LOCC distinguishability of unilaterally transformable quantum states

Somshubhro Bandyopadhyay\textsuperscript{1}, Sibasish Ghosh\textsuperscript{2} and Guruprasad Kar\textsuperscript{3}

\textsuperscript{1}Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Kolkata 700091, India
\textsuperscript{2}Optics and Quantum Information Group, The Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600113, India
\textsuperscript{3}Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 BT Road, Kolkata 700108, India
E-mail: som@bosemain.boseinst.ac.in, sibasish@imsc.res.in and gkar@isical.ac.in

New Journal of Physics 13 (2011) 123013 (16pp)
Received 17 August 2011
Published 8 December 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/12/123013

Abstract. We consider the question of perfect local distinguishability of mutually orthogonal bipartite quantum states, with the property that every state can be specified by a unitary operator acting on the local Hilbert space of Bob. We show that if the states can be exactly discriminated by one-way local operations and classical communication (LOCC) where Alice goes first, then the unitary operators can also be perfectly distinguished by an orthogonal measurement on Bob’s Hilbert space. We give examples of sets of $N \leq d$ maximally entangled states in $d \otimes d$ for $d = 4, 5, 6$ that are not perfectly distinguishable by one-way LOCC. Interestingly, for $d = 5, 6$, our examples consist of four and five states, respectively. We conjecture that these states cannot be perfectly discriminated by two-way LOCC.
1. Introduction

The question of local discrimination of orthogonal quantum states has received considerable attention in recent years [1–5, 7–21]. In the bipartite setting, Alice and Bob share a quantum system prepared in one of a known set of mutually orthogonal quantum states. Their goal is to determine the state in which the quantum system was prepared using only local operations and classical communication (LOCC). In some cases it is possible to identify the state without error, while in some others it is not by LOCC alone. For example, while any two orthogonal pure states can be perfectly distinguished by LOCC [3], a complete orthogonal basis of entangled states is locally indistinguishable [6, 7, 10]. The nonlocal nature of quantum information is therefore revealed when a set of orthogonal states of a composite quantum system cannot be reliably identified by LOCC. This has been particularly useful in exploring quantum nonlocality and its relationship with entanglement [1, 2, 4, 10] and has also found practical applications in quantum cryptography primitives such as secret sharing and data hiding [23–26].

The fundamental result of Walgate et al [3] shows that it is always possible to perfectly discriminate any two orthogonal quantum states by LOCC regardless of their dimension, multipartite structure and entanglement. As it turns out, quite remarkably, perfect discrimination of more than two orthogonal states is not always possible. Examples include any three orthogonal entangled states in $2 \otimes 2$, two maximally entangled states and a product state in $2 \otimes 2$ and so on [6]. When perfect discrimination is not possible, one may distinguish the states conclusively or unambiguously [18–20], where the unknown state is reliably identified with probability less than unity. A necessary and sufficient condition for unambiguous discrimination of quantum states, not necessarily orthogonal, was obtained by Chefles [20]. Recently, Bandyopadhyay and Walgate [16] have shown that for any set of three states conclusive identification is always possible. In the worst case scenario, only one member of the set, and not all, can be correctly identified, albeit with a nonzero probability.

Interestingly, the maximally entangled basis (Bell basis) in $2 \otimes 2$ [5] or a complete orthogonal entangled basis in $n \otimes m$ [10] is not even conclusively distinguishable, in which case we say that the sets are completely indistinguishable. Note that if an orthogonal set contains at least one product state, one can always distinguish the set conclusively. Therefore, all members of a completely indistinguishable set must necessarily be entangled.
This work was motivated by the results on local distinguishability of orthogonal maximally entangled states \[5, 7, 9, 11\] and, in particular, those that put an upper bound on the number of states that can be perfectly distinguished by LOCC \[7, 11\]. For example, it was first observed in \[7\] that not more than \(d\) maximally entangled states in \(d \otimes d\) can be perfectly distinguished provided the states were chosen from the Bell basis. This was soon followed by a more general result establishing this bound for any set of maximally entangled states in \(d \otimes d\) \[11\].

It is therefore natural to ask whether any \(N\) orthogonal maximally entangled states in \(d \otimes d\) can be perfectly distinguished by means of an LOCC protocol if \(N \leq d\). The general answer is not yet known except in dimensions \(2 \otimes 2\) \[3\] and \(3 \otimes 3\) \[11\]. In \(2 \otimes 2\) the answer follows as a corollary of the more general result that any two orthogonal quantum states of a composite quantum system can be reliably distinguished \[3\]. In \[11\], a constructive proof was given to show that any three orthogonal maximally entangled states in \(3 \otimes 3\) can be perfectly distinguished by LOCC. It is worth noting that in both \[3\] and \[11\] the maximally entangled states could be perfectly distinguished by one-way LOCC. Indeed, for almost all known sets of bipartite orthogonal states that are perfectly LOCC distinguishable, one-way protocols are sufficient. A notable exception to this can be found in \[1\], where it was shown that two-way LOCC is required to distinguish subsets of a locally indistinguishable orthogonal basis of \(3 \otimes 3\).

2. Formulation of the problem and results

In this work we consider the question of perfect LOCC distinguishability of bipartite orthogonal quantum states \(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B\) with the property

\[
|\psi_i\rangle = (I \otimes U_i)|\psi\rangle,
\]

\(i = 1, \ldots, N\) for \(U_i\) unitary. Equation (1) is equivalent to the fact that Bob alone can transform \(|\psi_i\rangle\) into \(|\psi_j\rangle\) for every pair \((i, j)\). These states are known not to be perfectly distinguishable by LOCC if \(N > \dim \mathcal{H}_B\) \[11\]. Therefore, the only case of interest is \(N \leq \dim \mathcal{H}_B\). Clearly, for a given \(|\psi_1\rangle\), the states defined by (1) are completely specified by the set of unitary operators \(\{U_1, U_2, \ldots, U_N\}\) on \(\mathcal{H}_B\). Let us point out that the maximally entangled states form a subset of the class of sets defined by (1).

