Class of unambiguous state discrimination problems achievable by separable measurements but impossible by local operations and classical communication

Scott M. Cohen*
Department of Physics, Portland State University, Portland, Oregon 97201, USA
(Received 13 August 2014; published 14 January 2015)

We consider an infinite class of unambiguous quantum state discrimination problems on multipartite systems, described by Hilbert space $\mathcal{H}$, of any number of parties. Restricting consideration to measurements that act only on $\mathcal{H}$, we find the optimal global measurement for each element of this class, achieving the maximum possible success probability of $1/2$ in all cases. This measurement turns out to be both separable and unique, and by our recently discovered necessary condition for local quantum operations and classical communication (LOCC) it is easily shown to be impossible by any finite-round LOCC protocol. We also show that, quite generally, if the input state is restricted to lie in $\mathcal{H}$, then any LOCC measurement on an enlarged Hilbert space is effectively identical to an LOCC measurement on $\mathcal{H}$. Therefore, our necessary condition for LOCC demonstrates directly that a higher success probability is attainable for each of these problems using general separable measurements as compared to that which is possible with any finite-round LOCC protocol.

DOI: 10.1103/PhysRevA.91.012321 PACS number(s): 03.67.Hk, 03.65.Ta, 03.67.Ac

I. INTRODUCTION

In a recent paper [1], we proved a necessary condition (reproduced as Theorem 1, below) that a multiparty quantum measurement can be implemented by local operations and classical communication (LOCC) in any finite number of rounds of communication. It is easily seen that such measurements must be separable—that is, the measurement operators must all be tensor products—and our Theorem 1 provides a strong, and quite general, constraint on the set of product operators representing any measurement implemented by finite-round LOCC. We also showed that the condition of Theorem 1 is extensively violated by separable measurements, a violation limited only by the size of the system, as measured by the number of parties involved.

Despite the generality of Theorem 1, we were unable, at the time of writing, to provide examples of separable measurements having obvious practical interest, and which violate the conditions of that theorem. A reasonable criticism, then, was that the theorem was "primarily of mathematical value with physical implications wanting" [2]. Here, we remedy this deficiency by providing an infinite class of physically motivated examples where the theorem can be directly used to demonstrate the LOCC impossibility of these specific operational tasks, each of which can, nonetheless, be implemented by separable measurements.

Our examples involve the optimal unambiguous discrimination of quantum states, a subject pioneered by Ivanovic [3], Dieks [4], and Peres [5]. This is one method of extracting information from nonorthogonal states, wherein due to this nonorthogonality the information cannot be obtained perfectly. There are numerous scenarios that involve the extraction of information under such conditions, including quantum cryptography and quantum key distribution [6]. It is therefore a subject of considerable significance in quantum information processing, with implications for both theory and experiment, and its study remains robust to this day [7–10].

In the scenario of unambiguous state discrimination, a quantum system is prepared in one of a given set of states, and the aim is to perform measurements on that system in order to determine in which state it was prepared. It is required that the error probability is zero—one can never guess one state when it happens to be another—which means that when the states are not mutually orthogonal there must be an inconclusive outcome, one for which the given state remains unknown.

Chefles [11] has shown that the states in the given set can be unambiguously discriminated if and only if they are linearly independent, and then the measurement involves the reciprocal set of states (see below). When the states form a symmetric set and the *a priori* probabilities are all equal, then an optimal measurement—one achieving the maximum possible success probability—was obtained in [12]. Later, Eldar [13] showed that the problem of finding an optimal measurement for an arbitrary set of linearly independent pure states can be formulated as a semidefinite programming problem.

We will assume that the quantum system under consideration is made up of P spatially separated parts, and that the separate parties utilize LOCC in order to discriminate the states. Chefles [14] found a condition, valid for both separable measurements and for LOCC, which is necessary and sufficient that a set of states can be unambiguously discriminated. The equivalence of LOCC and the full set of separable measurements for this question is not obvious, even though every LOCC is also separable [15]. The reason is the existence of separable measurements that cannot be implemented by LOCC, a discovery first made in [16]. Of course, this result of [14] does not say that, for unambiguous state discrimination, use of the full set of separable measurements is equivalent to using only LOCC, because there is still the question of finding an optimal measurement. Along these lines, it was shown in [17] that the success probability with general separable measurements can exceed that for LOCC for a pair of two-qubit states, one pure and the other mixed. As far as we are aware, this is the only known example of a separation between separable measurements and LOCC for unambiguous state discrimination. Here, we provide an infinite set of new examples showing such a separation, all of which only involve

*cohensm52@gmail.com

pure states, including one case involving two qubits. For these examples, we use Theorem 1 to show that LOCC cannot achieve as high a success probability as is possible with separable measurements. This then accomplishes a main goal of this paper, which is to demonstrate the utility of Theorem 1.

