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

(Received 27 February 2011; published 5 July 2011)

A subspace of a multipartite Hilbert space is said to be *locally indistinguishable* if any orthonormal 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 with $m > 2$ 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 in negative by showing that any $2 \otimes n$ bipartite subspace contains a basis that is locally distinguishable. As an interesting application, we show that any quantum channel with two Kraus operators has optimal environment-assisted classical capacity.

DOI: 10.1103/PhysRevA.84.012304 PACS number(s): 03.67.−a

I. INTRODUCTION

Local distinguishability of a finite set of orthogonal multipartite states has become an increasingly interesting topic in quantum information partly due to its important applications in classical data hiding [1] and quantum channel capacity [2–5]. It is well known that orthogonal quantum states can always be perfectly distinguished if there are no restrictions on the measurements one can perform on the system. However, the discrimination of multipartite states is difficult when only local operations and classical communication (LOCC) is allowed. Indeed, many results on LOCC discrimination are rather counterintuitive. For instance, Bennett *et al.* discovered that there exist $3 \otimes 3$ orthonormal pure product bases that are indistinguishable by LOCC [6]; it was then further shown that the members of an orthogonal unextendable product basis (UPB) are not perfectly distinguishable by LOCC [7]. On the other hand, 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].

The concept of local distinguishability can be generalized to multipartite subspaces. In 2005 Watrous demonstrated that there exists a class of $m \otimes m$ subspaces having no orthonormal bases locally distinguishable if $m > 2$ [4]. Such subspaces are said to be *locally indistinguishable*; 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 locally indistinguishable, and there exists a three-dimensional three-qubit locally indistinguishable subspace [13]. An interesting question that remains to be answered is whether there is any $2 \otimes n$ locally indistinguishable subspace.

The main contribution of this paper is to answer the above question in negative. 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 $m \leqslant 2$ or $n \leqslant 2$. 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).

We then apply our results to study the classical corrected capacity (or environment-assisted classical capacity) of quantum channels [3,5]. The classical corrected capacity of quantum channels introduced by Hayden and King is defined as the best classical capacity one can achieve when the receiver of the channel can be assisted with a friendly environment through LOCC [3]. This environment-assisted model was 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 sharp contrast, our result signifies that the classical corrected capacity of any quantum channel with only two Kraus operators is always optimal.

II. MAIN RESULTS

We will show that any $2 \otimes n$ subspace has an orthogonal basis that can be perfectly distinguished by a protocol where the owner of the *qubit goes first* (i.e., a nontrivial measurement is firstly performed upon the qubit system [11]). A measurement $\{M_1, \ldots, M_m\}$ is said to be nontrivial if there

*nengkunyu@gmail.com
†runyao.duan@uts.edu.au
‡mying@it.uts.edu.au

exists k such that $M_k^\dagger M_k$ is not proportional to the identity operator.

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

Lemma 1. (Walgate and Hardy [11]) A set of $2 \otimes n$ orthogonal states $\{|\psi_i\rangle : 1 \leqslant i \leqslant k\}$ is locally distinguishable by some qubit goes first protocol if and only if there is an orthonormal basis $\{|0\rangle,|1\rangle\}_A$ such that

$$|\psi_i\rangle = |0\rangle\big|\eta_0^i\big\rangle + |1\rangle\big|\eta_1^i\big\rangle, \tag{1}$$

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 an orthogonal basis $\{|\psi_i\rangle : 1 \leqslant i \leqslant d\}$ that is perfectly distinguishable by some qubit goes first LOCC protocol, where d is the dimension of $\mathcal{Q}$.

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

Arbitrarily choose an orthonormal bases of the qubit's system, say $\{|0\rangle,|1\rangle\}_A$. Let $\{|\varphi_i\rangle : 1 \leqslant i \leqslant d\}$ be an orthonormal basis of $\mathcal{Q}$ such that

$$|\varphi_i\rangle = |0\rangle \otimes M_0|i\rangle + |1\rangle \otimes M_1|i\rangle,$$

where M_0 and M_1 are $n \times d$ matrices, and $\{|i\rangle : i = 1,\ldots,d\}$ is a fixed orthonormal basis for a d-dimensional Hilbert space. The orthonormality of these vectors implies that

$$M_0^\dagger M_0 + M_1^\dagger M_1 = I_d.$$

One may therefore choose a d-by-d unitary matrix U such that $U^\dagger M_0^\dagger M_0 U$ is some diagonal matrix in basis $\{|i\rangle\}$. From $U^\dagger M_1^\dagger M_1 U = I_d - U^\dagger M_0^\dagger M_0 U$, one can obtain that $U^\dagger M_1^\dagger M_1 U$ is diagonal in $\{|i\rangle\}$, too.

Now, we define

$$\begin{aligned}|\psi_i\rangle &= |0\rangle \otimes M_0 U|i\rangle + |1\rangle \otimes M_1 U|i\rangle \\ &= (|0\rangle \otimes M_0 + |1\rangle \otimes M_1)U|i\rangle.\end{aligned}$$

It is clear that $\{|\psi_i\rangle : 1 \leqslant i \leqslant d\}$ is also an orthonormal basis of $\mathcal{Q}$, and Eq. (1) is satisfied. With that we complete the proof of Theorem 1. ■

According to the above proof, one can find that the owner of qubit even has the freedom to preselect an arbitrary orthonormal basis to be the projective measurement basis. That means for any $\{|0\rangle,|1\rangle\}_A$, $\mathcal{Q}$ has a basis that satisfies 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 $m,n > 2$.