The main result of this paper lies in showing that one-way LOCC distinguishability of the states (1) can be completely characterized by distinguishability of the unitary operators \(\{U_1, U_2, \ldots, U_N\}\) acting on Bob’s Hilbert space. Before we proceed let us first explain what we mean by distinguishing unitary operators.

A given set of unitary operators \(\{U_1, U_2, \ldots, U_n\}\) acting on some Hilbert space \(\mathcal{H}\) is said to be perfectly distinguishable in \(\mathcal{H}\) if there exists a vector \(|\eta\rangle \in \mathcal{H}\) such that

\[
\langle \eta|U_i^\dagger U_j|\eta\rangle = \delta_{ij}
\]

for all \(1 \leq i, j \leq n\). It could so happen that such a vector \(|\eta\rangle\) does not exist. This, however, does not mean that the unitary operators cannot be reliably distinguished because it may be possible to discriminate them exactly in a locally extended tensor product space.

A set of unitary operators \(\{U_1, U_2, \ldots, U_n\}\) on \(\mathcal{H}\) is perfectly distinguishable in an extended tensor product space \(\mathcal{H}' \otimes \mathcal{H}\) if there exists a vector \(|\zeta\rangle \in \mathcal{H}' \otimes \mathcal{H}\) such that

\[
\langle \zeta|(I \otimes U_i^\dagger U_j)|\zeta\rangle = \delta_{ij}
\]
Consider a set of mutually orthogonal vectors with the property that for every $i$, \((\langle \phi | \psi \rangle = 0)\) holds for all two-way LOCC protocols initiated by Alice. Otherwise it is trivially violated. Interestingly, if the states are in $\mathcal{H} \otimes \mathcal{H}$, then there exists at least one vector $|\phi\rangle \in \mathcal{H}_B$ such that for all $k,l$, with $1 \leq k,l \leq N$, $\langle \phi | U^*_k U_l | \psi \rangle = \delta_{kl}$.

Observe that the necessary condition is nontrivial and interesting only if $N \leq \dim \mathcal{H}_B$. Otherwise it is trivially violated. Interestingly, if the states are in $2 \otimes d$, then the above condition holds for all two-way LOCC protocols initiated by Alice.

We apply our results to the case of distinguishing maximally entangled states. We note that a similar property as that in (1) holds for maximally entangled states as well. That is, if $|\Psi\rangle$ is a maximally entangled state of $d \otimes d$, then it can be written in terms of the standard maximally entangled state
\[
|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \otimes |j\rangle
\]
Consider a set of maximally entangled vectors 
\[ |\Psi\rangle = (I \otimes U) |\Phi^+\rangle \]
\[ = (U^T \otimes I) |\Phi^+\rangle, \]
where \( U \) is unitary. The following result makes explicit use of equations (6) and (7) for one-way LOCC in the directions \( A \rightarrow B \) and \( B \rightarrow A \), respectively.

**Corollary 3.** Consider a set of maximally entangled vectors \( \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\} \) in \( \mathcal{H}_A \otimes \mathcal{H}_B \) where \( N \leq \dim \mathcal{H}_A = \dim \mathcal{H}_B = d \), with \( |\psi_i\rangle = (I \otimes U_i) |\Phi^+\rangle \). If the set is perfectly distinguishable by one-way LOCC in the direction \( A \rightarrow B \), then there exists at least one vector \( |\phi\rangle \in \mathcal{H}_B \) such that \( \langle \phi|U_i^T U_l|\phi\rangle = \delta_{kl} \) for \( 1 \leq k, l \leq N \). On the other hand if the set is perfectly distinguishable by one-way LOCC in the direction \( B \rightarrow A \), then there exists at least one vector \( |\phi\rangle \in \mathcal{H}_A \) so that \( \langle \phi'|V_k^T V_l|\phi'\rangle = \delta_{kl} \) for \( 1 \leq k, l \leq N \), where \( V_k = U_k^T \).

We note that the known cases in which a set of maximally entangled states can be perfectly distinguished by LOCC (these LOCC protocols are all one way in the direction \( A \rightarrow B \) [7, 9, 11]), the orthogonal measurements on Bob’s Hilbert space make explicit use of vectors \( \{|\phi_m\rangle\} \in \mathcal{H}_B \) with the property \( \langle \phi_m|U_k^T U_l|\phi_m\rangle = \delta_{kl} \) for every \( m \) and for all \( k \) and \( l \).

Given the existing symmetry in maximally entangled states, one might wonder whether there is any difference between the one-way LOCC protocols ‘Alice goes first’ and ‘Bob goes first’. This is an interesting question and intuitively it seems that for distinguishing maximally entangled states this should not be an issue. However, we have not been able to conclusively prove that this is the case. As noted in corollary 3, if the states are perfectly distinguishable when Bob goes first, then the orthogonality condition
\[ \langle \phi'|V_k^T V_l|\phi'\rangle = \delta_{kl} \]
must hold for all \( k \) and \( l \) for some \( |\phi'\rangle \). Using the fact that \( V_k = U_k^T \) the above equation can also be written as
\[ \langle \phi'|U_k^T U_l|\phi'\rangle = \delta_{kl}, \]
which in turn is equivalent to the condition
\[ \langle \phi^*|U_l U_k^T|\phi^*\rangle = \delta_{kl}. \]
Comparing the above condition with that of one-way LOCC in the direction \( A \rightarrow B \) (as mentioned in corollary 1) it is unclear if there is any one-to-one correspondence between the two. Hence, we conclude that if the maximally entangled states are perfectly distinguishable by one-way LOCC in the direction \( A \rightarrow B \), then they can also be perfectly distinguished in the opposite direction provided \( [U_k^T, U_l] = 0 \) for all \( k, l = 1, \ldots, N \). In the latter case, one can of course choose \( |\phi'\rangle = |\phi^*\rangle \).

