Distinguishability of complete and unextendible product bases

S. De Rinaldis[1,2,*]
[1]*Chemical Physics Theory Group, Department of Chemistry, University of Toronto, 80 St. George Street, Toronto, Ontario M5S 3H6, Canada*
[2]*IBM T.J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598, USA*
(Received 24 November 2004; published 12 August 2004)

It is not always possible to distinguish multipartite orthogonal states if only local operations and classical communication (LOCC) are allowed. We prove that we cannot distinguish the states of an unextendible product basis by LOCC even with infinite resources (infinite-dimensional ancillas, infinite number of operations). Moreover we give a necessary and sufficient condition for the LOCC distinguishability of a complete product basis.

DOI: 10.1103/PhysRevA.70.022309 PACS number(s): 03.67.−a, 03.65.−w, 89.70.+c

In quantum mechanics orthogonal quantum states can always be distinguished. This is not always true when we restrict the set of actions on the multipartite system to local operations and classical communication (LOCC) only. On this issue a number of results has been proved: three Bell states can never be distinguished [1], two orthogonal states can always be distinguished [2], a characterization of the $2\times n$ states that can be distinguished by LOCC has been given [3]. More surprisingly, there are pure orthogonal product vectors that can be distinguished only globally [4]. In this paper we prove that a class of product states, the unextendible product bases (UPB), cannot be distinguished by LOCC, and give a necessary and sufficient condition for the distinguishability of complete product bases. Therefore there is an entire class of separable superoperators that cannot be implemented by LOCC. With probabilistic LOCC, instead, every complete product basis can be distinguished [5,6], since a set of states is distinguishable by probabilistic LOCC if and only if it is distinguishable by separable superoperators. There are instead some UPB (but not all) that are not distinguishable even by separable operators (and therefore by probabilistic LOCC) [10].

Definition 1. We say that we cannot distinguish "perfectly" a set of states by LOCC if we cannot distinguish between them even using an infinite number of resources (infinite number of LOCC "rounds," infinite dimensional ancillas, etc.) while "exact" distinguishability is defined when finite resources are used.

The distinction could appear of little importance if we think that in practical situations we never have an infinite amount or resources, but it seems significant if we restate it in terms of information. If we cannot distinguish exactly, but perfectly, between a set of states then we can acquire as much information as we want about the states, therefore we could optimize the amount of resorces employed versus the information attainable. If the states cannot be distinguished perfectly, then the information we can obtain between them is bounded above by a finite amount. In terms of superoperators theory, this implies that we have found an entire class of separable superoperators that are not in the class of LOCC superoperators [7].

Definition 2. Consider a multipartite Hilbert space $H=H_1\otimes H_2\otimes\ldots\otimes H_n$ and a product basis that span a space H_{PB}. An unextendible product basis (UPB) [8] is a product basis whose complementary subspace $H_{PB}^{\perp}$ does not contain product vectors. Let us introduce the concept of "irreducible product basis."

Definition 3. An "irreducible product basis" is a product basis in $H_A\otimes H_B$ that cannot be divided in two set of vectors contained, respectively, in the subspaces $H'_A\otimes H_B$ and $H'^{\perp}_A\otimes H_B$ (or $H_A\otimes H'^{\perp}_B$ and $H_A\otimes H'^{\perp}_B$). "Irreducible UPB" and "irreducible complete product basis" are specific cases considered in this paper.

Every UPB contains an "irreducible UPB" in one of its subspaces. It is trivial to prove that, if this assumption were false, then the UPB would be a complete product basis. UPBs have been studied for their properties related to bound entanglement [9]. Bennett *et al.* [4] have shown a set of nine orthogonal product states that cannot be perfectly distinguished by LOCC. This is the only example known to us. Are there other product states that are not perfectly distinguishable? In this paper we answer to this question by showing a class of product states, the UPB, that can never be perfectly distinguished by LOCC. It has already been proven that UPB cannot be exactly distinguishable [10]. This is relevant because it proves that there is an entire class of separable superoperators that cannot be implemented by LOCC, i.e., the two classes are *not* equal except for a few particular cases.

Theorem 1. We cannot perfectly distinguish an UPB (unextendible product basis) by LOCC operations.