Consider a multipartite system of P parts, described by Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_P$ of overall dimension D, and a separable measurement on $\mathcal{H}$ consisting of N measurement operators $\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \cdots \otimes \mathcal{K}_j^{(P)}$ satisfying $\mathcal{K}_j \geqslant 0$ and $\sum_j \mathcal{K}_j = I$, with I the identity on $\mathcal{H}$. Following the ideas in [1], we consider the convex cones generated by the set of local operators $\{\mathcal{K}_j^{(\alpha)}\}$, for each α. As the number of operators is finite, these are polyhedral cones, having a finite number of extreme rays.[1] Let us count the distinct extreme rays in the convex cone generated by the set of local operators $\{\mathcal{K}_j^{(\alpha)}\}$, for each party α, and define this number to be e_α. Then, the following theorem was proved in [1].

Theorem 1. For any finite-round LOCC protocol of P parties implementing a separable measurement corresponding to the N distinct positive product operators $\{\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \ldots \otimes \mathcal{K}_j^{(P)}\}_{j=1}^N$, it must be that

$$\sum_{\alpha=1}^{P} e_\alpha \leqslant 2(N-1), \tag{1}$$

where e_α is the number of distinct extreme rays in the convex cone generated by operators $\{\mathcal{K}_j^{(\alpha)}\}_{j=1}^N$, and the sum includes only those parties for which at least one of these local operators is not proportional to the identity.

In [1], we presented separable measurements consisting of a set of product operators $\{\Psi_k\}_{k=1}^N$ for every D and prime $N > D$, for which the upper bound in this theorem is violated maximally, satisfying $\sum e_\alpha = PN$, thus demonstrating a very strong difference between separable measurements and LOCC. In Sec. II, we use these same operators to construct sets of states for which the optimal global measurement for unambiguous state discrimination is separable and (for present purposes, effectively) unique (see Theorem 2), and which cannot be implemented by finite-round LOCC, a result that follows immediately from Theorem 1. Theorem 2 thus demonstrates that the optimal probability of success, which is achievable by a separable measurement, cannot be achieved using finite-round LOCC, even when applied to an enlarged Hilbert space. In Sec. III, we give a proof of Theorem 2, and then we offer our conclusions in Sec. IV.

II. SEPARABLE MEASUREMENTS THAT ARE STRICTLY BETTER THAN LOCC

Consider any prime number $N \geqslant 5$ and a multipartite system having overall dimension $D = N - 1$. The number of parties P can be chosen in any way consistent with the prime factorization of D—this choice is generally not unique, but it is unimportant for our present purposes. Let $\mathcal{H}_\alpha$ be the Hilbert space describing party α's subsystem, and the overall Hilbert space is then $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_P$. Define states

$$|\Psi_j\rangle = \left|\psi_j^{(1)}\right\rangle \otimes \ldots \otimes \left|\psi_j^{(P)}\right\rangle, \quad j = 1, \ldots, N, \tag{2}$$

with

$$\left|\psi_j^{(\alpha)}\right\rangle = \frac{1}{\sqrt{d_\alpha}} \sum_{m_\alpha=0}^{d_\alpha-1} e^{2\pi i j p_\alpha m_\alpha / N} |m_\alpha\rangle, \tag{3}$$

where d_α is the dimension of $\mathcal{H}_\alpha$, with parties ordered such that $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_P$, and overall dimension $D = d_1 d_2 \ldots d_P$. Here, $p_1 = 1$ and, for $\alpha \geqslant 2, p_\alpha = d_1 d_2 \ldots d_{\alpha-1}$, and $|m_\alpha\rangle$ is the standard basis for party α. It was shown in [1] that

$$I = \frac{D}{N} \sum_{j=1}^{N} \Psi_j, \tag{4}$$

where $\Psi_j = |\Psi_j\rangle\langle\Psi_j|$.

