Extended necessary condition for local operations and classical communication: Tight bound for all measurements

Scott M. Cohen

Phys. Rev. A **91**, 062125 — Published 24 June 2015

DOI: 10.1103/PhysRevA.91.062125

Extended necessary condition for local operations and classical communication: Tight bound for all measurements

Scott M. Cohen*

Department of Physics, Portland State University, Portland OR 97201

(Dated: April 29, 2015)

We give a necessary condition that a separable measurement can be implemented by local quantum operations and classical communication (LOCC) in any finite number of rounds of communication, generalizing and strengthening a result obtained previously. That earlier result involved a bound that is tight when the number of measurement operators defining the measurement is relatively small. The present results generalize that bound to one that is tight for any finite number of measurement operators, and we also provide an extension which holds when that number is infinite. We apply these results to the famous example on a 3×3 system known as "domino states", which were the first demonstration of nonlocality without entanglement. Our new necessary condition provides an additional way of showing that these states cannot be perfectly distinguished by (finite-round) LOCC. It directly shows that this conclusion also holds for their cousins, the rotated domino states. We also introduce a class of problems involving the unambiguous discrimination of quantum states, each of which is an example where the states can be optimally discriminated by a separable measurement, but according to our new condition, cannot be optimally discriminated by LOCC. These examples nicely illustrate the usefulness of the present results, since our earlier necessary condition, which the present result generalizes, is not strong enough to reach a conclusion in any of these cases.

PACS numbers: 03.65.Ta, 03.67.Ac

* cohensm52@gmail.com

I. INTRODUCTION

In a recent publication [1], we proved a necessary condition such that a quantum measurement can be implemented by local operations on subsystems and classical communication between parties (LOCC) in any finite number of rounds of communication.[1] We also demonstrated that there exist examples of separable measurements for which the condition is extensively violated, this violation growing without limit as the number of parties increases. A class of the examples given in [1] was later shown [2] to be applicable to the optimal unambiguous discrimination of certain sets of quantum states, and includes an infinite number of cases for each number of parties where each case is such that separable measurements are strictly better than finite-round LOCC. We also discussed in [1] why we believe that these results apply to all LOCC, including those using an infinite number of rounds, but to date a proof remains elusive.

Each quantum measurement involves a set of operators K_j where, for the jth outcome of the measurement, the state of the measured system changes as $\rho \to K_j \rho K_j^\dagger / p_j$, with $p_j = \mathrm{Tr}(\rho \mathcal{K}_j)$, where the associated 'POVM element' is defined as $\mathcal{K}_j := K_j^\dagger K_j$. A measurement on P parties is separable [3] if and only if each K_j is a product operator, in which case the POVM elements are also product, $\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \ldots \otimes \mathcal{K}_j^{(P)}$. It is well-known that every LOCC measurement is separable, but there exist separable measurements that are not LOCC [4–7]. In an effort to better understand the difference between separable measurements and LOCC [8–15], we have undertaken a series of works [1, 2, 16, 17] aimed at finding conditions on the sets of POVM elements that could serve to distinguish between these two important classes of quantum measurements.

In [16], we showed how to construct an LOCC protocol for a given bipartite separable measurement whenever such a protocol exists in a finite number of rounds. This result was generalized to any number of parties in [17]. The approach in these papers involves looking for intersections of convex cones generated by subsets of the local operators $\mathcal{K}_j^{(\alpha)}$ associated with the measurement under consideration, and the starting point is to consider subsets that each consist of a single operator. Each operator $\mathcal{K}_j^{(\alpha)}$ generates a ray $\{\lambda \mathcal{K}_j^{(\alpha)} | \lambda \geq 0\}$, any collection of these rays generates a convex cone, and the extreme rays of these cones are those associated with operators in that collection which cannot be written as a positive linear combination of the others in the same collection. Clearly, if for each party α, every $\mathcal{K}_j^{(\alpha)}$ is extreme in the cone of the full set of these operators for a given measurement and no two $\mathcal{K}_j^{(\alpha)}$ are proportional, then the starting point mentioned above will fail, as no two cones involving just a single operator will intersect. More generally, it appeared that (loosely speaking) too many extreme rays would make it difficult to find enough intersections to build a full LOCC protocol for the measurement. Motivated by this idea, we proved the following theorem in [1].