Proof. Let us consider first a bipartite UPB: $\{|\psi_i\rangle=|\phi_i\rangle|\chi_i\rangle\}$. We will prove that the effect on every state of a (POVM) element we can apply, without creating nonorthogonal states, is either to eliminate a state or to create a state parallel to the previous one. Let us consider an Alice POVM element E. It is an hermitian operator, so it is diagonal in an orthonormal basis $|0\rangle\langle 0|,\ldots,|N\rangle\langle N|$. We expand the set of vectors $\{|\phi_i\rangle\}$ in this basis:

*Electronic address: srinaldi@chem.utoronto.ca

$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle c_{00}|\chi_0\rangle + |1\rangle c_{10}|\chi_0\rangle + \cdots + |N\rangle c_{N0}|\chi_0\rangle \\
&\vdots \\
|\psi_l\rangle &= |0\rangle c_{0l}|\chi_l\rangle + |1\rangle c_{1l}|\chi_l\rangle + \cdots + |N\rangle c_{Nl}|\chi_l\rangle \\
&\vdots \\
|\psi_k\rangle &= |0\rangle c_{0k}|\chi_k\rangle + |1\rangle c_{1k}|\chi_k\rangle + \cdots + |N\rangle c_{Nk}|\chi_k\rangle \qquad (1)
\end{aligned}
$$

Let us suppose that E is nonzero on $|\phi_0\rangle$. Since the resulting vectors $\{E\otimes I|\psi_i\rangle=(E|\phi_i\rangle)|\chi_i\rangle\}$ must remain orthogonal, the vectors orthogonal to $|\phi_0\rangle$ must remain orthogonal after the application of E, that is $\langle\phi_i|\phi_0\rangle=0\Rightarrow\langle\phi_i|E^\dagger E|\phi_0\rangle=0$. We write E in the diagonal basis: $E=\lambda_0|0\rangle\langle 0|+\ldots+\lambda_N|N\rangle\langle N|$, where the $\{\lambda_i\}$ are real positive numbers less than (or equal to) 1.

The orthogonality condition translates into the following equations:

$$c_{0i}^{*}\lambda_0^2 c_{00} + \cdots + c_{Ni}^{*}\lambda_N^2 c_{N0} = 0 \qquad (2)$$

for all the vectors for which

$$c_{0i}^{*}c_{00} + \cdots + c_{Ni}^{*}c_{N0} = 0. \qquad (3)$$

The condition above means that the product vector $|\psi_0'\rangle = |0\rangle\lambda_0^2 c_{00}|\chi_0\rangle + |1\rangle\lambda_1^2 c_{10}|\chi_0\rangle + \ldots\ldots + |N\rangle\lambda_N^2 c_{N0}|\chi_0\rangle$ is orthogonal to all the vectors to which $|\psi_0\rangle$ is orthogonal. The vector $|\psi_0'\rangle$ must be parallel to $|\psi_0\rangle$, because if not we could construct the vector $|\psi_0'\rangle - \langle\psi_0|\psi_0'\rangle|\psi_0\rangle$ that is orthogonal to all the vectors of the UPB, thus against the assumption that the product basis is unextendible. At this point we have considered only local measurement, i.e., we have restricted the set of Alice operators to POVM elements, but our results hold also in the general case. In fact, Alice action is described by a superoperator and for every operation element S, from the polar decomposition theorem, S is a product of a unitary (U) and a positive (E) operator: $S=EU$ (right polar decomposition). We have $S|\phi_i\rangle=(EU|\phi_i\rangle=E|\phi_i'\rangle$ where the set $\{|\phi_i'\rangle\}$ is an UPB because an UPB is tranformed in another UPB with a unitary operation U. It is trivial to see that if we could extend the basis to a new orthogonal product vector then we could apply U^{-1} to this vector to obtain a new product vector orthogonal to the previous set, unextendible by assumption. Therefore there is no loss of generality in considering only local measurements. The new set of vector $\{E|\psi_i\rangle\}$ is an UPB in the subspace spanned by the vectors that constitute the basis in which E is diagonal. If we could extend the product basis in this subspace to another product vector, this vector would be orthogonal also to the ones eliminated by E and therefore the starting basis would be extendible. In general the set $\{E|\psi_i\rangle\}$ could be a complete basis that, by definition, is a "trivial" UPB because it also has the property that we cannot find another product state orthogonal to all the member of the basis. However, in a local measurement with POVM elements $\{E_l\}$ we have just proved that the operators E_l are either orthogonal or proportional, therefore not all the sets $\{E_l|\psi_i\rangle\}$ can be complete bases unless the starting set $\{|\psi_i\rangle\}$ is a complete basis. From the property of the set $\{E_l\}$, we notice that even if we have an infinite number of elements in the set, only a finite number of outcomes are different. To prove the theorem excluding that we could distinguish with an infinite number of rounds we notice that, since the only two operations that we can perform with a measurement on a state is either to leave the state unchanged or to eliminate it, if we want that they remain orthogonal, at some point, when we could not eliminate other states, the only POVM that we could apply is proportional to the identity. However it is not sufficient to show that at some point of the LOCC protocol the state must become nonorthogonal, because in principle an infinite set of weak measurements strategies [11] is possible and if the states at every protocol step are "nearly" orthogonal they could still be distinguished. This is completely general, as proved by construction in [4], because any strategy involving weak and strong measurements can be replaced by a strategy involving only weak measurements. To complete the proof we must show that at some point if we want to acquire information about the states they should become nonorthogonal by a finite amount. At this point we will show that the mutual information between the measurement outcome and the state is less than the information obtainable by a nonlocal measurement. We will restrict the attention to an "irreducible UPB" and prove that the information attainable about the state of an irreducible UPB is bounded above by $O(\delta)$ where δ is the maximum overlap between two vectors of the new set of states. Since every UPB contains an "irreducible UPB" then it will follow that also the set of states forming the UPB are not distinguishable by LOCC. Let us consider an irreducible UPB and the first Alice operation. If we want that the states remain orthogonal, only an operator proportional to the identity is possible. In fact since we have proved that a POVM element either eliminate a vector or leave it unchanged, then we could either eliminate some vectors or leave all unchanged. The first case leads to a contradiction because we could divide the set of states of the UPB in two sets: the vectors eliminated in $H_A'\otimes H_B$ and the others in $H_A'^{\perp}\otimes H_B$, in constrast to the definition of irreducible UPB. If we want to leave all the vectors unchanged then we must apply an operator proportional to the identity. Therefore if we want that the states are "nearly" orthogonal, we must use an operator of the form $E=\lambda I+\lambda\delta' A$, where λ is a real positive number less than one, δ' is an infinitesimal real positive number related to the maximum overlap among the new set of vectors, and A is a positive operator. The maximum overlap between two states is

