

Any $2 \otimes n$ subspace is locally distinguishable

Nengkun Yu,^{*} Runyao Duan,[†] and Mingsheng Ying[‡]

State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China and

Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology,

University of Technology, Sydney, NSW 2007, Australia

(Dated: August 14, 2011)

A subspace of a multipartite Hilbert space is called *locally indistinguishable* if any orthogonal basis of this subspace cannot be perfectly distinguished by local operations and classical communication. Previously it was shown that any $m \otimes n$ bipartite system such that $m > 2$ and $n > 2$ has a locally indistinguishable subspace. However, it has been an open problem since 2005 whether there is a locally indistinguishable bipartite subspace with a qubit subsystem. We settle this problem by showing that any $2 \otimes n$ bipartite subspace is locally distinguishable in the sense it contains a basis perfectly distinguishable by LOCC. As an interesting application, we show that any quantum channel with two Kraus operations has optimal environment-assisted classical capacity.

PACS numbers: 03.67.-a, 3.65.Ud

1. Introduction:—LOCC distinguishability of finite set of orthogonal multipartite states is a fundamental task in quantum information theory, it has attracted much attention and has been extensively studied as it has important implications in classical data hiding [1] and channel capacity [2–4].

Orthogonal states can always be exactly distinguished if there are no restrictions on the measurements one can perform. However, the discrimination of multipartite states is difficult when only local operations and classical communication (LOCC) is allowed. Many results on LOCC discrimination seem rather counterintuitive. For instance, Bennett et al discovered that there exist $3 \otimes 3$ orthonormal pure product bases that are indistinguishable by LOCC [6]. Furthermore, it was shown that the members of an unextendible product basis (UPB) are not perfectly distinguishable by LOCC [7]. On the other hand, it has been proven that any two orthogonal multipartite quantum states, no matter entangled or not, can be perfectly distinguished by LOCC [8]. Some powerful methods for checking distinguishability were introduced in [9, 10].

In 2005 Watrous demonstrated that there exist a class of $m \otimes m$ subspaces having no orthonormal bases locally distinguishable if $m > 2$ [4]. Such subspaces are named locally indistinguishable subspaces; otherwise, they are said to be locally distinguishable. Watrous also proved that there is no $2 \otimes 2$ locally indistinguishable subspace, by directly employing the results from [11]. Winter’s result [5] implies that the existence of bipartite subspace \mathcal{Q} such that $\mathcal{Q}^{\otimes k}$ is locally indistinguishable for any k . Duan et al generalized Watrous’s result to the most general $m \otimes n$ systems for $m \neq n$ and the multipartite setting, and found locally indistinguishable subspaces with smaller dimensions [12, 13]. Most notably, it was shown that any subspace spanned by three-qubit UPB is lo-

cally indistinguishable, and there exists a 3-dimensional three-qubit locally distinguishable subspace. An interesting question remains to be answered is whether there is any $2 \otimes n$ locally indistinguishable subspace.

The main contribution of this Letter is to answer the above question negatively. We show that any $2 \otimes n$ subspace is locally distinguishable. Combining with the previous results [4, 12, 13], we conclude that there is no locally indistinguishable $m \otimes n$ subspace if and only if one of m or n should be 2. Our key techniques can be used to study the distinguishability of three-dimensional bipartite subspace which contains a product state. We show that any such subspace has a basis that can be distinguished under local projective measurements and one-way classical communication (LPCC).

Since the connection between distinguishability of subspace and capacity of channel, classical corrected capacity of a quantum channel is considered. The classical corrected capacity of channel introduced by Hayden and King is defined as the best classical capacity can be obtained when the receiver of the channel is capable to select an optimal measurement on the channel’s output by using classical information obtained from a measurement on the environment [3]. This environment-assisted model was first introduced by Gregoratti and Werner in [2], where they are interested in correcting the errors incurred from sending quantum information. According to the well known result by Walgate et al [8], Hayden and King were able to show that the classical corrected capacity of any quantum channel is at least one bit [3]. In particular, the existence of locally indistinguishable subspaces implies the existence of quantum channel with suboptimal classical corrected capacity, that is, the corrected capacity is less than $\log_2 d$ with d the dimension of the input state space. In contrast, our result signifies that the classical corrected capacity of any quantum

channel with only two Kraus operators is always optimal.