We will choose D of the $|\Psi_j\rangle$ and then show they are a basis of the full space. First note that diagonal unitary

$$U^{(\alpha)} = \sum_{m_\alpha=0}^{d_\alpha-1} e^{2\pi i p_\alpha m_\alpha / N} |m_\alpha\rangle\langle m_\alpha|$$

permutes the states $|\psi_j^{(\alpha)}\rangle$. That is, $U^{(\alpha)}|\psi_j^{(\alpha)}\rangle = |\psi_{j+1}^{(\alpha)}\rangle$, and we have set $|\psi_{N+1}^{(\alpha)}\rangle = |\psi_1^{(\alpha)}\rangle$. Therefore, $U = U^{(1)} \otimes \cdots \otimes U^{(P)}$ permutes the $|\Psi_j\rangle$, showing that the latter N states are a symmetric set. (Note, however, that the chosen $D = N - 1$ states are *not* a symmetric set.) As a consequence, it does not matter which of the N states we omit in choosing a basis of the full D-dimensional space—any conclusions reached by omitting one could equally well have been reached by omitting any other—so without loss of generality we will choose to omit $|\Psi_1\rangle$.

Let us then define two sets of states,

$$\mathcal{S}_\Psi = \{|\Psi_j\rangle\}_{j=2}^N \tag{5}$$

and

$$\mathcal{S}_\Phi = \{|\Phi_j\rangle\}_{j=2}^N, \tag{6}$$

each set reciprocal to the other. [Given Eqs. (2) and (3), this reciprocity is how the $|\Phi_j\rangle$ are to be determined; see Eq. (8) below.] Our aim is to unambiguously discriminate $\mathcal{S}_\Phi$. Existence of a reciprocal set of states requires that the original set is linearly independent, so we must demonstrate that the D states of $\mathcal{S}_\Psi$ possess this property. Actually, the following lemma is more general than what we need.

Lemma 1. Given a prime number N and any $D \leqslant N$, any subset $\mathcal{I} \subseteq [1, \ldots, N]$ of D or fewer of the states $|\Psi_j\rangle$, defined in Eq. (2), constitutes a linearly independent set.

Proof. Consider

$$\begin{aligned} 0 &= \sum_{j\in\mathcal{I}} c_j |\Psi_j\rangle \\ &= \sum_{m_1=0}^{d_1-1} \cdots \sum_{m_P=0}^{d_P-1} \left(\sum_{j\in\mathcal{I}} c_j e^{2\pi i j \sum_\alpha p_\alpha m_\alpha / N} \right) |m_1 \ldots m_P\rangle \\ \iff 0 &= \sum_{j\in\mathcal{I}} c_j e^{2\pi i j \sum_\alpha p_\alpha m_\alpha / N} \forall m_1, \ldots, m_P. \end{aligned} \tag{7}$$

[1] A ray is a half-line of the form $\{\lambda \hat{\mathcal{K}}_j^{(\alpha)} | \lambda \geqslant 0\}$. An extreme ray of a convex cone is a ray that lies in the cone but cannot be written as a positive linear combination of other rays in that cone.

By an argument similar to that following Eq. (6) of [1], one sees that $\sum_\alpha p_\alpha m_\alpha$ takes on each value ranging from zero to $D-1$, and each of these values corresponds to a unique set of the indices, m_α. Choosing any $|\mathcal{I}|$ values of $k = k(\{m_\alpha\}) = \sum_\alpha p_\alpha m_\alpha$ from Eq. (7), we can represent these $|\mathcal{I}|$ constraints as $M\vec{c} = 0$, where the jth component of $\vec{c}$ is c_j, and $|\mathcal{I}| \times |\mathcal{I}|$ matrix M has components $M_{kj} = e^{2\pi i jk/N}$. It is clear that M is a submatrix of the $N \times N$ matrix $\Omega = (\omega^{jk})_{j,k=0}^{N-1}$, with $\omega = e^{2\pi i/N}$ a primitive root of unity. Then, by Chebotarëv's theorem on roots of unity [18], M is invertible. This implies that $c_j = 0$ for all $j \in \mathcal{I}$ and that the set $\{|\Psi_j\rangle\}_{j\in\mathcal{I}}$ is linearly independent, which completes the proof. ■

Given states $|\Psi_j\rangle$, the reciprocal states $|\Phi_j\rangle$ are defined by the relations

$$\langle\Psi_k|\Phi_j\rangle = \delta_{jk}\langle\Psi_j|\Phi_j\rangle \;\; \forall\; j,k = 2,\ldots,N. \tag{8}$$

The set of states $\mathcal{S}_\Phi$, given with *a priori* probabilities η_j, can be unambiguously discriminated [11] by the measurement $\mathcal{M}(\{w_j\})$ consisting of operators $\{w_j\Psi_j\}_{j=2}^N$ and one additional "failure" operator:

$$\Pi_f = I - \sum_{j=2}^{N} w_j\Psi_j. \tag{9}$$

To find an optimal measurement, the weights w_j are chosen so as to minimize the probability of failure,

$$\Pr(f) = \sum_{j=2}^{N} \eta_j \mathrm{Tr}(\Pi_f \Phi_j), \tag{10}$$

with $\Phi_j = |\Phi_j\rangle\langle\Phi_j|$.