$$
\begin{aligned}
\max_{i,j(i\neq j)}\langle\phi_i|E^\dagger E|\phi_j\rangle &= \max_{i,j(i\neq j)}(2\lambda^2\delta'\langle\phi_i|A|\phi_j\rangle \\
&\quad + \lambda^2\delta'^2\langle\phi_i|A^\dagger A|\phi_j\rangle) \\
&> \max_{i,j(i\neq j)} 2\lambda^2\delta'\langle\phi_i|A|\phi_j\rangle = \delta' c, \qquad (4)
\end{aligned}
$$

where c is a real number. We define $p(\phi_i,m)$ as the probability that, once the measurement result m is obtained, the state is $|\phi_i\rangle$. The probabilities before starting the protocol are all the same. We define

$$\epsilon = \max_i p(\phi_i,m) - \frac{1}{n}, \tag{5}$$

where ϵ is the maximum amount of information we can obtain about a state. From the definition we have

$$p(\phi_i,m) = \frac{\langle\phi_i|E_m^\dagger E_m|\phi_i\rangle}{\sum_j \langle\phi_j|E_m^\dagger E_m|\phi_j\rangle}. \tag{6}$$

If we define $a_j = 2\langle\phi_j|A|\phi_j\rangle$ we have, neglecting the terms in δ'^2

$$p(\phi_i,m) = \frac{1+\delta' a_i}{n+\delta'\sum_j a_j} \leqslant \frac{1}{n} + \frac{\delta' a_i}{n}. \tag{7}$$

Therefore

$$\epsilon = \max_i p(\phi_i,m) - \frac{1}{n} \leqslant \max_i \delta' \frac{a_i}{n}. \tag{8}$$

This last equation means that if we want to acquire a finite amount of information, then also the states are nonorthogonal by a finite amount. Let us consider N rounds of measurements. We can write a general operation element implemented by LOCC as [12]