2. *Main result:*—Suppose there is a $2 \otimes n$ quantum system shared by Alice and Bob such that Alice is the owner of the qubit. We will show that any $2 \otimes n$ subspace has an orthogonal basis which can be perfectly distinguished by some protocol where Alice goes first [11].

We will make use of the following Lemma from [11], which gives a complete characterization of the local discrimination of orthogonal $2 \otimes n$ states when Alice goes first.

Lemma 1. If Alice goes first, a set of k $2 \otimes n$ orthogonal states $\{|\psi_i\rangle : 1 \leq i \leq k\}$ is locally distinguishable if and only if there is an orthonormal basis $\{|0\rangle, |1\rangle\}_A$ such that:

$$|\psi_i\rangle = |0\rangle|\eta_0^i\rangle + |1\rangle|\eta_1^i\rangle \quad (1)$$

where $\langle\eta_0^i|\eta_0^j\rangle = \langle\eta_1^i|\eta_1^j\rangle = 0$ for all $i \neq j$.

Now we are ready to present our main result as follows.

Theorem 1. For any $2 \otimes n$ subspace \mathcal{Q} , there exists orthogonal basis $\{|\phi_i\rangle | 1 \leq i \leq d\}$ which can be perfectly distinguished by some Alice goes first LOCC protocol, where d is the dimension of \mathcal{Q} .

Proof:—We only need to show that \mathcal{Q} has orthogonal basis $\{|\psi_i\rangle | 1 \leq i \leq d\}$ with the form of Eq.(1).

Choose arbitrary basis of the qubit's system, called $\{|0\rangle, |1\rangle\}$.

Let $\{|\varphi_i\rangle | 1 \leq i \leq d\}$ an orthonormal basis of \mathcal{Q} with $|\varphi_i\rangle = |0\rangle|\zeta_0^i\rangle + |1\rangle|\zeta_1^i\rangle$, then an n -by- d matrix A can be defined as $A = (|\zeta_0^1\rangle, |\zeta_0^2\rangle \cdots, |\zeta_0^d\rangle)$. From singular value decomposition, there exists a factorization of the form $A = W\Lambda V$, where $W \in U(n)$, $V \in U(d)$ and the matrix Λ is n -by- d diagonal matrix with nonnegative real numbers on the diagonal, it's worth to notice that AV^\dagger is a n -by- d matrix with orthogonal columns.

For any unitary $U = (u_{ij})_{d \times d}$, we can get another orthonormal basis of $\{|\phi_i\rangle | 1 \leq i \leq d\}$ such that

$$|\phi_i\rangle = \sum_{j=1}^d u_{ji} |\varphi_j\rangle = |0\rangle|\eta_0^i\rangle + |1\rangle|\eta_1^i\rangle.$$

where $|\eta_0^i\rangle = \sum_{j=1}^d u_{ji} |\zeta_0^j\rangle$ and $|\eta_1^i\rangle = \sum_{j=1}^d u_{ji} |\zeta_1^j\rangle$. The essential piece is that the matrix A becomes $AU = (|\eta_0^1\rangle, |\eta_0^2\rangle \cdots, |\eta_0^d\rangle)$ under this transformation U .