### 3. Maximally entangled states indistinguishable under one-way local operations and classical communication

We now give examples of one-way locally indistinguishable sets of \( N \) orthogonal maximally entangled states in \( d \otimes d \), where \( N \leq d \) and \( d = 4, 5, 6 \). Our examples comprise the following: (a) a set of four maximally entangled states in \( 4 \otimes 4 \), (b) a set of four maximally entangled states in \( 5 \otimes 5 \) and (c) a set of five maximally entangled states in \( 6 \otimes 6 \). To show that these states are
locally indistinguishable by all one-way LOCC protocols it suffices to show (see corollary 3) that the local unitary operators (or their transposes) cannot be perfectly distinguished in $\mathcal{H}_B$ (or $\mathcal{H}_A$). We provide complete proofs for all the examples.

The maximally entangled states considered in these examples belong to the family of generalized Bell states. In $d \otimes d$, $d^2$ generalized Bell states written in the standard basis can be expressed as

$$|\Psi_{nm}^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi i j n/d} |j\rangle \otimes |j \oplus_d m\rangle$$

for $n, m = 0, 1, \ldots, d - 1$, where $j \oplus_d m \equiv (j + m) \mod d$. The standard maximally entangled state $|\Phi^+\rangle$ in $d \otimes d$ is simply $|\Psi_{00}^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$. These states are related to the standard maximally entangled state in the following way:

$$(I \otimes U^{(d)}_{nm}) |\Psi_{00}^{(d)}\rangle = |\Psi_{nm}^{(d)}\rangle,$$

where

$$U^{(d)}_{nm} = \sum_{j=0}^{d-1} e^{2\pi i j n/d} |j \oplus_d m\rangle \langle j|$$

are $d \times d$ unitary matrices for $n, m = 0, 1, \ldots, d - 1$.

**Example 1.** The following four maximally entangled states $|\Psi_{00}^{(4)}\rangle$, $|\Psi_{11}^{(4)}\rangle$, $|\Psi_{32}^{(4)}\rangle$, $|\Psi_{31}^{(4)}\rangle$ in $4 \otimes 4$ are not perfectly distinguishable by one-way LOCC.

**Example 2.** The following four maximally entangled states $|\Psi_{00}^{(5)}\rangle$, $|\Psi_{01}^{(5)}\rangle$, $|\Psi_{31}^{(5)}\rangle$, $|\Psi_{22}^{(5)}\rangle$ in $5 \otimes 5$ are not perfectly distinguishable by one-way LOCC.

**Example 3.** The following five maximally entangled states $|\Psi_{00}^{(6)}\rangle$, $|\Psi_{01}^{(6)}\rangle$, $|\Psi_{41}^{(6)}\rangle$, $|\Psi_{12}^{(6)}\rangle$, $|\Psi_{33}^{(6)}\rangle$ in $6 \otimes 6$ are not perfectly distinguishable by one-way LOCC.

**4. Proofs**

**Proof of proposition 1.** Assume that the unitary operators $U_1, U_2, \ldots, U_n$ acting on $\mathcal{H}$ can only be distinguished in an extended tensor product space $\mathcal{H}' \otimes \mathcal{H}$. This implies that there does not exist any vector $|\phi\rangle \in \mathcal{H}$, such that for all $k, l$, with $1 \leq k, l \leq n$,

$$\langle \phi | U^*_k U_l | \phi \rangle = \delta_{kl}.$$  \hspace{1cm} (14)

We will now show that if the set of states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$ defined by equation (4) is perfectly distinguishable by one-way LOCC in the direction $\mathcal{H}' \rightarrow \mathcal{H}$ where the class of LOCC operations is defined with respect to the tensor product space $\mathcal{H}' \otimes \mathcal{H}$, then there must exist a vector $|\phi\rangle \in \mathcal{H}$, such that for all $k, l$, with $1 \leq k, l \leq n$,

$$\langle \phi | U^*_k U_l | \phi \rangle = \delta_{kl}.$$  \hspace{1cm} (15)

Suppose that the states $|\psi_1\rangle, \ldots, |\psi_n\rangle \in \mathcal{H}' \otimes \mathcal{H}$ are perfectly distinguishable by one-way LOCC in the direction $\mathcal{H}' \rightarrow \mathcal{H}$. Let $\mathcal{A} = \{A_1, A_2, \ldots\}$ be the positive operator valued measure (POVM) of the local measurement on $\mathcal{H}'$ satisfying the usual constraints that $\{A_i\}$ are positive.
operators and $\sum_i A_i \leq I$ of $\mathcal{H}$. Associated with the $i$th outcome, let $B^i = \{B_{ij}\}$ be the POVM of the local measurement on $\mathcal{H}$ satisfying $\sum_j B_{ij} \leq I$ where $\{B_{ij}\}$ are positive operators. It may be noted that by defining $B_i = \sum_j B_{ij}$, the collection of positive operators $\{A_i \otimes B_i\}$ represents a separable POVM satisfying $\sum_i A_i \otimes B_i \leq I \otimes I_{\mathcal{H}}$.

