Bipartite Subspaces Having No Bases Distinguishable by Local Operations and Classical Communication

John Watrous*

Institute for Quantum Information Science and Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4

(Received 16 March 2005; published 18 August 2005)

It is proved that there exist subspaces of bipartite tensor product spaces that have no orthonormal bases that can be perfectly distinguished by means of local operations and classical communication. A corollary of this fact is that there exist quantum channels having suboptimal classical capacity even when the receiver may communicate classically with a third party that represents the channel's environment.

DOI: 10.1103/PhysRevLett.95.080505 PACS numbers: 03.67.−a, 03.65.Ud

Introduction.—One of the main goals of the theory of quantum information in recent years has been to understand the powers and limitations of local operations and classical communication (LOCC) *protocols*. These are protocols wherein two or more physically separated parties possess the ability to perform arbitrary operations on local quantum systems and to communicate with one another, but only classically. The paradigm of LOCC provides a setting in which to address basic questions about the nature of entanglement and nonlocality, generally viewed as principal characteristics of quantum information.

One particular question along these lines that has been considered by several researchers is that of LOCC *distinguishability* of sets of states. In the two-party case, the two parties (Alice and Bob) share one of a known orthogonal collection of pure states, and their goal is to determine which of the states it is [1–10]. In some cases it is possible for Alice and Bob to perform this task without error and in some it is not. For example, the fundamental result of Walgate *et al.* [9] establishes that any two orthogonal pure states can be distinguished without error. On the other hand, large sets of maximally entangled states cannot; for instance, if Alice's and Bob's systems each correspond to n dimensional spaces, then it is impossible for them to perfectly distinguish $n + 1$ or more maximally entangled states [7]. Other examples of sets of orthogonal states that cannot be perfectly distinguished by LOCC protocols include those of Ref. [1] and any set of states forming an unextendable product basis [2]. These examples demonstrate that entanglement is not an essential feature of LOCC-indistinguishable sets of states given that these sets contain only product states.

This Letter considers a related question, which is whether there exist subspaces of bipartite tensor product spaces such that *no* orthonormal basis of the subspace has the property that its elements can be perfectly distinguished by means of an LOCC protocol. Many examples of LOCC-indistinguishable sets fail to give an example of such a subspace in that they span subspaces for which one can easily find a perfectly distinguishable basis. For example, the four Bell states are not perfectly distinguishable by any LOCC protocol, but the space spanned by these states obviously does have a perfectly distinguishable basis—the standard basis. Indeed, *every* subspace of a tensor product space $\mathcal{A} \otimes \mathcal{B}$ for which $\dim(\mathcal{A}) = \dim(\mathcal{B}) = 2$ has a basis whose elements can be perfectly distinguished by some LOCC protocol, and therefore fails to have the property we are considering. We prove, however, that if the dimension of both $\mathcal{A}$ and $\mathcal{B}$ is at least three, then there do exist subspaces of $\mathcal{A} \otimes \mathcal{B}$ with the property that no basis of the subspace is LOCC distinguishable. In particular, it is proved that in the case $n = \dim(\mathcal{A}) = \dim(\mathcal{B})$ for $n \geq 3$, the subspace of dimension $n^2 - 1$ that is orthogonal to the canonical maximally entangled state (or any other fixed maximally entangled state) has this property.

One motive for investigating this property is to identify quantum channels having suboptimal classical corrected capacity with respect to the definition of Hayden and King [11]. More precisely, Hayden and King considered the situation in which a sender transmits classical information over a quantum channel to a receiver, who has the added capability to measure the environment and use the result to correct the channel's output. This notion of correcting the output of a quantum channel by measuring the environment was considered earlier by Gregoratti and Werner [12], who focused primarily on the quantum capacity of such channels. Based on the result of Walgate *et al.* [9], Hayden and King proved that the *classical corrected capacity* of any quantum channel is at least 1 bit of information. Many natural examples of channels can easily be seen to, in fact, have *optimal* classical corrected capacity, meaning that the capacity is $\log_2 n$ for n the dimension of the input space, and no examples of channels were previously proved to have less than optimal classical corrected capacity. The existence of subspaces having no LOCC-distinguishable bases implies the existence of such channels, even if the definition of Hayden and King is extended to allow two-way communication between the receiver and the environment.