Furthermore, 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, let $\{|\varphi_i\rangle|0 \leqslant i \leqslant 2\}$ be an orthonormal basis of $\mathcal{Q}$ with $|\varphi_0\rangle = |0\rangle|0\rangle$. We also denote $\mathcal{P} = \text{span}\{|\varphi_1\rangle,|\varphi_2\rangle\}$. Similar to the proof of Theorem 1, one can find an orthonormal basis $\{|\phi_1\rangle,|\phi_2\rangle\}$ of $\mathcal{P}$ such that

$$\begin{aligned}|\phi_1\rangle &= |0\rangle\big|\eta_0^1\big\rangle + \sum_{i\neq 0}|i\rangle|\alpha_i\rangle, \\ |\phi_2\rangle &= |0\rangle\big|\eta_0^2\big\rangle + \sum_{i\neq 0}|i\rangle|\beta_i\rangle,\end{aligned}$$

with $\langle\eta_0^1|\eta_0^2\rangle = 0$. Let $|\phi_0\rangle = |0\rangle|0\rangle$. Then $\{|\phi_i\rangle|0 \leqslant i \leqslant 2\}$ is an orthonormal basis for $\mathcal{Q}$.

According to [8], one can always find an orthogonal basis $\{|0\rangle',|1\rangle',\ldots,|m-1\rangle'\}$ of $\mathcal{C}^m$ such that $|0\rangle' = |0\rangle$ and

$$\begin{aligned}|\phi_1\rangle &= |0\rangle'\big|\eta_0^1\big\rangle + \sum_{i\neq 0}|i\rangle'|\alpha_i'\rangle, \\ |\phi_2\rangle &= |0\rangle'\big|\eta_0^2\big\rangle + \sum_{i\neq 0}|i\rangle'|\beta_i'\rangle,\end{aligned}$$

where $|\alpha_i'\rangle$ and $|\beta_i'\rangle$ may not be normalized but $\langle\alpha_i'|\beta_i'\rangle = 0$ holds for any $i \neq 0$.

In order to distinguish $|\phi_1\rangle$ and $|\phi_2\rangle$, one can perform the projective measurement $\{P_0,P_1,\ldots,P_m\}$ upon the first subsystem, where $P_i = |i\rangle'\langle i|$. If the outcome is P_0, then the remaining three product states are mutually orthogonal states at the second subsystem, and can be further perfectly distinguished. If the outcome is some P_i with $i > 0$, the remaining two pure states are orthogonal and are LPCC distinguishable. Thus $\mathcal{Q}$ is one-way LPCC distinguishable. ■

This protocol also works when the second subsystem goes first.

III. 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 may write

$$\Phi(\rho) = \text{tr}_{\text{env}}[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger],$$

where $|e_0\rangle$ is the initial state of environment and the partial trace is taking according to environment.

Since U is unitary, it maps orthogonal input states to orthogonal ones in $\mathcal{H} \otimes \mathcal{E}$. However after the partial trace-over of the environment, the output of the system may not be orthogonal any more. Thus they cannot be distinguished perfectly and the classical capacity of the channel is strictly decreased.

It is possible to enhance channel capacity using measurements on the environment in addition to measurements on the principal system [2,3], and this yields the notion of environment-assisted classical capacity of quantum channels. See also [5] and [4] for details about this model.

Here we try to apply our previous results to determine the capacity for some special channels. 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 an $n \otimes 2$ space. Before traced over the the environment, the output space $\mathcal{Q} = U(\mathcal{H} \otimes |e_0\rangle)$ 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. Formally, for any orthonormal basis $\{|0\rangle,|1\rangle\}_E$, there is an orthonormal basis $\{|\phi_i\rangle|1 \leqslant i \leqslant d\}$ of $\mathcal{Q}$ that can be represented as Eq. (1). Therefore this basis can be distinguished by some environment goes first LPCC protocol. One can easily verify that the basis $\{|\phi_i\rangle|1 \leqslant i \leqslant d\}$ corresponds to an input basis $\{|\psi_i\rangle|1 \leqslant i \leqslant d\}$ of $\mathcal{H}$ with $|\phi_i\rangle = U(|\psi_i\rangle \otimes |e_0\rangle)$. We have therefore proved the following corollary.

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

IV. CONCLUSION

We have proven that there is no $2 \otimes n$ locally indistinguishable subspace. The local distinguishability of such subspace implies that the environment-assisted classical capacity of any quantum channel with two Kraus operators is optimal.

There are several interesting, unanswered questions relating to the local distinguishability of subspaces. For instance, does there exist any three-dimensional indistinguishable multipartite subspace? A tripartite example, consisting of three qubits, has been given in [13]. The case of bipartite subspaces is still unknown. We have shown that for all three-dimensional subspaces with a product state, the answer is negative Corollary 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 using one-way LOCC in [14]. Recall our proof of Theorem 1; the qubit subsystem can perform arbitrary projective measurement. That suggests some additional freedom to preselect an orthonormal basis of one part is not used for this case. Is this freedom helpful for subspace discrimination? In particular, is any three-dimensional subspace of $\mathcal{C}^3 \otimes \mathcal{C}^3$ LPCC distinguishable?

ACKNOWLEDGMENTS

This work was partly supported by the National Natural Science Foundation of China (Grants No. 60736011 and No. 60702080), and the Centre for Quantum Computation & Intelligent Systems, University of Technology, Sydney.

[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 Inf. Comput. **5**, 156 (2005).
[4] J. Watrous, Phys. Rev. Lett. **95**, 080505 (2005).
[5] A. Winter, e-print 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, and M. Ying, IEEE Trans. Inf. Theory **55**, 1320 (2009).
[13] R. Duan, Y. Xin, and M. Ying, Phys. Rev. A **81**, 032329 (2010).
[14] C. King and D. Matysiak, J. Phys. A: Math. Theor. **40**, 7939 (2007).