Let $A_i = A_i^j A_j$, where $A_i$ is the Kraus element. Subsequent to the $i$th outcome of the measurement $A$, the reduced density matrix on $\mathcal{H}$ (for the input state $|\psi_k\rangle$) is given by

$$\sigma_{k,A_i} = \frac{\operatorname{Tr}_{\mathcal{H}'}(\rho_k A_i \otimes I)}{\operatorname{Tr}(\rho_k A_i \otimes I)}, \tag{16}$$

where $\rho_k = |\psi_k\rangle\langle\psi_k|$. Because a measurement now perfectly distinguishes the set of reduced density matrices $\{\sigma_{k,A_i} : \mathcal{H} \rightarrow \mathcal{H} | k = 1, \ldots, n\}$, they must be mutually orthogonal; that is,

$$\operatorname{Tr}(\sigma_{k,A_i} \sigma_{l,A_j}) = 0 : k \neq l. \tag{17}$$

Noting that the states we are trying to perfectly distinguish are of the form

$$|\psi_k\rangle = (I \otimes U_k) |\psi_1\rangle \tag{18}$$

for $k = 1, \ldots, n$, the transformed state $|\psi_{k,A_i}\rangle$ (unnormalized) post measurement on $\mathcal{H}'$ is given by

$$|\psi_{k,A_i}\rangle = (A_i \otimes I) (I \otimes U_k) |\psi_1\rangle = (I \otimes U_k) |\psi_{1,A_i}\rangle. \tag{19}$$

This in turn implies that the reduced density matrices $\sigma_{k,A_i}$ for all $k$ can be expressed in terms of $\sigma_{1,A_i}$ as

$$\sigma_{k,A_i} = U_k \sigma_{1,A_i} U_k^\dagger. \tag{20}$$

Let the spectral decomposition of the density matrix $\sigma_{1,A_i}$ be

$$\sum_{p=1}^r \lambda_p^i |\chi_p^i\rangle \langle \chi_p^i|, \tag{21}$$

where $0 < \lambda_p^i \leq 1$, $\sum_{p=1}^r \lambda_p^i = 1$ and $\langle \chi_p^i | \chi_q^i \rangle = \delta_{pq}$. Using equations (20) and (21), we can rewrite $\sigma_{k,A_i}$ as

$$\sigma_{k,A_i} = \sum_{p=1}^r \lambda_p^i U_k |\chi_p^i\rangle \langle \chi_p^i| U_k^\dagger. \tag{22}$$

We now apply the orthogonality condition: $\operatorname{Tr}(\sigma_{k,A_i} \sigma_{l,A_j}) = 0$ if $k \neq l$ to obtain

$$\operatorname{Tr}(\sigma_{k,A_i} \sigma_{l,A_j}) = \sum_p (\lambda_p^i)^2 |\langle \chi_p^i | U_k^\dagger U_l |\chi_p^i\rangle|^2 + \sum_{p \neq q} \lambda_p^i \lambda_q^i |\langle \chi_p^i | U_k^\dagger U_l |\chi_q^i\rangle|^2 = 0 \tag{23}$$

from which it follows that every term in the summation must be identically zero. This is because each term is non-negative (note that $0 < \lambda_p^i \leq 1$) and by adding all the terms we get zero. Moreover, equation (23) holds for all $k$ and $l$. Therefore, for every $p$ we have

$$|\langle \chi_p^i | U_k^\dagger U_l |\chi_p^i\rangle|^2 = 0 \tag{24}$$

from which it follows that there exist vectors $\{|\chi_p^i\rangle, U_k |\chi_p^i\rangle \in \mathcal{H} | k = 2, \ldots, n\}$ forming an orthogonal set. This is in contradiction to the fact that the unitary operators are distinguishable only in an extended tensor product space. This proves the result. \hfill \Box
Remark 1. As noted before, corollary 1 is a direct consequence of proposition 1. The result of corollary 2, however, holds for all two-way LOCC protocols initiated by Alice. The proof is given below.

Proof of corollary 2. We assume that the set of vectors \{|\psi_i\rangle : i = 1, \ldots, N\} in \(2 \otimes d\) can be perfectly distinguished by LOCC if Alice goes first. From a result in [4], it follows that there exists a basis \{(|0\rangle, |1\rangle)\} for Alice such that in that basis,

\[|\psi_i\rangle = |0\rangle|\chi_i^0\rangle + |1\rangle|\chi_i^1\rangle,\]

where \(\langle \chi_i^0 | \chi_j^0 \rangle = \langle \chi_i^1 | \chi_j^1 \rangle = 0\) if \(i \neq j\). Using the fact that for every \(i\),

\[|\psi_i\rangle = (I \otimes U_i)|\psi_1\rangle,\]

where \(U_i\) is unitary, equation (25) can be rewritten as

\[|\psi_i\rangle = |0\rangle U_i|\chi_i^0\rangle + |1\rangle U_i|\chi_i^1\rangle,\]

where the states \(\{U_i|\chi_i^x\rangle : x = 0, 1 : i = 1, \ldots, N\}\) satisfy the following orthogonality conditions:

\[\langle \chi_i^0 | U_i^\dagger U_j |\chi_i^0 \rangle = \langle \chi_i^1 | U_i^\dagger U_j |\chi_i^1 \rangle = 0\]

if \(i \neq j\). This concludes the proof.