Now let $U = V^\dagger$ be the unitary transformation, then $AU = AV^\dagger = W\Lambda$ is a matrix with orthogonal columns, which means that after the transformation U , the basis $|\phi_i\rangle = |0\rangle|\eta_0^i\rangle + |1\rangle|\eta_1^i\rangle$ satisfy that $\langle\eta_0^i|\eta_0^j\rangle = 0$ for all $i \neq j$, note that the Orthogonality to $|\phi_i\rangle$ implies $\langle\eta_0^i|\eta_0^j\rangle + \langle\eta_1^i|\eta_1^j\rangle = 0$, so $\langle\eta_1^i|\eta_1^j\rangle = 0$, thus Eq.(1) is satisfied, which completes the proof of our theorem. ■

According to the proof, one can find that Alice even has the freedom to preselect arbitrary orthonormal basis to be her projective measurement basis, which is to say

that for any $\{|0\rangle, |1\rangle\}$, there exists a basis of \mathcal{Q} satisfying Eq.(1).

Combining our result with the existence of locally(separability) indistinguishable subspace for $m \otimes n$ when $m, n > 2$ [4, 12, 13], we have the following corollary:

Corollary 1. There exists $m \otimes n$ subspace indistinguishable by LOCC (or LPCC, Separable operations) if and only if $m, n > 2$.

Also, we can employ the techniques deriving the above theorem to show that

Corollary 2. Any three-dimensional bipartite subspace \mathcal{Q} that contains a product state is one-way LPCC distinguishable.

Proof:—Without loss of generality, assume that $|0\rangle|0\rangle \in \mathcal{Q}$, let $\{|\varphi_i\rangle | 1 \leq i \leq 3\}$ be an orthonormal basis of \mathcal{Q} with $|\varphi_1\rangle = |0\rangle|0\rangle$. Let $\mathcal{P} = \text{span}\{|\varphi_2\rangle, |\varphi_3\rangle\}$, similar as the proof of Theorem 1, one can find orthonormal basis $|\phi_2\rangle, |\phi_3\rangle$ of \mathcal{P} , such that

$$\begin{aligned} |\phi_2\rangle &= |0\rangle|\eta_0^2\rangle + \sum_{i \neq 0} |i\rangle|\alpha_i\rangle, \\ |\phi_3\rangle &= |0\rangle|\eta_0^3\rangle + \sum_{i \neq 0} |i\rangle|\beta_i\rangle, \end{aligned}$$

with $\langle\eta_0^2|\eta_0^3\rangle = 0$. Then $\{|\phi_i\rangle | 1 \leq i \leq 3\}$ are the basis of \mathcal{Q} .

According to [8], one can always find a orthogonal basis $\{|0\rangle', |1\rangle', \dots, |m\rangle'\}$ of \mathcal{C}^m with $|0\rangle = |0\rangle'$, in which the two orthogonal states can be represented

$$\begin{aligned} |\phi_2\rangle &= |0\rangle'|\eta_0^2\rangle + \sum_{i \neq 0} |i\rangle'|\alpha_i\rangle', \\ |\phi_3\rangle &= |0\rangle'|\eta_0^3\rangle + \sum_{i \neq 0} |i\rangle'|\alpha_i^\perp\rangle', \end{aligned}$$

where $|\alpha_i\rangle'$ are not normalized, and $|\alpha_i^\perp\rangle'$ is orthogonal to $|\alpha_i\rangle'$.

In order to distinguish them, one can perform the projective measurement $\{P_0, P_1, \dots, P_m\}$ upon the first part where $P_i = |i\rangle\langle i|$. If the outcome is P_0 , then the left three mutual orthogonal states are on one part, this leads to perfect discrimination. If the our come is P_i with $i > 0$, the left two states are pure orthogonal, they are LPCC distinguishable. \mathcal{Q} is one-way LPCC distinguishable. ■

This protocol also works when the other part goes first.