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

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

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. The upper bound in (1) can be achieved with equality when $N \leq 2^P$.

The last line in this theorem, that the upper bound in (1) is tight for $N \leq 2^P$, is rather restrictive. In general, N will be larger, in many cases significantly so. For example, any measurement aimed at discriminating a full basis of states will consist of $N = d_1 d_2 \ldots d_P$ operators (d_α is the dimension of the Hilbert space $\mathcal{H}_\alpha$ for subsystem α), which exceeds 2^P unless all subsystems are qubits, the smallest nontrivial system. Therefore, it would be of interest to have an upper bound that is tight for $N > 2^P$, as well. At the time of writing of [1], we had been able to prove that for bipartite systems, $\sum_\alpha e_\alpha \leq 3N/2$, which is a tight bound whenever $N \geq 2^P = 4$. We had suspected that an upper bound of $2N(1 - 2^{-P})$ might be valid

[1] We define each round of communication as consisting of one party broadcasting the result of her measurement to all the other parties.

for all P, but our method of proof for bipartite systems could not be generalized to more than two parties and at the time, we saw no way of approaching it differently. Recently, we realized that the techniques of [1] could be used to prove this conjectured upper bound, which is tight for $N \geq 2^P$ and any P. We present the results of this approach in Theorems 2, 3, and 4, below, where the latter two theorems apply to the case of infinite N.

Theorem 2 is quite similar in form to Theorem 1, which may give the impression that the former represents only a very small improvement over the latter. This is misleading, however, as the newer theorem is able to prove LOCC impossibility for a much wider range of problems since, as just observed, $N \leq 2^P$ is a quite restrictive condition. In Sec. III, we give examples of separable measurements for which Theorem 1 is too weak a condition and does not allow one to reach a conclusion, but where Theorem 2 directly demonstrates that these measurements cannot be implemented by finite-round LOCC. We do this in the context of (i) a well-known problem commonly referred to as the domino states [4], along with its generalization, the rotated domino states [12]; and (ii) a continuous class of problems involving the optimal unambiguous discrimination of states on two qubits.

In unambiguous state discrimination, a quantum system is prepared in one of a set of possible non-orthogonal states, and the aim is to measure the system in a way that identifies the chosen state without ever making an error. Since the states are not mutually orthogonal, this cannot be achieved with unit probability, so there must be an outcome of the measurement that leads to an inconclusive result; that is, for this outcome, the state of the system remains unknown, but for all other outcomes, the state can be identified with certainty. The study of unambiguous state discrimination was pioneered by Ivanovic [18], Dieks [19], and Peres [20], with important further results obtained in [21], where it was shown that the set of states must be linearly independent. This study was extended to the case of LOCC in [22], and further results for LOCC in this context were obtained in [23–25]. The study of optimal unambiguous state discrimination, where the probability of obtaining an inconclusive result is minimized, received attention in [26–28]. In [26], it was shown that LOCC is as good as global measurements for discriminating any set of two states that are given with equal *a priori* probability, and this was generalized [27] to the case of any *a priori* probabilities, again with only two states. A two-qubit example involving a specific, symmetric set of states given with equal *a priori* probabilities and for which LOCC is as good as general separable measurements but weaker than global measurements, was given in [28]. The examples we introduce here go beyond these earlier results in that they each involve a set of four (non-symmetric) states on two qubits, where the *a priori* probabilities for each example can vary over a continuous range, and for which we can use Theorem 2 to demonstrate that the best separable measurement is better than the best LOCC protocol, while Theorem 1 does not lead to a conclusion for any of these examples. We have elsewhere [2] given a different class of unambiguous state discrimination problems for each of which the best separable measurement is also better than LOCC, but this is shown by a violation of Theorem 1, so that our present generalization to Theorem 2 is not needed for those cases.

In the following section, we state and prove the finite-N result, Theorem 2. Its infinite-N counterparts, Theorems 3 and 4, are also stated in this section, and their proof is given in Appendix A. In Section III, we present physically motivated tasks for which Theorem 2, but not Theorem 1, can be used to demonstrate directly that these tasks cannot be accomplished by finite-round LOCC. Finally, in Section IV, we offer our conclusions. As with Theorem 1, we also conjecture that these theorems need not be restricted to finite-round LOCC, but rather apply to infinite-round LOCC, as well.