Preliminaries.—Standard mathematical notation rather than Dirac notation is used to represent vectors and linear mappings in this Letter. All vector spaces discussed are assumed to be finite dimensional complex vector spaces. The standard basis of a vector space $\mathcal{X}$ of the form $\mathcal{X} = \mathbb{C}^n$ is $\{e_1, \ldots, e_n\}$, where e_i is the elementary unit vector defined by $e_i[j] = \delta_{ij}$. The space of linear mappings from a space $\mathcal{Y}$ to a space $\mathcal{X}$ is denoted $\mathrm{L}(\mathcal{Y}, \mathcal{X})$, and we write $\mathrm{L}(\mathcal{X})$ as shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$ and $\mathcal{X}^*$ as shorthand for $\mathrm{L}(\mathcal{X}, \mathbb{C})$. If $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$, then elements of $\mathcal{X}$ are identified with n dimensional column vectors, elements of $\mathcal{X}^*$ are identified with n dimensional row vectors, and elements of $\mathrm{L}(\mathcal{Y}, \mathcal{X})$ are identified with $n \times m$ matrices in the typical way. For $x \in \mathcal{X}$ we let $\bar{x} \in \mathcal{X}$ and $x^{\mathsf{T}}, x^* \in \mathcal{X}^*$ denote the entrywise complex conjugate, transpose, and conjugate transpose of x, and similar for linear mappings; $\bar{X} \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ and $X^{\mathsf{T}}, X^* \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ denote the entrywise complex conjugate, transpose, and conjugate transpose of $X \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$. The usual inner products on $\mathcal{X}$ and $\mathrm{L}(\mathcal{Y}, \mathcal{X})$ are given by $\langle x, y \rangle = x^* y$ and $\langle X, Y \rangle = \mathrm{tr}(X^* Y)$ for $x, y \in \mathcal{X}$ and $X, Y \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$. The standard basis of the space $\mathrm{L}(\mathcal{Y}, \mathcal{X})$ consists of the mappings $E_{i,j} = e_i e_j^*$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

The identity operator acting on a given space $\mathcal{X}$ is denoted $I_{\mathcal{X}}$, or just as I when $\mathcal{X}$ is implicit or otherwise understood. It is sometimes helpful to give different names to distinct but otherwise identical spaces; in particular, we assume that $\mathcal{A} = \mathbb{C}^n$ and $\mathcal{B} = \mathbb{C}^n$ are vector spaces referring to Alice's and Bob's systems, respectively. We define $I_{\mathcal{B},\mathcal{A}} \in \mathrm{L}(\mathcal{B}, \mathcal{A})$ to be the linear mapping that identifies vectors in $\mathcal{A}$ with vectors in $\mathcal{B}$ by identifying the standard bases of these spaces. Often this mapping is used implicitly. For instance, if $a \in \mathcal{A}$ and $b \in \mathcal{B}$ then $\langle a, b \rangle$ is shorthand for $\langle a, I_{\mathcal{B},\mathcal{A}} b \rangle$, and when $X \in \mathrm{L}(\mathcal{A}, \mathcal{B})$ we write $\mathrm{tr}(X)$ to mean $\mathrm{tr}(I_{\mathcal{B},\mathcal{A}} X)$.

It is convenient when discussing bipartite quantum states to define a linear bijection vec: $\mathrm{L}(\mathcal{Y}, \mathcal{X}) \rightarrow \mathcal{X} \otimes \mathcal{Y}$ by the action $\mathrm{vec}(E_{i,j}) = e_i \otimes e_j$ on standard basis elements, extending by linearity. For any choice of linear mappings A, X, and B the equation

$$(A \otimes B^{\mathsf{T}})\,\mathrm{vec}(X) = \mathrm{vec}(AXB)$$

is satisfied. For $\mathcal{A} = \mathbb{C}^n$ and $\mathcal{B} = \mathbb{C}^n$, the unit vector

$$\frac{1}{\sqrt{n}}\,\mathrm{vec}(I_{\mathcal{B},\mathcal{A}}) = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} e_i \otimes e_i \in \mathcal{A} \otimes \mathcal{B}$$

represents the canonical maximally entangled pure state in the space $\mathcal{A} \otimes \mathcal{B}$. Let $P \in \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ represent the projection onto the space spanned by this vector,

$$P = \frac{1}{n}\,\mathrm{vec}(I_{\mathcal{B},\mathcal{A}})\,\mathrm{vec}(I_{\mathcal{B},\mathcal{A}})^*,$$

and let $Q \in \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ denote the projection onto the orthogonal complement of this space, $Q = I_{\mathcal{A}\otimes\mathcal{B}} - P$. Also let $\mathcal{P}$ and $\mathcal{Q}$ denote the subspaces of $\mathcal{A} \otimes \mathcal{B}$ onto which P and Q project.