Note that since the D chosen $|\Psi_j\rangle$ are linearly independent and a basis of the full Hilbert space $\mathcal{H}$, their reciprocal states $|\Phi_j\rangle$ are also linearly independent and a basis of $\mathcal{H}$. Therefore, since $\langle\Psi_k|\Phi_j\rangle = 0$ for all $j \neq k$, if for some k we replace $|\Phi_k\rangle$ by $|\Psi_k\rangle$ in the basis formed by the states in $\mathcal{S}_\Phi$, we will still have a basis of $\mathcal{H}$. This means that if we exclude $|\Phi_k\rangle$ from the set $\mathcal{S}_\Phi$ the only positive operator that annihilates all of the remaining states is Ψ_k, up to multiplicative factors. Hence, we have the following corollary to Lemma 1.

Corollary. The only positive operators acting on $\mathcal{H}$ that will unambiguously identify $|\Phi_k\rangle$ are those proportional to Ψ_k defined in Eq. (2). This implies that the only such measurements unambiguously discriminating the set $\mathcal{S}_\Phi$ are those of the form $\mathcal{M}(\{w_j\})$ defined above Eq. (9), and the only freedom available for optimizing these measurements lies in the choice of the w_j.

In the next section, we will prove the following theorem.

Theorem 2. If *a priori* probabilities $\eta_j = 1/D$ for all j, then the optimal global measurement, $\mathcal{M}_{\mathrm{opt}}$, for unambiguous discrimination of the set of states that is reciprocal to any $D = N-1$ of the states defined in Eq. (2) (i) is separable; (ii) is unique, when restricting to measurements that act only on $\mathcal{H}$; (iii) consists of measurement operators $D\Psi_j/N, j = 1,\ldots,N$; and (iv) achieves $\Pr(f) = 0.5$. In addition, $\Pr(f) > 0.5$ for this task when using any finite-round LOCC protocol.

The last statement in this theorem requires the following lemma, which is proved in the Appendix.

Lemma 2. Given a multipartite system of P parties described by Hilbert space $\mathcal{H}$, consider any enlargement of $\mathcal{H}$ to $\mathcal{H}'$. Then, for any LOCC protocol $\mathcal{L}$ implementing a measurement on $\mathcal{H}'$ that involves input states that are supported only on $\mathcal{H}$, there exists an effectively identical LOCC measurement on $\mathcal{H}$ which accomplishes precisely what is accomplished by $\mathcal{L}$.

Before moving on to the proof of Theorem 2, let us give an explicit example, providing expressions for the states, $|\Phi_j\rangle$, in the case of two qubits with $N = 5$. These four states are

$$\begin{aligned}
|\Phi_2\rangle &= \frac{1}{\sqrt{5+\sqrt{5}}}\big(-e^{-2\pi i/5}|00\rangle + (1+e^{-2\pi i/5})|01\rangle - (1+e^{2\pi i/5})|10\rangle + e^{2\pi i/5}|11\rangle\big),\\
|\Phi_3\rangle &= \frac{1}{\sqrt{5+\sqrt{5}}}\left(\frac{e^{2\pi i/5}}{2\cos(2\pi/5)}|00\rangle - |01\rangle - e^{\pi i/5}|10\rangle + (1+e^{-2\pi i/5})|11\rangle\right),\\
|\Phi_4\rangle &= \frac{1}{\sqrt{5+\sqrt{5}}}\big((1+e^{2\pi i/5})|00\rangle - e^{\pi i/5}|01\rangle + e^{\pi i/5}|10\rangle - (1+e^{2\pi i/5})|11\rangle\big),\\
|\Phi_5\rangle &= \frac{1}{\sqrt{5+\sqrt{5}}}\left(|00\rangle + \frac{e^{2\pi i/5}}{2\cos(2\pi/5)}|01\rangle + (1+e^{2\pi i/5})|10\rangle - e^{-2\pi i/5}|11\rangle\right).
\end{aligned} \tag{11}$$