3. *Classical corrected capacity of rank two channel:*—Any quantum channel Φ can be regarded as arising from a unitary interaction U of the principle system \mathcal{H} and an environment system \mathcal{E} . Without loss of generality, we can let

$$\Phi(\rho) = \text{tr}_{env}[U(\rho \otimes |\varepsilon\rangle\langle\varepsilon|)U^\dagger].$$

Because U is unitary, it will map the orthogonal input state to orthogonal state in $\mathcal{H} \otimes \mathcal{E}$. However after the

trace over of the environment system, the output of the system may be no longer orthogonal. Thus they cannot be distinguished perfectly, which decreases the classical capacity of the channel.

It is possible to enhance channel capacity using measurements on the environment in addition to measurements on the principal system [2, 3].

For any rank two channel, the dimension of the environment can be assumed as 2, thus the whole space $\mathcal{H} \otimes \mathcal{E}$ is a $n \otimes 2$ space, before tracing over the the environment, the output space $\mathcal{Q} = U(\mathcal{H} \otimes |\varepsilon\rangle)$ is a d -dimensional subspace of $\mathcal{H} \otimes \mathcal{E}$, where d is the dimension of \mathcal{H} . According to Theorem 1, it is distinguishable by some environment goes first LPCC protocol, which means that for any orthonormal basis $\{|0\rangle, |1\rangle\}$, there is an orthonormal basis $\{|\phi_i\rangle | 1 \leq i \leq d\}$ of \mathcal{Q} can be represented as Eq.(1), and thus can be distinguished by some environment goes first LPCC protocol. One can easily verify that the basis $\{|\phi_i\rangle | 1 \leq i \leq d\}$ corresponds to an input basis $\{|\psi_i\rangle | 1 \leq i \leq d\}$ of \mathcal{H} with $|\phi_i\rangle = U(|\psi_i\rangle \otimes |\varepsilon\rangle)$. We have therefore proved the following corollary.

Corollary 3. *Any quantum channel with two Kraus operators has optimal environment-assisted classical capacity.*

4. *Conclusion:*—We have proven that there is no $2 \otimes n$ locally indistinguishable subspace. The local distinguishability of such subspace implies that all rank two channel's environment-assisted classical capacity is optimal.

There are several interesting, unanswered questions relating to the distinguishability of subspaces having. For instance, if there exists three-dimensional indistinguishable multipartite subspace? The tripartite qubit indistinguishable example has been given in [13], what left is the bipartite case. We have shown that for all three-dimensional subspaces with a product state, the answer is negative 2. Numerical evidence was presented to show that any three-dimensional subspace of $C^3 \otimes C^n$ has an orthonormal basis which can be reliably distinguished us-

ing one-way LOCC in [14]. Recall our proof of Theorem 1, Alice can perform arbitrary projective measurement, which indicated that the freedom to preselect an orthonormal basis of one part is not used for this case. Is this freedom helpful for subspace discrimination, particularly, is any three-dimensional subspace of $C^3 \otimes C^3$ LPCC distinguishable?

This work was partly supported by the Natural Science Foundation of China (Grant Nos.60736011 and 60702080), and QCIS, University of Technology, Sydney.

* Electronic address: nengkunyu@gmail.com

† Electronic address: runyao.duan@uts.edu.au

‡ Electronic address: mying@it.uts.edu.au

- [1] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
- [2] M. Gregoratti and R. F. Werner, J. Math. Phys. **45**, 2600 (2004).
- [3] P. Hayden and C. King, Quantum Information and Computation **5**, 156 (2005).
- [4] J. Watrous, Phys. Rev. Lett. **95**, 080505 (2005).
- [5] A. Winter, arxiv: quant-ph/0507045.
- [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] C. H. Bennett, D. P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
- [8] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
- [9] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).
- [10] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
- [11] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
- [12] R. Duan, Y. Feng, Y. Xin, M. Ying, IEEE Trans. Inform. Theory **55**, 1320 (2009).
- [13] R. Duan, Y. Xin, and M. Ying, Phys. Rev. A **81**, 032329 (2010). Arxiv: quant-ph/0708.3559.
- [14] C. King and D. Matysiak, quant-ph/0510004.