Separable measurements and LOCC state discrimination.—A *separable measurement* on $\mathcal{A} \otimes \mathcal{B}$ with possible outcomes $\{1, \ldots, N\}$ is a positive operator valued measure described by a collection $\{A_i \otimes B_i\colon i = 1, \ldots, N\} \subset \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ where each A_i and B_i is positive semidefinite. If we have that each of the operators A_i and B_i has rank equal to one, we will say that the measurement is a *rank one separable measurement.* If $u_1, \ldots, u_m \in \mathcal{A} \otimes \mathcal{B}$ is a collection of unit vectors, then the separable measurement $\{A_i \otimes B_i\colon i = 1, \ldots, N\}$ is said to *perfectly distinguish* this collection of vectors if there exists a partition $S_1 \cup \cdots \cup S_m = \{1, \ldots, N\}$, $S_k \cap S_l = \varnothing$ for $k \neq l$, such that

$$u_k^* \bigg(\sum_{i \in S_l} A_i \otimes B_i \bigg) u_k = \delta_{kl}$$

for $1 \leq k, l \leq m$.

Any measurement that can be realized by means of an LOCC protocol can be described by a rank one separable measurement, which implies that the following proposition holds.

Proposition 1. *If Alice and Bob can perfectly distinguish the states $u_1, \ldots, u_m$ by means of an LOCC protocol, then there exists a rank one separable measurement $\{a_i a_i^* \otimes b_i b_i^*\colon i = 1, \ldots, N\}$ that perfectly distinguishes $u_1, \ldots, u_m$.*

The converse of this proposition does not hold—see Refs. [1,13] for further information.

It will be helpful below in the proof of the main result to have noted a simple fact concerning rank one separable measurements. Assume $\{a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}}\colon i = 1, \ldots, N\}$ describes such a measurement. Then $\sum_{i=1}^{N} a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}} = I_{\mathcal{A}\otimes\mathcal{B}}$, and thus

$$\begin{aligned}\mathrm{vec}\,(I_{\mathcal{B},\mathcal{A}}) &= \bigg(\sum_{i=1}^{N} a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}} \bigg) \mathrm{vec}(I_{\mathcal{B},\mathcal{A}}) \\ &= \mathrm{vec}\bigg(\sum_{i=1}^{N} a_i a_i^* b_i b_i^* \bigg) = \mathrm{vec}\bigg(\sum_{i=1}^{N} \langle a_i, b_i \rangle a_i b_i^* \bigg).\end{aligned}$$

It therefore holds that $\sum_{i=1}^{N} \langle a_i, b_i \rangle a_i b_i^* = I_{\mathcal{B},\mathcal{A}}$. Taking the trace of both sides yields $\sum_{i=1}^{N} |\langle a_i, b_i \rangle|^2 = n$.

The main theorem.—We are now ready to prove the main result, which is stated in the following theorem.

Theorem 2. *For $n \geq 3$, there is no basis of $\mathcal{Q}$ that is perfectly distinguishable by an LOCC protocol.*

Proof.—The proof is by contradiction. To this end, assume $\{u_1, \ldots, u_m\}$ is an orthonormal basis of $\mathcal{Q}$ whose elements are perfectly distinguished by some LOCC protocol. Then there exists a rank one separable measurement $\{a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}}\colon i = 1, \ldots, N\}$ together with a partition $S_1 \cup \cdots \cup S_m = \{1, \ldots, N\}$, $S_k \cap S_l = \varnothing$ for $k \neq l$, such that

$$u_k^* \bigg(\sum_{i \in S_l} a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}} \bigg) u_k = \delta_{kl}$$

for all $1 \leq k, l \leq m$. Without loss of generality it may be assumed that $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are linearly independent for every choice of $i \neq j$.