We note that these states are all entangled, their reduced density matrices having von Neumann entropy approximately equal to 0.3, the same for all four states. The optimal measurement to unambiguously discriminate this set of states is given by operators $D\Psi_j/N, j = 1,2,3,4,5$, with

$$\begin{aligned}
|\Psi_1\rangle &= \tfrac{1}{2}(|00\rangle + e^{4\pi i/5}|01\rangle + e^{2\pi i/5}|10\rangle + e^{-4\pi i/5}|11\rangle),\\
|\Psi_2\rangle &= \tfrac{1}{2}(|00\rangle + e^{-2\pi i/5}|01\rangle + e^{4\pi i/5}|10\rangle + e^{2\pi i/5}|11\rangle),\\
|\Psi_3\rangle &= \tfrac{1}{2}(|00\rangle + e^{2\pi i/5}|01\rangle + e^{-4\pi i/5}|10\rangle + e^{-2\pi i/5}|11\rangle),\\
|\Psi_4\rangle &= \tfrac{1}{2}(|00\rangle + e^{-4\pi i/5}|01\rangle + e^{-2\pi i/5}|10\rangle + e^{4\pi i/5}|11\rangle),\\
|\Psi_5\rangle &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).
\end{aligned} \tag{12}$$

The failure operator in this case is $\Pi_f = D\Psi_1/N$. We now proceed to the proof of Theorem 2.

III. PROOF OF THEOREM 2

We begin by noting that Lemma 2 applies to any number of parties, including when there is only one. Therefore, if we find an optimal global measurement under the restriction that it acts only on $\mathcal{H}$, then this measurement is also optimal without such a restriction. Then, according to our corollary, we can find an optimal measurement by considering $\mathcal{M}(\{w_j\})$, defined by Eq. (9) and the sentence which precedes it, and then minimizing the probability of failure over all choices of the weights, w_j. Inserting Eq. (4) into Eq. (9), we have

$$\begin{aligned}\Pi_f &= \frac{D}{N}\sum_{j=1}^{N}\Psi_j - \sum_{j=2}^{N} w_j\Psi_j \\ &= \frac{D}{N}\Psi_1 + \sum_{j=2}^{N}\left(\frac{D}{N} - w_j\right)\Psi_j. \end{aligned} \tag{13}$$

For each $l \neq 1$, define a dual basis for the D states obtained by omitting $|\Psi_l\rangle$ from the full set $\{|\Psi_j\rangle\}_{j=1}^{N}$. Denote these bases—one basis for each l—as $|\xi_k^{(l)}\rangle$, which satisfy

$$\langle\xi_k^{(l)}|\Psi_j\rangle = \delta_{jk} \;\; \forall\; j,k \neq l. \tag{14}$$

Let us first show that $|\langle\xi_k^{(l)}|\Psi_l\rangle| = 1$. Recalling the comment in the sentence following Eq. (7), we have

$$0 = \sum_{j=1}^{N} e^{2\pi ij/N}|\Psi_j\rangle. \tag{15}$$

Since $|\xi_k^{(l)}\rangle$ is orthogonal to $|\Psi_j\rangle$ for all $j \neq k,l$, then multiplying Eq. (15) from the left by $\langle\xi_k^{(l)}|$ yields

$$0 = e^{2\pi ik/N} + e^{2\pi il/N}\langle\xi_k^{(l)}|\Psi_l\rangle, \tag{16}$$

and the desired result follows immediately. Recalling that $\Pi_f \geqslant 0$, we now have from Eq. (13) that

$$0 \leqslant \langle\xi_k^{(l)}|\Pi_f|\xi_k^{(l)}\rangle = \frac{D}{N} - w_k + \left(\frac{D}{N} - w_l\right)\left|\langle\xi_k^{(l)}|\Psi_l\rangle\right|^2, \tag{17}$$

or

$$w_k + w_l \leqslant \frac{2D}{N}, \forall k,l \neq 1, \tag{18}$$

a result we will use below.

We now turn to the failure probability,

$$\begin{aligned}\Pr(f) &= \frac{1}{D}\sum_{j=2}^{N}\mathrm{Tr}(\Pi_f\Phi_j) \\ &= \frac{1}{D}\sum_{j=2}^{N}\mathrm{Tr}\left(\left[I - \sum_{k=2}^{N} w_k\Psi_k\right]\Phi_j\right) \\ &= 1 - \frac{1}{D}\sum_{j=2}^{N} q_j w_j, \end{aligned} \tag{19}$$

where we have used Eq. (9) followed by Eq. (8), and defined $q_j = |\langle\Phi_j|\Psi_j\rangle|^2$. The q_j can be found by taking the inner product of $|\Phi_k\rangle$ with Eq. (15), obtaining

$$0 = e^{2\pi i/N}\langle\Phi_k|\Psi_1\rangle + e^{2\pi ik/N}\langle\Phi_k|\Psi_k\rangle, \tag{20}$$

