in part at the Asian Conference on Quantum Information Science (AQIS), Seoul, South Korea. We are grateful to the participants for their interest. 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),
the National Basic Research Program of China (Grant No. 2007CB807901), and the QCIS, University of Technology, Sydney (UTS). RD is also partially supported by the ECRG scheme of UTS.

[1] R. Y. Duan, Y. Feng, Y. Xin, and M. S. Ying, IEEE Trans. Inf. Theory 55, 2799 (2009).
[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, Commun. Math. Phys. 238, 379 (2003).
[4] N. Alon and L. Lovasz, J. Combinatorial Theory Ser. A 95, 169 (2001).
[5] J. Niset and N. J. Cerf, Phys. Rev. A 74, 052103 (2006).
[6] 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).
[7] J. Watrous, Phys. Rev. Lett. 95, 080505 (2005).
[8] M. Gregoratti and R. F. Werner, J. Mod. Opt. 50, 913 (2003).
[9] M. Gregoratti and R. F. Werner, J. Math. Phys. 45, 2600 (2004).
[10] P. Hayden and C. King, Quantum Inf. Comput. 5, 156 (2005).
[11] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. 85, 4972 (2000).
[12] A. Winter, e-print arXiv:quant-ph/0507045.
[13] M. B. Hastings, Nature Phys. 5, 255 (2009).
[14] C. King and D. Matysiak, J. Phys. A: Math. Theor. 40, 7939 (2007).
[15] J. Walgate and L. Hardy, Phys. Rev. Lett. 89, 147901 (2002).
[16] S. M. Cohen, Phys. Rev. A 75, 052313 (2007).
[17] M.-Y. Ye, W. Jiang, P. X. Chen, Y. S. Zhang, Z. W. Zhou, and G.-C. Guo, Phys. Rev. A 76, 032329 (2007).
[18] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory 48, 580 (2002).
[19] R. Y. Duan and Y. Y. Shi, Phys. Rev. Lett. 101, 020501 (2008).
[20] S. Bravyi, Quant. Info. Proc. 3, 309 (2004).
[21] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Phys. Rev. Lett. 98, 230502 (2007).
[22] A. Chefles, Phys. Rev. A 69, 050307(R) (2004).
[23] S. Bandyopadhyay and J. Walgate, J. Phys. A 42, 072002 (2009).
[24] T. Cubitt, A. Harrow, D. Leung, A. Montanaro, and A. Winter, Commun. Math. Phys. 284, 281 (2008).