Proof of corollary 3. We first note that a given set of orthogonal maximally entangled vectors can be written in the form of equation (4) by virtue of equation (6). Clearly, the results of proposition 1 and corollary 1 apply for one-way LOCC protocols in the direction \(A \rightarrow B\) where the corresponding unitary operators acting on Bob’s Hilbert space are denoted by \(U_1, \ldots, U_N\). On the other hand, owing to equation (7) we know that the same given set of maximally entangled states can also be defined by the action of unitary operators \(U_1^T, \ldots, U_N^T\) acting only on the local Hilbert space of Alice. Thus the results of proposition 1 and corollary 1 also apply to one-way LOCC protocols in the direction \(B \rightarrow A\).

5. Proofs of the examples

Proof of example 1. We will show that the states are not perfectly distinguishable by one-way LOCC in the direction \(A \rightarrow B\). A similar proof can be worked out in the direction \(B \rightarrow A\). We write the states as \(|\Psi_0^{(4)}, |\Psi_1^{(4)}\rangle = (I \otimes U_{11}^{(4)})|\Psi_0^{(4)}\rangle, |\Psi_2^{(4)}\rangle = (I \otimes U_{32}^{(4)})|\Psi_0^{(4)}\rangle\) and \(|\Psi_3^{(4)}\rangle = (I \otimes U_{31}^{(4)})|\Psi_0^{(4)}\rangle\). From corollary 3, a necessary condition for these four states to be perfectly distinguishable by one-way LOCC in the direction \(A \rightarrow B\) is that there must exist a vector (normalized) \(|\phi\rangle = \sum_{j=0}^3 \phi_j |j\rangle \in \mathcal{H}_B\) satisfying the normalization condition

\[\sum_{j=0}^3 |\phi_j|^2 = 1\]

such that the four vectors \(|\phi\rangle, U_{11}^{(4)}|\phi\rangle, U_{32}^{(4)}|\phi\rangle\) and \(U_{31}^{(4)}|\phi\rangle\) are pairwise orthogonal. From here on, we will omit the superscript in the unitaries. It is easy to verify that the six unitary operators...
where all the exponents of $\omega = e^{\frac{2\pi i}{4}}$ are taken to be numbers addition modulo 4. From equations (30), (31) and (33), one finds that the vector $(\phi_0^*, \phi_1^*, \phi_2^*, \phi_3^*) \in \mathbb{C}^4$ is orthogonal to the following three vectors: $(1, \omega^2, \omega^3)$, $(1, \omega^3, \omega^2, \omega)$ and $(1, \omega^2, 1, \omega^3)$. Therefore, we must have

\[
(\phi_0^*, \phi_1^*, \phi_2^*, \phi_3^*) = \lambda (1, 1, 1, 1)
\]

for some $\lambda \in \mathbb{C}$. We will show that the above equality cannot be satisfied except when $\phi_i = 0$ for every $i$ and $\lambda = 0$, thereby completing the proof. To show this, we need to consider two cases, namely $\lambda \neq 0$ and $\lambda = 0$.

**Case 1 ($\lambda \neq 0$).** From equation (36), here we must have $\forall j, \phi_j \neq 0$. Thus, for $j = 0, 1, 2, 3$, we have the following two relations:

\[
\phi_j^* \phi_{j^\oplus 1} = \frac{\lambda^2}{|\phi_{j^\oplus 1}|^2},
\]

\[
\phi_j^* \phi_{j^\oplus 2} = \frac{\lambda^3}{|\phi_{j^\oplus 1} \phi_{j^\oplus 2}|^2}.
\]

Then from equation (35) we see that

\[
\lambda^3 \sum_{j=0}^{3} \frac{1}{|\phi_{j^\oplus 1} \phi_{j^\oplus 2}|^2} = 0
\]

immediately implying that $\lambda = 0$, which is a contradiction.
Case 2 ($\lambda = 0$). Here the nontrivial cases arise only when any two $\phi_i$s are zero and the remaining two are nonzero. It is simple to verify that a contradiction is always reached. For example, suppose $\phi_0 = \phi_2 = 0$ and $\phi_1 \neq 0$, $\phi_3 \neq 0$. From equation (34), we obtain $|\phi_1|^2 + |\phi_3|^2 = 0$, which immediately implies that $\phi_1 = \phi_3 = 0$. This therefore completes the proof.

Proof of example 2. We will prove local indistinguishability in the direction $A \to B$. A similar proof holds for $B \to A$ as well. Consider the following four maximally entangled states in $5 \otimes 5$:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{5}} \sum_{j=0}^{4} |jj\rangle,$$

$$|\Psi_{n_11}\rangle = (I \otimes U_{n_11})|\Psi_{00}\rangle,$$

$$|\Psi_{n_1'1}\rangle = (I \otimes U_{n_1'1})|\Psi_{00}\rangle,$$

$$|\Psi_{n_22}\rangle = (I \otimes U_{n_22})|\Psi_{00}\rangle.$$

According to corollary 3, a necessary condition for these four states to be perfectly distinguishable by one-way LOCC in the direction $A \to B$ is that there must exist a vector (normalized) $|\phi\rangle = \sum_{j=0}^{4} \phi_j |j\rangle \in \mathcal{H}_B$ satisfying the normalization condition

$$\sum_{j=0}^{4} |\phi_j|^2 = 1 \quad (37)$$

and such that the four vectors $|\phi\rangle$, $U_{n_11} |\phi\rangle$, $U_{n_1'1} |\phi\rangle$ and, $U_{n_22} |\phi\rangle$ are pairwise orthogonal. We now write the orthogonality conditions:

$$\langle \phi | U_{n_11} | \phi \rangle = \sum_{j=0}^{4} \omega^{n_1 j} \phi_j \phi_j^* = 0, \quad (38)$$

$$\langle \phi | U_{n_1'1} | \phi \rangle = \sum_{j=0}^{4} \omega^{n_1' j} \phi_j \phi_j^* = 0, \quad (39)$$