which gives

$$q_k = |\langle\Phi_k|\Psi_1\rangle|^2. \tag{21}$$

On the other hand, multiplying Eq. (4) by Φ_k and taking the trace, we have

$$\begin{aligned}\frac{N}{D} &= |\langle\Phi_k|\Psi_1\rangle|^2 + |\langle\Phi_k|\Psi_k\rangle|^2 \\ &= 2q_k, \end{aligned} \tag{22}$$

having used Eq. (21) to obtain the last line. Hence,

$$q_k = \frac{N}{2D}\forall k = 2,\ldots,N. \tag{23}$$

Inserting this into Eq. (19), we have

$$\Pr(f) = 1 - \frac{N}{2D^2}\sum_{j=2}^{N} w_j. \tag{24}$$

Let us now see what happens if there exists k such that $w_k > D/N$. Then,

$$\begin{aligned}\sum_{j=2}^{N} w_j &= \sum_{2=j\neq k}^{N} w_j + w_k \\ &\leqslant \sum_{2=j\neq k}^{N}\left(\frac{2D}{N} - w_k\right) + w_k \\ &= (N-2)\frac{2D}{N} - (N-3)w_k \\ &< (D-1)\frac{2D}{N} - (D-2)\frac{D}{N} = \frac{D^2}{N}, \end{aligned} \tag{25}$$

where we used Eq. (18) to obtain the second line, and the fact that $D = N - 1$ to get the last inequality. Therefore, the maximum of this sum has $w_j = D/N$ for all $j = 2,\ldots,N$, because in this case

$$\sum_{j=2}^{N} w_j = \frac{D^2}{N}. \tag{26}$$

Maximizing this sum minimizes $\Pr(f)$ [see Eq. (24)], and since by Eq. (4) the latter choice of w_j is a valid complete measurement—having measurement operators $\{D\Psi_j/N\}_{j=1}^{N}$, with $\Pi_f = D\Psi_1/N$—this is therefore our optimal global measurement. From Eq. (24), we see that this measurement achieves

$$\Pr(f) = 0.5, \tag{27}$$

which is thus our optimal probability of failure. As each Ψ_j is a product operator, this measurement is clearly separable. By our corollary along with the fact, just demonstrated, that there is one and only one set of $\{w_j\}$ that minimizes $\Pr(f)$, it is also the unique optimal measurement whose action is restricted to $\mathcal{H}$. Since every operator in this measurement is a tensor product of positive, rank-1 operators on P parties, and noting that rank-1

positive operators are extreme rays in the convex cone of all positive operators and therefore must be extreme in the convex cone generated by any set of positive operators, each local part $\psi_j^{(\alpha)}$ of each Ψ_j is extreme in the collection of all $\psi_j^{(\alpha)}$, for each party α. We thus see that $e_\alpha = N$ for all α, and the sum of extreme rays yields $\sum_\alpha e_\alpha = PN > 2(N-1)$, an extensive violation of Theorem 1. Therefore, it is not possible to implement this measurement by finite-round LOCC acting on $\mathcal{H}$.

By Lemma 2 we see that for these input states and any LOCC measurement on an enlarged Hilbert space there is an effectively identical LOCC measurement on $\mathcal{H}$. The phrase "effectively identical" means that the two measurements have the same set of outcomes (excluding those outcomes that can never occur; see the Appendix), where each outcome in the measurement on the enlarged space has the same probability (and output state) as the corresponding outcome in the other measurement, which is a measurement that acts only on $\mathcal{H}$. Therefore, if there is a finite-round LOCC measurement on the enlarged Hilbert space that achieves the optimal probability of success, then its "effectively identical" counterpart, which achieves the same probabilities, is a finite-round LOCC measurement on $\mathcal{H}$ that also achieves that optimal probability of success. This is a contradiction, since we have just seen that no such measurement on $\mathcal{H}$ exists, implying there is no such LOCC measurement on the enlarged Hilbert space, either.[2] We therefore see that no finite-round LOCC protocol can be optimal, including those that act on an enlarged Hilbert space, and this completes the proof of Theorem 2.

IV. CONCLUSIONS

We have presented a class of problems involving the unambiguous discrimination of quantum states, and have shown in Theorem 2 that for each element in this class there exists an optimal, separable measurement, achieving the minimum possible failure probability of 0.5, which is the unique such measurement that acts only on the space $\mathcal{H}$ spanned by the set of states to be discriminated. We then demonstrated the utility of Theorem 1 of [1], a recently discovered necessary condition that a separable measurement can be implemented by finite-round LOCC, by using the latter theorem to (easily) prove that this separable measurement cannot be implemented by LOCC in any finite number of rounds. Finally, we showed that any LOCC measurement on an enlarged Hilbert space must also be strictly less than optimal. We note that this class of problems is infinitely large, having at least one element for each prime number N. (Generally it will, in fact, have more than one element for any given N, as long as $D = N-1$ is not the product of two primes.) Therefore, we have solved an infinite set of unambiguous discrimination problems, each of which has an optimal measurement that is separable, but for which there is no finite-round LOCC measurement that is optimal. Due to a result of [19], this class of problems includes an infinite number of examples for each number of parties, P, and we have included an explicit example here for the simplest system of two qubits [see Eq. (11)].