As $u_k^*(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}}) u_k = |\langle u_k, a_i \otimes \bar{b}_i \rangle|^2$, it follows that u_k and $a_i \otimes \bar{b}_i$ are orthogonal whenever $i \notin S_k$. Consequently, it holds that $u_k^*(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}}) u_l = 0$ for $k \neq l$, given that S_k and S_l are disjoint. The projection Q acts trivially on each of the vectors $u_1, \ldots, u_m$, and thus $u_k^* Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})\; Q u_l = 0$ for $k \neq l$. Letting $v = \frac{1}{\sqrt{n}} \mathrm{vec}(I_{\mathcal{B},\mathcal{A}})$ we have $Qv = 0$, and thus $u_k^* Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})\; Qv = v^* Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})\; Qu_k = 0$ for each choice of k as well. It has been shown that the orthonormal basis $\{u_1, \ldots, u_m, v\}$ of $\mathcal{A} \otimes \mathcal{B}$ diagonalizes each of the operators $Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})Q$, for $1 \leq i \leq N$. As these operators are all simultaneously diagonalized by a common orthonormal basis, they must commute. To establish a contradiction completing the proof, it will therefore suffice to prove that there exists at least one choice of $i \neq j$ such that $Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})Q$ and $Q(a_j a_j^* \otimes \bar{b}_j b_j^{\mathsf{T}})Q$ do *not* commute.

Let $\alpha_{i,j} = (a_i^* \otimes b_i^{\mathsf{T}})Q(a_j \otimes \bar{b}_j)$ for all i, j. It will first be proved that there exists a choice of $i \neq j$ such that $\alpha_{i,j} \neq 0$. In order to prove this, assume toward contradiction that $\alpha_{i,j} = 0$ for every pair $i \neq j$. As

$$\begin{aligned} \alpha_{i,j} &= (a_i^* \otimes b_i^{\mathsf{T}})Q(a_j \otimes \bar{b}_j) \\ &= \langle a_i, a_j \rangle \langle b_j, b_i \rangle - \frac{1}{n} \langle a_i, b_i \rangle \langle b_j, a_j \rangle, \end{aligned}$$

this implies

$$\langle a_i, a_j \rangle \langle b_j, b_i \rangle = \frac{1}{n} \langle a_i, b_i \rangle \langle b_j, a_j \rangle$$

for all choices of $i \neq j$. Because $\sum_i |\langle a_i, b_i \rangle|^2 = n > 0$, we may choose some value of i for which $\langle a_i, b_i \rangle \neq 0$. We then have

$$\begin{aligned} \langle a_i, b_i \rangle &= a_i^* \Big(\sum_j \langle a_j, b_j \rangle a_j b_j^* \Big) b_i \\ &= \sum_j \langle a_j, b_j \rangle \langle a_i, a_j \rangle \langle b_j, b_i \rangle \\ &= \sum_{j \neq i} \langle a_j, b_j \rangle \langle a_i, a_j \rangle \langle b_j, b_i \rangle + \langle a_i, b_i \rangle \|a_i\|^2 \|b_i\|^2 \\ &= \frac{1}{n} \sum_{j \neq i} \langle a_j, b_j \rangle \langle a_i, b_i \rangle \langle b_j, a_j \rangle + \langle a_i, b_i \rangle \|a_i\|^2 \|b_i\|^2 \\ &= \Big(1 - \frac{1}{n} |\langle a_i, b_i \rangle|^2 + \|a_i\|^2 \|b_i\|^2 \Big) \langle a_i, b_i \rangle. \end{aligned}$$

As $\langle a_i, b_i \rangle \neq 0$ this implies $\frac{1}{n} |\langle a_i, b_i \rangle|^2 = \|a_i\|^2 \|b_i\|^2$. But then by the Cauchy-Schwarz inequality we have

$$|\langle a_i, b_i \rangle|^2 \leq \|a_i\|^2 \|b_i\|^2 = \frac{1}{n} |\langle a_i, b_i \rangle|^2,$$

which implies $|\langle a_i, b_i \rangle|^2 = 0$. This contradicts the fact that i was chosen so that $\langle a_i, b_i \rangle \neq 0$, and so it has been proved that $\alpha_{i,j} \neq 0$ for some choice of $i \neq j$. Fix such a choice for the remainder of the proof.

Next, let us prove that the two vectors $Q(a_i \otimes \bar{b}_j)$ and $Q(a_j \otimes \bar{b}_j)$ are linearly independent. To this end let β and γ be scalars that satisfy $\beta Q(a_i \otimes \bar{b}_i) + \gamma Q(a_j \otimes \bar{b}_j) = 0$. This implies

$$\beta a_i \otimes \bar{b}_i + \gamma a_j \otimes \bar{b}_j = \frac{1}{n} (\beta \langle b_i, a_i \rangle + \gamma \langle b_j, a_j \rangle) \mathrm{vec}(I_{\mathcal{B},\mathcal{A}}),$$

or equivalently

$$\beta a_i b_i^* + \gamma a_j b_j^* = \frac{1}{n} (\beta \langle b_i, a_i \rangle + \gamma \langle b_j, a_j \rangle) I_{\mathcal{B},\mathcal{A}}.$$

The left hand side of this equation has rank at most 2. Because we are assuming that $n \geq 3$, this means that the right hand side must be 0, for otherwise it would have rank $n \geq 3$. Thus $\beta a_i b_i^* + \gamma a_j b_j^* = 0$, which is equivalent to $\beta a_i \otimes \bar{b}_i + \gamma a_j \otimes \bar{b}_j = 0$. As $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are necessarily linearly independent, however, this implies that $\beta = \gamma = 0$. Consequently, $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ are linearly independent.