$$\langle \phi | U_{n_11}^\dagger U_{n_22} | \phi \rangle = \sum_{j=0}^{4} \omega^{(n_2 - n_1) j} \phi_j \phi_j^* = 0, \quad (40)$$

$$\langle \phi | U_{n_1'1}^\dagger U_{n_22} | \phi \rangle = \sum_{j=0}^{4} \omega^{(n_2 - n_1') j} \phi_j \phi_j^* = 0, \quad (41)$$

$$\langle \phi | U_{n_22} | \phi \rangle = \sum_{j=0}^{4} \omega^{n_2 j} \phi_j \phi_j^* = 0, \quad (42)$$

$$\langle \phi | U_{n_11}^\dagger U_{n_2'2} | \phi \rangle = \sum_{j=0}^{3} \omega^{(n_1 - n_1') j} |\phi_j|^2 = 0, \quad (43)$$

where all the exponents of $\omega = e^{i 2\pi / 5}$ are taken to be numbers addition modulo 5. For the set of values $n_1 = 0$, $n_1' = 3$ and $n_2 = 2$ (other suitable choices of $n_1, n_1', n_2$ are also

New Journal of Physics 13 (2011) 123013 (http://www.njp.org/)
orthogonality conditions can be written as

\[
\langle \phi | \phi \rangle = \sum_{nm} \phi^*_n \phi_m = 0
\]

and such that the five vectors

\[
\phi_i \in \mathbb{C}^5
\]

are pairwise orthogonal. Using equation (44) in equation (42) we see that

\[
\sum_{j=0}^{4} \frac{1}{|\phi_j|} = 0
\]

implying that \(\lambda = 0\), which is a contradiction.

**Case 2** (\(\lambda = 0\)). Here we need to consider several possibilities depending upon the values of \(\phi_i\). A straightforward but tedious calculation shows that all the possibilities are ruled out for not being able to satisfy the orthogonality conditions and equation (44) simultaneously unless \(|\phi\rangle = 0\). This therefore completes the proof.

**Proof of example 3.** As in the proof of the previous example, we begin with a more general family of five orthogonal states in \(6 \otimes 6\). We will prove the local indistinguishability in the direction \(A \rightarrow B\). We note that a similar proof holds in the direction \(B \rightarrow A\) as well. The states are defined as follows:

\[
\Psi_{00} = \frac{1}{\sqrt{6}} \sum_{j=0}^{5} |jj\rangle,
\]

\[
\Psi_{n1} = (I \otimes U_{n1}) \Psi_{00},
\]

\[
\Psi_{n1}' = (I \otimes U_{n1})' \Psi_{00},
\]

\[
\Psi_{n2} = (I \otimes U_{n2}) \Psi_{00},
\]

\[
\Psi_{n3} = (I \otimes U_{n3}) \Psi_{00},
\]

where \(U_{nm} = \sum_{j=0}^{5} e^{2\pi i j n} \otimes \mathbb{I} \otimes m \rangle \langle n|\), with \(n, m = 0, 1, 2, 3, 4, 5\) and \(j \otimes m = (j + m) \mod 6\). Also, we denote \(\omega = e^{2\pi i / 6}\).

From corollary 3, a necessary condition that the above five states be perfectly distinguishable by one-way LOCC in the direction \(A \rightarrow B\) is that there must exist a normalized vector \(|\phi\rangle = \sum_{j=0}^{5} \phi_j |j\rangle \in \mathbb{C}^6\) satisfying the normalization condition

\[
\sum_{j=0}^{5} |\phi_j|^2 = 1
\]

and such that the five vectors \(|\phi\rangle, U_{n1} |\phi\rangle, U_{n1}' |\phi\rangle, U_{n2} |\phi\rangle, U_{n3} |\phi\rangle\) are pairwise orthogonal. The orthogonality conditions can be written as

\[
\langle \phi | U_{n1} | \phi \rangle = \sum_{j=0}^{5} \omega^n \phi_j \phi_j^* = 0
\]

and

\[
\langle \phi | U_{n1}' | \phi \rangle = \sum_{j=0}^{5} \omega^n \phi_j \phi_j^* = 0
\]

\[
\langle \phi | U_{n2} | \phi \rangle = \sum_{j=0}^{5} \omega^n \phi_j \phi_j^* = 0
\]

\[
\langle \phi | U_{n3} | \phi \rangle = \sum_{j=0}^{5} \omega^n \phi_j \phi_j^* = 0
\]
We now have to consider two cases, namely when \( \lambda \neq 0 \) and \( \lambda = 0 \).
Case 1. Let $\lambda \neq 0$. Using equation (57) into (54) we see that

$$\lambda^3 \omega^{3n_4} \sum_{j=0}^{5} \frac{\omega^{(n_2 + 3n_4)j}}{|\phi_j \oplus 1 \phi_j \oplus 2|^2} = 0,$$

from which we readily obtain $\lambda = 0$ (note that $n_3 + 3n_4 = 0 \pmod{6}$), which is a contradiction.

Case 2. Let $\lambda = 0$. This gives rise to several subcases that need to be considered individually.

Case 2.1. In this case we assume that any five elements of the set $\{\phi_i : i = 0, \ldots, 5\}$ are zero. Suppose that $\phi_5 \neq 0$, and the rest are all zero. The normalization condition implies that $|\phi_5|^2 = 1$. On the other hand, from equation (55) we see that $\omega^{5(n'_1 - n_1)}|\phi_5|^2 = 0$, thus arriving at a contradiction. Similarly, contradictions can be reached for other cases as well.