If the parties are given multiple copies of the chosen state,

$$\left|\Phi_j^{\otimes n}\right\rangle = \overbrace{|\Phi_j\rangle \otimes \cdots \otimes |\Phi_j\rangle}^{n \text{ copies}}, \tag{28}$$

then one can use the same arguments used above for a single copy to also show that there exists an optimal global measurement that is separable and that achieves the minimum possible $\Pr(f) = 2^{-n}$. This optimal measurement consists of the N^n measurement operators $\{(D/N)^n \Psi_{j_1} \otimes \Psi_{j_2} \otimes \cdots \otimes \Psi_{j_n}, j_k = 1, \ldots, N \forall k\}$, and one can easily show that this measurement cannot be implemented by finite-round LOCC, again by using Theorem 1. However, there are now an infinite number of other measurements that act only on the original Hilbert space and also achieve this same $\Pr(f)$, and we do not at present know whether any of these are separable, let alone if they are LOCC. It is thus an open question whether or not LOCC is as good as separable measurements for these states in the multiple-copy scenario.

For the single-copy case considered in this paper, we conjecture that the set of states $\mathcal{S}_\Phi$ cannot be optimally unambiguously discriminated by LOCC even with an infinite number of rounds of communication. We have discussed why we believe this is so in the conclusions of [1]. As an early step toward proving this conjecture, we have recently managed to prove a result which implies the following conclusion about the optimal measurement for this task, $\mathcal{M}_{\text{opt}}$ of Theorem 2: If there exists an LOCC protocol implementing $\mathcal{M}_{\text{opt}}$, then every branch of this protocol must continue for an infinite number of rounds. That is, in any such protocol, no outcome of any intermediate measurement can be terminal—the parties must continue measuring forever no matter what outcomes have been obtained in earlier rounds. While this result does not in itself prove the conjecture, it does strengthen our belief that $\mathcal{M}_{\text{opt}}$ cannot be implemented by LOCC even with an infinite number of rounds, and we hope to find a full proof of this result in the not-too-distant future.

ACKNOWLEDGMENTS

The author would like to thank Li Yu for helpful comments, and an anonymous referee for asking about the possibility of measurements on an enlarged Hilbert space, a question which led directly to Lemma 2. This work has been supported in part by the NSF through Grant No. 1205931.

APPENDIX: PROOF OF LEMMA 2

Consider any measurement on the enlarged Hilbert space $\mathcal{H}'$ and suppose the Kraus operators for that measurement are the set $\{K_j\}$. Define $\Pi = \Pi_1 \otimes \Pi_2 \otimes \ldots$ to be the projector (from $\mathcal{H}'$) onto the original system $\mathcal{H}$. Then, the set of Kraus operators, $\{K_j\Pi, I' - \Pi\}$, is a complete measurement on $\mathcal{H}'$, where I' is the identity operator on $\mathcal{H}'$. There is no guarantee that $I' - \Pi$ is a product operator, but one can write

$$\begin{aligned} I' - \Pi = {} & (I_1' - \Pi_1) \otimes I_2' \otimes \ldots \otimes I_P' \\ & + \Pi_1 \otimes (I_2' - \Pi_2) \otimes I_3' \otimes \ldots \otimes I_P' + \ldots \\ & + \Pi_1 \otimes \Pi_2 \otimes \ldots \otimes \Pi_{P-1} \otimes (I_P' - \Pi_P), \end{aligned} \tag{A1}$$

[2]Note that since Theorem 1 only provides a *necessary* condition for LOCC it may well be the case that the measurement on $\mathcal{H}'$ satisfies the bound in that theorem, even when that measurement cannot be implemented by LOCC.