$$S_m = A_m \otimes B_m, \tag{9}$$

$$A_m = E_N E_{N-1} \ldots E_1, \tag{10}$$

$$B_m = F_N F_{N-1} \ldots F_1, \tag{11}$$

where E_i and F_i are positive operators. We can consider only the product of positive operators. In fact let us consider a general separable operator $S'_m = A'_m \otimes B'_m$. $A'_m = H_N H_{N-1} \ldots H_1$ and $B'_m = K_N K_{N-1} \ldots K_1$. We can construct an operator $S_m = S_N S_{N-1} \ldots S_1$, where S_i is a positive operator such that $\langle\phi_i|H_m^\dagger H_m|\phi_i\rangle = \langle\phi_i|S_m^\dagger S_m|\phi_i\rangle$. We use first a left polar decomposition: $H_i = U_i E_i$ and we have $H_m = U_N E_N U_{N-1} E_{N-1} \ldots U_1 E_1$, then we take all the unitary operators to the left, thanks to the fact that every linear operator has a left and a right polar decomposition: $E_1 U_1 = U_2 E_2$. After some steps we arrive at a "generalized" polar decomposition: $H_m = U_N U_{N-1} \ldots U_1 S_N S_{N-1} \ldots S_1$. Therefore the result is formally equivalent to a product of positive operators.

To maintain the states nearly orthogonal in every round we must have: $E_i = \lambda_i I + \lambda_i \delta' A_i$ and $F_i = \rho_i I + \rho_i \delta' B_i$.

Following the same procedure of the single step case, we have that the overlap between two states is (with $j \neq k$, neglecting the terms superior to first order in δ')

$$\begin{aligned}\delta &= \max_{j,k} \delta_{jk} = \max_{j,k} \langle\phi_j|S^\dagger S|\phi_k\rangle \\ &= \max_{j,k} \sum_i \left(2\delta'\lambda_i\rho_i\langle\phi_j|A_i\otimes I|\phi_k\rangle + 2\delta'\lambda_i\rho_i\langle\phi_j|I\otimes B_i|\phi_k\rangle\right) \\ &= \max_{j,k} \delta' \sum_i \lambda_i\rho_i(a_{ijk}+b_{ijk}),\end{aligned} \tag{12}$$

where $a_{ijk} = 2\langle\phi_j|A_i\otimes I|\phi_k\rangle$ and $b_{ijk} = 2\langle\phi_j|I\otimes B_i|\phi_k\rangle$.

Following the same calculation that leads to Eq. (8) we can find that

$$\epsilon = \max_i p(\phi_i,m) - \frac{1}{n} \leqslant \delta'\lambda_i\rho_i \sum_j (c_{ij}+d_{ij}), \tag{13}$$

where $c_{ij} = a_{ij}/n$ and $d_{ij} = b_{ij}/n$ ($a_{ij} = 2\langle\phi_j|A_i\otimes I|\phi_j\rangle$ and $b_{ij} = 2\langle\phi_j|I\otimes B_i|\phi_j\rangle$).

In order to find a relation analog to Eq. (4), we notice that formally we are in the same situation but with the operator $O(N) = \sum_{i=1}^N \lambda_i\rho_i(A_i\otimes I + I\otimes B_i)$, and we find, analog to (8)

$$\epsilon_N \leqslant \delta' \frac{a_i}{n} = \delta' M_N, \tag{14}$$

where $a_i = \langle\phi_i|O(N)|\phi_i\rangle$ and

$$\max_{j,k(j\neq k)} \langle\phi_j|S^\dagger S|\phi_k\rangle = \delta = \delta' c_N, \tag{15}$$

where $c_N = \max_{j,k(j\neq k)}\langle\phi_j|O(N)|\phi_k\rangle$. We arrive at the final expression

$$\epsilon_N \leqslant \delta \frac{M_N}{c_N}. \tag{16}$$

Let us consider the behavior of $O(N)$ when $N\to\infty$. We examine the different cases. If $\|O(N)\|\to\infty$ we can write $O'(N) = K_N O(N)$ (where $K_N\to\infty$) and $\|O'(N)\|\to a$ (a real number), so the ratio $\frac{M_N}{c_N}$ is finite because the K_N in the ratio cancel. The same argument holds if $\|O(N)\|\to 0$. If $O(N)$ tends to a multiple of the identity (when $N\to\infty$), then $c_N \to 0$, but not M_N, so we cannot bound ϵ with a multiple of δ as in Eq. (16). However, we can easily see that in this case we do not need the bound (16) to see that we cannot extract a finite amount of information about the states. In fact from Eqs. (5) and (6) we can easily calculate that $\epsilon\to 0$ [13]. We conclude that if we mantain the states nonorthogonal by an infinitesimal amount, we cannot reach a finite amount of information about them. The generalization to N-parties states i straightforward. It simply leads to a redefinition of $O(N)$; for example for three parties it becomes: $O(N) = \sum_{i=1}^N A_i\otimes I \otimes I + I\otimes B_i\otimes I + I\otimes I\otimes C_i$ and the conclusions are the same.