Case 2.2. Here we assume that any four elements of the set $\{\phi_i : i = 0, \ldots, 5\}$ are zero. Suppose that $\phi_0 = \phi_1 = \phi_2 = \phi_3 = 0$. This clearly violates equation (57) and hence this is not possible. Likewise other cases can be ruled out. Nevertheless it is instructive to look at another case in which the proof is slightly more nontrivial. Suppose that $\phi_0 = \phi_1 = \phi_2 = \phi_4 = 0$. Here from equations (51)–(53) we obtain

$$\phi_3 \phi_5^* = 0,$$

and from equation (55)

$$|\phi_3|^2 + \omega^{2(n'_1 - n_1)}|\phi_5|^2 = 0,$$

and from the normalization condition we obtain

$$|\phi_3|^2 + |\phi_5|^2 = 1.$$

Clearly, the above three equations are incompatible.

Case 2.3. Here we assume that any three elements of the set $\{\phi_i : i = 0, \ldots, 5\}$ are zero. One can show that all the cases can be ruled out because contradictions are reached with the orthogonality conditions and/or equation (57). We give two instances for a better understanding among the readers. If we take $\phi_0 = \phi_1 = \phi_2 = 0$, then this is clearly in contradiction to equation (57). Somewhat more complicated is the proof of the case corresponding to $\phi_0 = \phi_2 = \phi_4 = 0$. From equations (51)–(53), and explicitly substituting the values $n_1 = 0$, $n'_1 = 4$, $n_2 = 1$ and $n_3 = 3$, one can show after some simple algebra that the vector $(\phi_1^* \phi_3, \phi_3^* \phi_5, \phi_5^* \phi_1) \in \mathbb{C}^3$ is a null vector. That is,

$$(\phi_1^* \phi_3, \phi_3^* \phi_5, \phi_5^* \phi_1) = (0, 0, 0).$$

On the other hand, equation (55) and the normalization condition give us the following two relations:

$$|\phi_1|^2 + \omega^{2(n'_1 - n_1)}|\phi_3|^2 + \omega^{4(n'_1 - n_1)}|\phi_5|^2 = 0,$$

$$|\phi_1|^2 + |\phi_3|^2 + |\phi_5|^2 = 1.$$

The above three equations are clearly inconsistent with each other.

The remaining cases, namely when any two of the elements are zero and only one element is zero, are easily shown to be ruled out for they all give rise to contradiction with equation (57). This completes the proof. Thus, we have shown that the five maximally entangled states $|\Psi_{00}^{(6)}\rangle, |\Psi_{01}^{(6)}\rangle, |\Psi_{11}^{(6)}\rangle, |\Psi_{12}^{(6)}\rangle$ and $|\Psi_{33}^{(6)}\rangle$ in $6 \otimes 6$ are not perfectly distinguishable by one-way LOCC.

New Journal of Physics 13 (2011) 123013 (http://www.njp.org/)
6. Discussions and conclusions

We have considered in this work one-way local distinguishability of a set of orthogonal states which are unilaterally transformable. That is to say, the states can be mapped onto one another by unitary operators acting on the local Hilbert spaces. We have shown that the one-way local distinguishability of such states is intimately related to the question of perfect distinguishability of the corresponding unitary operators in the local Hilbert space they act upon. In particular, if the unitary operators cannot be distinguished in their local Hilbert space but instead are perfectly distinguishable in an extended Hilbert space, then the set of orthogonal states thus generated are indistinguishable by one-way LOCC. We then apply these results to distinguish maximally entangled states by one-way LOCC.

Maximally entangled states, by definition, belong to the family of unilaterally transformable states, although symmetry implies that maximally entangled states are unilaterally transformable in both Alice’s and Bob’s Hilbert spaces. Maximally entangled states are of considerable importance in quantum information theory and foundations of quantum mechanics because of their role in quantum communication primitives such as quantum teleportation and superdense coding as well demonstrating maximal violations of Bell inequalities. Thus local distinguishability of maximally entangled states has attracted much attention in recent years and one of the main open questions in this area is whether a set of $N \leq d$ orthogonal maximally entangled states in $d \otimes d$ can be perfectly distinguished by LOCC for all $d \geq 4$.

To help answer this question, we have established a one-to-one correspondence between one-way LOCC distinguishability of a set of orthogonal quantum states and distinguishability of the local unitary operators that generate such a set. With the help of this correspondence we have been able to show that there are sets of $N \leq d$ maximally entangled states in $d \otimes d$ for $d = 4, 5, 6$ such that these states cannot be perfectly distinguished by one-way LOCC alone. This provides strong evidence in support of the conjecture that such sets of states indeed exist. Very recently, in [22], a set of four maximally entangled states in $4 \otimes 4$ were presented that are not perfectly distinguishable by PPT operations and therefore by LOCC, but the question in higher dimensions remains open. We conjecture that these examples are potentially strong candidates to establish that any $N$ maximally entangled states in $d \otimes d$ may not be perfectly distinguished by LOCC even if $N \leq d$. We believe that a reasonable way to conclusively answer this question would be to extend the applicability of the necessary condition presented in this paper (see proposition 1 and corollary 3 for maximally entangled states) to two-way LOCC protocols.