Finally, we will prove that the operators

$$\begin{aligned} Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})Q(a_j a_j^* \otimes \bar{b}_j b_j^{\mathsf{T}})Q = \alpha_{i,j} Q(a_i \otimes \bar{b}_i) \\ \times (a_j^* \otimes b_j^{\mathsf{T}})Q \end{aligned}$$

and

$$\begin{aligned} Q(a_j a_j^* \otimes \bar{b}_j b_j^{\mathsf{T}})Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})Q = \bar{\alpha}_{i,j} Q(a_j \otimes \bar{b}_j) \\ \times (a_i^* \otimes b_i^{\mathsf{T}})Q \end{aligned}$$

are not equal, which is equivalent to proving that $Q(a_i a_i^* \otimes \bar{b}_i b_i^{\mathsf{T}})Q$ and $Q(a_j a_j^* \otimes \bar{b}_j b_j^{\mathsf{T}})Q$ do not commute. Because $\alpha_{i,j} \neq 0$ and the vectors $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ are nonzero (as they are linearly independent), neither of these operators is 0. The images of the two operators are therefore the spaces spanned by the vectors $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$, respectively. The linear independence of $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ therefore implies that the two operators are not equal, which completes the proof.

It should be noted that the assumption $n \geq 3$ in Theorem 2 is necessary. Indeed, every subspace of a tensor product space $\mathcal{A} \otimes \mathcal{B}$ where $\mathcal{A} = \mathbb{C}^2$ and $\mathcal{B} = \mathbb{C}^2$ has a perfectly distinguishable basis. To see this, let $\mathcal{V}$ be a subspace of $\mathcal{A} \otimes \mathcal{B}$ and let $m = \dim(\mathcal{V})$. There is nothing to prove for $m = 0$ or $m = 1$, the claim for $m = 2$ follows from Walgate *et al.* [9], and it is trivial for $m = 4$. In the remaining case, $m = 3$, it must be that $\mathcal{V}$ is the orthogonal complement of some unit vector $u \in \mathcal{A} \otimes \mathcal{B}$. By considering the Schmidt decomposition of a given u, it is straightforward to find two product states $a_1 \otimes b_1$ and $a_2 \otimes b_2$ so that the set $\{u, a_1 \otimes b_1, a_2 \otimes b_2\}$ is orthonormal. Letting v be any vector orthogonal to the span of $\{u, a_1 \otimes b_1, a_2 \otimes b_2\}$, we have that $\{v, a_1 \otimes b_1, a_2 \otimes b_2\}$ is an orthonormal basis of $\mathcal{V}$. Walgate and Hardy [8] have shown that any such set is perfectly distinguishable given that at least two members of the set are product states.

Channels with suboptimal classical corrected capacity.—Hayden and King [11] considered the classical capacity of quantum channels when the receiver has the capability to measure the channel's environment and to use the classical result of this measurement when measuring the output of the channel. We now give examples of channels that have suboptimal capacity with respect to this definition. In fact, the capacity of the channels remains suboptimal even when two-way communication is allowed between the receiver and the environment.

As our aim is to prove only the existence of channels with suboptimal classical corrected capacity rather than proving quantitative bounds on this capacity, we will use the following qualitative definition that does not refer to any specific measure of capacity. An admissible (i.e., completely positive and trace-preserving) mapping Φ: $\mathrm{L}(\mathcal{X}) \rightarrow \mathrm{L}(\mathcal{A})$ is said to have *optimal two-way classical corrected capacity* if the following holds. (i) There exists a space $\mathcal{B}$ and a unitary embedding $U \in \mathrm{L}(\mathcal{X}, \mathcal{A} \otimes \mathcal{B})$ such that $\Phi(X) = \mathrm{tr}_{\mathcal{B}} U X U^*$ for all $X \in \mathrm{L}(\mathcal{X})$, and (ii) there exists an orthonormal basis $\{x_1, \ldots, x_n\}$ of $\mathcal{X}$ such that the set $U x_1, \ldots, U x_n \in \mathcal{A} \otimes \mathcal{B}$ is perfectly distinguishable by some LOCC protocol.