Now let us consider the case in which the state is nonorthogonal by a finite amount δ at Nth measurement round, that we consider stage I. The stage II is when the protocol is completed. We will generalize the argument in Ref. [4], that, indeed, is very general, i.e., does not depend on neither the number of parties nor on the number of states, finding a bound for the mutual information attainable. We use the same notation of Ref. [4]; $M_{\rm I}(M_{\rm II})$ is the random variable describing the stage-I (stage-II) outcomes; W is the variable that figures out which of the states has been measured; $I(W;M_{\rm I},M_{\rm II})$ is the mutual information between the measurement outcomes $M_{\rm I}$, $M_{\rm II}$ and W. Using the additivity property and the definition of mutual information we find

$$I(W;M_{\mathrm{I}},M_{\mathrm{II}}) = \log_2 n - \sum_{m_{\mathrm{I}}} p(m_{\mathrm{I}})[H(W|m_{\mathrm{I}}) - \mathrm{I}(W;M_{\mathrm{II}}|m_{\mathrm{I}})], \tag{17}$$

where n is the number of states to be distinguished, $p(m_{\mathrm{I}})$ is the probability of outcome m_{I} of the measurement in stage I, H is the entropy function. At the end of stage I the states are $\rho_i = |\phi_{i,m_{\mathrm{I}}}\rangle\langle\phi_{i,m_{\mathrm{I}}}|$ with probabilities $q_i = p(\psi_i|m_{\mathrm{I}})$ and $\{M_b\}$ is a positive operator valued measurement performed in stage II. Let us consider the two states that are nonorthogonal at stage I $\langle\phi_{1,m_{\mathrm{I}}}|\phi_{2,m_{\mathrm{I}}}\rangle = \delta$ and divide the density operator in two parts

$$\tau_1 = \sum_{i=1}^{2} \frac{q_i}{s_1}\rho_i, \quad \tau_2 = \sum_{i=3}^{n} \frac{q_i}{s_2}\rho_i \tag{18}$$

with $s_1 = q_1 + q_2$ and $s_2 = 1 - s_1$. We have $\rho = s_1\tau_1 + s_2\tau_2$. Using the concavity of Shannon entropy and removing the dependence of all the states except the first two we arrive at the expression

$$\begin{aligned} &H(W|m_{\mathrm{I}}) - \mathrm{I}(W;M_{\mathrm{II}}|m_{\mathrm{I}}) \\ &\quad \geqslant 2\left[\left(\frac{1}{n} - (n-1)\epsilon\right)\right]\left[1 + \sum_b (tr\tau_1 M_b)\log_2(tr\tau_1 M_b)\right. \\ &\quad \left. - \sum_{i=1}^{2}\frac{1}{2}\sum_b (tr\rho_i M_b)\log_2(tr\rho_i M_b)\right]. \end{aligned} \tag{19}$$

Minimizing the expression above as in Ref. [4] we find

$$\begin{aligned} H(W|m_{\mathrm{I}}) - I(W;M_{\mathrm{II}}|m_{\mathrm{I}}) \geqslant 2\left[\left(\frac{1}{n} - (n-1)\varepsilon\right)h\left(\tfrac{1}{2}\right.\right. \\ \left.\left. - \tfrac{1}{2}\sqrt{1-\delta^2}\right)\right]. \end{aligned} \tag{20}$$

The quantity in Eq. (20) is strictly positive if $\delta > 0$.

Therefore we conclude that $\mathrm{I}(W;M_1,M_{\mathrm{II}}) < \log_2 n$ if the states at some stage of the protocol are nonorthogonal by a finite amount. Note that part (iii) of the proof is valid for a general set of states and measurements. The extension to the multipartite case is immediate. This completes the proof.

Theorem 2 [14]. A complete product basis is distinguishable by LOCC *if and only if* it does not contain an "irreducible complete product basis." Moreover, if a complete product basis is distinguishable by LOCC, then it is distinguishable by von Neumann measurements.