A very interesting avenue of further research based on the results presented here would be to extend these results to multipartite systems. For multipartite systems, except for very special cases, the extension is not straightforward and generally gives rise to complex scenarios. To illustrated, let us consider the simplest multipartite scenario consisting of three parties, Alice, Bob and Charlie. Assume that the set of states are being generated by applying unitary operations on some standard state, either on the local Hilbert space of Bob or Charlie or both. Then a straightforward generalization of the bipartite case now gives rise to several independent cases corresponding to the following forms of unitary operations: (a) $\{I \otimes U_i \otimes I\}$, (b) $\{I \otimes I \otimes V_j\}$ and (c) $\{I \otimes U_i \otimes V_j\}$. The interesting cases are when the unitary operators $\{U_i\}$ and $\{V_j\}$ are not perfectly distinguishable on the local Hilbert spaces they act upon, and instead can be perfectly distinguished in an extended tensor product space.
In the first two cases, it is possible to obtain results similar to that obtained in this work with respect to the following one-way LOCC in the directions $A \rightarrow C \rightarrow B$ for case (a) and $A \rightarrow B \rightarrow C$ for case (b). On the other hand, case (c) merits careful consideration, and it is not obvious at all how the results in this paper could be generalized to include such cases. Thus, for a general multipartite system consisting of, say, $N$ subsystems, our results can be applied when the states can be mapped onto one another by applying local unitaries only once on a subsystem. For more complex scenarios that involve unitaries, mapping the states onto one another by acting on two or more subsystems would call for further research and is beyond the scope of this paper.

Finally, we would like to mention that quantum cryptography primitives such as both classical and quantum data hiding, secret sharing protocols [23–26] make use of the fact that it is not possible to perfectly determine the state of a quantum system even though it was prepared in one of several orthogonal states. In this paper, several examples of locally one-way indistinguishable minimal (possibly) sets of maximally entangled states are presented with the property that they are unilaterally transformable. It is conceivable that these states with their very special properties may find applications in developing new protocols for secret sharing and data hiding.

Acknowledgments

SG acknowledges the hospitality of Bose Institute, Kolkata and ISI, Kolkata during his visits in 2010 when part of this work was completed.

References

[1] Bennett C H, DiVincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W, Smolin J A and Wootters W K 1999 Quantum nonlocality without entanglement Phys. Rev. A 59 1070
[2] Bennett C H, DiVincenzo D P, Mor T, Shor P W, Smolin J A and Terhal B M 1999 Unextendible product bases and bound entanglement Phys. Rev. Lett. 82 5385
[3] Walgate J, Short A J, Hardy L and Vedral V 2000 Local distinguishability of multipartite orthogonal quantum states Phys. Rev. Lett. 85 4972
[4] Walgate J and Hardy L 2002 Nonlocality, asymmetry and distinguishing bipartite states Phys. Rev. Lett. 89 147901
[5] Ghosh S, Kar G, Roy A, Sen (De) A and Sen U 2001 Distinguishability of Bell states Phys. Rev. Lett. 87 277902
[6] Ghosh S, Kar G, Roy A, Sarkar D, Sen (De) A and Sen U 2002 Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement Phys. Rev. A 65 062307
[7] Ghosh S, Kar G, Roy A and Sarkar D 2004 Distinguishability of maximally entangled states Phys. Rev. A 70 022304
[8] Chen P-X and Li C-Z 2003 Orthogonality and distinguishability: criterion for local distinguishability of arbitrary orthogonal states Phys. Rev. A 68 062107
[9] Fan H 2004 Distinguishability and indistinguishability by local operations and classical communication Phys. Rev. Lett. 92 177905
[10] Horodecki M, Sen (De) A, Sen U and Horodecki K 2003 Local distinguishability: more nonlocality with less entanglement Phys. Rev. Lett. 90 047902
[11] Nathanson M 2005 Distinguishing bipartite orthogonal states by LOCC: best and worst cases J. Math. Phys. 46 062103
[12] Watrous J 2005 Bipartite subspaces having no bases distinguishable by local operations and classical communication Phys. Rev. Lett. 95 080505
[13] Hayashi M, Markham D, Murao M, Owari M and Virmani S 2006 Bounds on entangled orthogonal state discrimination using local operations and classical communication Phys. Rev. Lett. 96 040501
[14] Duan R Y, Feng Y, Ji Z F and Ying M S 2007 Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication Phys. Rev. Lett. 98 230502
[15] Duan R Y, Feng Y, Xin Y and Ying M S 2009 Distinguishability of quantum states by separable operations IEEE Trans. Inf. Theory 55 1320
[16] Bandyopadhyay S and Walgate J 2009 Local distinguishability of any three quantum states J. Phys. A: Math. Theor. 42 072002
[17] Bandyopadhyay S 2010 Entanglement and perfect discrimination of a class of multiqubit states by local operations and classical communication Phys. Rev. A 81 022327
[18] Virmani S, Sacchi M F, Plenio M B and Markham D 2001 Optimal local discrimination of two multipartite pure states Phys. Lett. A 288
[19] Chen Y-X and Yang D 2002 Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communication Phys. Rev. A 65 022320
[20] Chefles A 2004 Condition for unambiguous state discrimination using local operations and classical communication Phys. Rev. A 69 050307
[21] Cohen S M 2007 Local distinguishability with preservation of entanglement Phys. Rev. A 75 052313
[22] Yu N, Duan R Y and Ying M S 2011 Distinguishing maximally entangled states by PPT operations and entanglement catalysis discrimination arXiv:1107.3224
[23] Terhal B M, DiVincenzo D P and Leung D W 2001 Hiding bits in Bell states Phys. Rev. Lett. 86 5807
[24] DiVincenzo D P, Leung D W and Terhal B M 2002 Quantum data hiding IEEE Trans. Inf. Theory 48 580
[25] Eggeling T and Werner R F 2002 Hiding classical data in multipartite quantum states Phys. Rev. Lett. 89 097905
[26] Markham D and Sanders B C 2008 Graph states for quantum secret sharing Phys. Rev. A 78 042309