By the Stinespring dilation theorem, the collection of all choices for the unitary embedding U in item (i) are equivalent up to a unitary operator on $\mathcal{B}$, and consequently a given mapping Φ fails to have optimal two-way classical corrected capacity if item (ii) fails to hold for even a single choice of U.

The admissible mappings that fail to satisfy the above definition of optimality are based on the subspaces considered previously. Let $n \geq 3$, let $\mathcal{X} = \mathbb{C}^{n^2-1}$, and let $\mathcal{A} = \mathcal{B} = \mathbb{C}^n$. Choose $u_1, \ldots, u_{n^2-1} \in \mathcal{A} \otimes \mathcal{B}$ to be an arbitrary orthonormal basis for the subspace $\mathcal{Q}$ of $\mathcal{A} \otimes \mathcal{B}$. Define $U \in \mathrm{L}(\mathcal{X}, \mathcal{A} \otimes \mathcal{B})$ as

$$U = \sum_{i=1}^{n^2-1} u_i e_i^*.$$

This is a unitary embedding, implying that the mapping $\Phi \in \mathrm{L}(\mathcal{X}) \rightarrow \mathrm{L}(\mathcal{A})$ defined by $\Phi(X) = \mathrm{tr}_{\mathcal{B}} U X U^*$ for all $X \in \mathrm{L}(\mathcal{X})$ is admissible.

If Φ had optimal two-way classical corrected capacity, there would exist a choice of an orthonormal basis $\{x_1, \ldots, x_{n^2-1}\}$ of $\mathcal{X}$ such that $U x_1, \ldots, U x_{n^2-1} \in \mathcal{A} \otimes \mathcal{B}$ is perfectly distinguishable by an LOCC protocol. As any such set is necessarily an orthonormal basis of $\mathcal{Q}$, this cannot be by Theorem 2. We have therefore proved the following corollary.

Corollary 4. *The mapping Φ does not have optimal two-way classical corrected capacity.*

It is, of course, simple to adjust the above example to give a channel where the input and output spaces have the same dimension by viewing that the receiver's space $\mathcal{A}$ is embedded in $\mathcal{X}$. One may therefore view the example above for $n = 3$ as giving a three-qubit channel having suboptimal two-way classical corrected capacity.

Conclusion.—In this Letter it has been proved that there exist subspaces of bipartite tensor product spaces having no orthonormal bases whose elements can be perfectly distinguished by means of LOCC protocols. The existence of such subspaces gives a strong illustration of the limitations that face physically separated observers that measure composite systems—even given the freedom to preselect an orthonormal basis of such a subspace and to communicate classically during the measurement process, it may be impossible for separated observers to distinguish the states that form the basis. Previously this was known only for fixed collections of states rather than for arbitrary bases of a given subspace. An implication of the existence of such subspaces to channel capacities was also discussed. Specifically, channels having suboptimal classical corrected capacity, which were not previously known to exist, were constructed based on these subspaces.

There are several interesting, unanswered questions relating to subspaces having no LOCC-distinguishable bases. For instance, can such subspaces exist for a bipartite system in which one of the systems is a two-level system? As has been observed above, this would forbid the second system from also being a two-level system. Another question is ''What is the minimum possible dimension of such subspaces?'' The dimension must be at least 3, following from Walgate *et al.* [9], while the smallest dimension achieved in this Letter is 8. Finally, what sorts of quantitative bounds can be proved on the classical corrected capacity of quantum channels?

I thank Somshubhro Bandyopadhyay, Mehdi Mhalla, and Jonathan Walgate for several helpful discussions and suggestions. This research was supported by Canada's NSERC, the Canada Research Chairs program, and the Canadian Institute for Advanced Research (CIAR).

*Electronic address: jwatrous@cpsc.ucalgary.ca

[1] 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).

[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] P.-X. Chen and C.-Z. Li, Phys. Rev. A **68**, 062107 (2003).

[4] H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).

[5] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).

[6] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).

[7] M. Nathanson, J. Math. Phys. (N.Y.) **46**, 062103 (2005).

[8] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).

[9] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[10] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004).

[11] P. Hayden and C. King, Quantum Inf. Comput. **5**, 156 (2005).

[12] M. Gregoratti and R. F. Werner, J. Math. Phys. (N.Y.) **45**, 2600 (1999).

[13] E. Rains, quant-ph/9707002.