which as we will see in a moment is a sum of product operators that, along with Π, can be implemented by LOCC. Now suppose the measurement under consideration, which acts on the larger space, can be implemented by LOCC using, say, protocol $\mathcal{L}$. Then, consider the LOCC protocol consisting of protocol $\mathcal{L}$ preceded by a series of measurements as follows: Party 1 starts out by doing a two-outcome measurement $\{\Pi_1, I'_1 - \Pi_1\}$. If she gets the second outcome, they terminate the protocol, but otherwise party 2 measures $\{\Pi_2, I'_2 - \Pi_2\}$. If he gets the second outcome, they terminate, but otherwise party 3 measures $\{\Pi_3, I'_3 - \Pi_3\}$, and so on until all parties have done this, after which they proceed with protocol $\mathcal{L}$. Now, since we consider only input states supported on $\mathcal{H}, I'_1 - \Pi_1$ has zero probability of occurrence, as do the other outcomes $I'_\alpha - \Pi_\alpha$ for each party α. Under these circumstances, the modification of protocol $\mathcal{L}$ becomes an LOCC measurement acting on the original space $\mathcal{H}$ alone, which has the exact same probabilities as does protocol $\mathcal{L}$, and in fact the output states for each branch of the protocol are also identical in the two cases.

Or perhaps it is more precise to put it this way: Since outcomes $I'_\alpha - \Pi_\alpha$ have zero probability of success, nothing changes if we simply begin at the point where Π has been implemented (after all P parties have performed their two-outcome measurements $\{\Pi_\alpha, I'_\alpha - \Pi_\alpha\}$). From a purely technical perspective, we cannot really do this on the enlarged space, because then the collection of measurement operators does not represent a complete measurement, but we can certainly do this on the original space instead of the enlarged one. Then this is an LOCC measurement on $\mathcal{H}$, which achieves the exact same result as does protocol $\mathcal{L}$. Indeed, in a matrix representation, we can write $\Pi = \mathrm{diag}(I_\mathcal{H}, 0_{\mathcal{H}^\perp})$ and

$$K_j \Pi = (\tilde{K}_j \; \tilde{0}), \tag{A2}$$

where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$, $\tilde{K}_j$ is an operator that acts only on $\mathcal{H}$, and $0_{\mathcal{H}^\perp}$ and $\tilde{0}$ are zero operators that act only on $\mathcal{H}^\perp$, which we define to be the orthogonal complement of $\mathcal{H}$ in $\mathcal{H}'$. Note that, whereas $0_{\mathcal{H}^\perp}$ is a square matrix, $\tilde{K}_j$ and $\tilde{0}$ need not be square; they may map to a space larger or smaller than that on which they act, but both map to the same output space, say $\mathcal{H}_{\mathrm{out}}$, which is also the output space for the operator on $\mathcal{H}'$ that we started with, K_j. Then the matrix $\tilde{K}_j$ represents an operator that acts on $\mathcal{H}$ (and whose output is $\mathcal{H}_{\mathrm{out}}$), and the collection of these operators constitutes a measurement $\{\tilde{K}_j\}$ acting only on $\mathcal{H}$, which is effectively identical to the measurement $\{K_j\}$ when the latter acts only on inputs that are confined to $\mathcal{H}$. That is, measurement $\{\tilde{K}_j\}$, which is a measurement that acts only on $\mathcal{H}$, achieves exactly what is achieved when $\{K_j\}$ acts on inputs that are confined to $\mathcal{H}$. This completes the proof. ■

[1] S. M. Cohen, Phys. Rev. A **90**, 012336 (2014).

[2] Many thanks go to an anonymous referee who voiced this criticism and provided the impetus for the present work.

[3] I. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[4] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[5] A. Peres, Phys. Lett. A **128**, 19 (1988).

[6] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).

[7] L. Roa, C. Hermann-Avigliano, R. Salazar, and A. B. Klimov, Phys. Rev. A **84**, 014302 (2011).

[8] J. A. Bergou, U. Futschik, and E. Feldman, Phys. Rev. Lett. **108**, 250502 (2012).

[9] E. Chitambar, R. Duan, and M.-H. Hsieh, IEEE Trans. Inf. Theory **60**, 1549 (2014).

[10] G. Waldherr, A. C. Dada, P. Neumann, F. Jelezko, E. Andersson, and J. Wrachtrup, Phys. Rev. Lett. **109**, 180501 (2012).

[11] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[12] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[13] Y. C. Eldar, IEEE Trans. Inf. Theory **49**, 446 (2003).

[14] A. Chefles, Phys. Rev. A **69**, 050307 (2004).

[15] E. M. Rains, Phys. Rev. A **60**, 173 (1999).

[16] 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).

[17] M. Koashi, F. Takenaga, T. Yamamoto, and N. Imoto, arXiv:0709.3196.

[18] R. J. Evans and I. M. Isaacs, Proc. Am. Math. Soc. **58**, 51 (1976).

[19] P. Erdös and A. M. Odlyzko, J. Number Theory **11**, 257 (1979).