Proof. The proof follows from the results on UPB; in fact a complete basis is a trivial UPB, because it has the property that we cannot find another product state orthogonal to all the member of the basis. In the proof of Theorem 1 we have only used the property, common to UPB and complete product bases, that another product states, orthogonal to all the members of the set, does not exist. Therefore if the complete basis contains an irreducible complete product basis, then the information attainable about that set of states is less, by a finite amount, then the maximum information. Otherwise, by definition, we can divide the states in two set of vectors contained in the subspaces $H'_A \otimes H_B$ and $H'^{\perp}_A \otimes H_B$ or $H_A \otimes H'_B$ and $H_A \otimes H'^{\perp}_B$. This fact gives a procedure for distinguishing the states by a protocol consisting only in von Neumann measurements: we use the projectors P_A and $P_A^{\perp}$ (or P_B and $P_B^{\perp}$) that project, respectively, on subspace $H'_A \otimes H_B$ and $H'^{\perp}_A \otimes H_B$ (or $H_A \otimes H'_B$ and $H_A \otimes H'^{\perp}_B$). We can iterate this procedure until only one state remains, so we have successfully completed the task. This completes the proof.

Remark. Since it cannot always be obvious to check if a complete basis contains or not an "irreducible complete product basis," we can give a method to check the perfect distinguishability of a complete basis with a simple algorithm, without involving lenght calculations. The method works as follows: Let us first consider the Alice vector and construct an ensemble; we start with one vector and find all the vectors that are nonorthogonal to it; we have therefore constructed a set of vectors; we expand this set performing a series of steps in each one we find the vectors nonorthogonal to at least one member of the set. Since a POVM element that is nonzero on one vector of this set must have as eigenvectors all the vectors of the set for construction, then it could be only the identity in the subspace spanned by the vectors of the set. Thus if this protocol finds all the vectors of the basis, then the only POVM element we can apply is the identity. If the same holds also for Bob vectors, then whatever POVM elements we apply (except the identity) we create nonorthogonal states and therefore we cannot perfectly distinguish the states. In general if we find only a subset of the total set of vectors, we split in two the total set of states with a von Neumann measurement. After that the protocol continues with classical communication to Bob; Bob repeats the same procedure. This protocol continues until either we distinguish the states or we arrive at a point where only the identity can be applied (that means that we have found an "irreducible complete product basis").

Note that at most Σn_j steps [therefore $(\Sigma n_j) - 1$ bits of classical communication], where n_j are the dimensions of the multipartite Hilbert space, are necessary to distinguish between the states, since every step must eliminate at least one dimension of the total space. Therefore the number of bits grows at most linearly, whereas the number of states grows exponentially with the number of parties.

Example. As a corollary of Theorem 2 we can answer to the question (posed in Ref. [4]) of LOCC distinguishability of the Lagarias-Shor 1024 state ten-parties complete basis [16]. Every party has a qubit which is one state out of $|0\rangle$, $|1\rangle$, $|0+1\rangle$, $|0-1\rangle$. Since for every party in the set of 1024 states there are all the four states above, then the states cannot be divided in two orthogonal subspaces. Therefore this complete basis is an irreducible complete product basis. We conclude that this basis is not perfectly distinguishable by LOCC.

ACKNOWLEDGMENTS

The main part of this work was completed at IBM T.J. Watson Research Center. I would like to thank the Quantum Information Group at IBM for their hospitality; Dr. David DiVincenzo for useful discussion, advice, and a careful reading of the manuscript; Dr. Charles Bennett and Dr. Barbara Terhal for helpful discussions.

[1] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).
[2] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[3] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
[4] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. A **59**, 1070 (1999).
[5] M. Horodecki, A. Sen (De), U. Sen, K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
[6] A. Chefles, quant-ph/0302066.
[7] E. Rains, Phys. Rev. A **60**, 173 (1999).
[8] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[9] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[10] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Commun. Math. Phys. **238**, 379 (2003).
[11] Y. Aharonov, D. Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).
[12] This is only a necessary condition for writing a LOCC operator. Actually in the proof we never use neither that in every round the POVM element must sum to the identity nor classical communication. In fact the Part II of the proof is valid for separable operators, but only for the ones "near" the identity, since a complete product basis is always distinguishable by separable superoperators.
[13] The fact, proved in part (i), that there are not POVM elements (except multiples of the identity, that keep the states orthogonal, is essential. If not we could have $\epsilon > 0$ and $\delta = 0$ after stage I.
[14] In the particular case of the nine dominolike state of Ref. [4], in Refs. [3,15] a similar argument is applied showing that a POVM different from the unitary operator leads to nonorthogonality of states. However it requires to write the equations for the specific case and to prove that they have no solutions.
[15] B. Groisman and L. Vaidman, e-print quant-ph/0103084.
[16] J. C. Lagarias, and P. Shor, Bull. Am. Math. Soc. **27**, 279 (1992); Discrete Comput. Geom. **11**, 359 (1994).