II. MAIN RESULTS

Our starting point in obtaining Theorem 2 is to represent any given LOCC measurement by a canonical LOCC tree, as defined in [1], a representation which is possible for any measurement implemented by LOCC. In these trees, each node is labeled by the POVM element corresponding to the cumulative action, to that point in the protocol, of the party for whom that node represents one outcome of a measurement by that party. If that party who measured is α, we refer to that node as an α-node. A canonical LOCC tree is then one where every nonleaf node has exactly two child nodes, and for any given node, the pair of POVM elements labeling its two child nodes are not proportional to each other.[2] Given this structure, these are full

[2] A brief reminder about terminology: A tree is a collection of nodes, each node has one parent node except the root, which has no parent, and every node has some number of children. Siblings are the set of nodes that are children of the same parent.

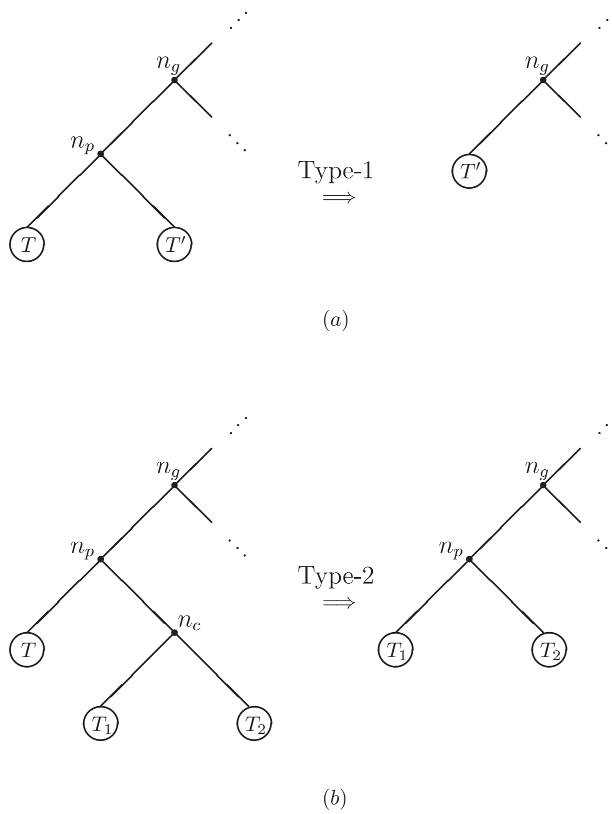

FIG. 1. Illustration of the two types of removals used in pruning a canonical LOCC tree. (a) A type-1 removal, where the parent n_p is removed along with the maximal keeperless subtree T. This type of removal is used when there is at least one $\hat{\mathcal{K}}_j$ leaf in T whose corresponding keeper is not in T's sibling subtree, T'. The root of T' is n_c, which may be the only node in T', in which case it turns out that n_c is itself a keeper leaf. (b) A type-2 removal where n_c, which is the root of the sibling subtree of T, is removed with T. This type of removal is used when every leaf in T has its corresponding keeper leaf in either T_1 or T_2. Under these circumstances, n_c cannot be a leaf. Figure reproduced from Ref. [1]

binary trees, so if they have N leaf nodes, they will also have a total of $2N-1$ nodes in all [29].

In [1], we showed how any canonical LOCC tree can be pruned down to a full binary tree that has one and only one leaf for each distinct $\mathcal{K}_j$ in the corresponding separable measurement, but nonetheless still has at least one appearance of each of the $\mathcal{K}_j^{(\alpha)}$ that is an extreme ray, for every party α. In addition, the method of pruning the tree is such that descendants of a given node in the final tree were also descendants of that node in the original tree. We now briefly review this method of pruning. For each j, find the right-most $\mathcal{K}_j$ leaf and choose this as the keeper leaf for that j. Then, starting from the left-most non-keeper leaf in the full tree, determine the largest complete subtree containing that leaf and not containing a single keeper leaf. Remove this "maximal keeperless" subtree along with one other node. The latter node is chosen to ensure the remaining tree is still full binary, and such that there is still at least one instance of every extreme ray in the fully pruned tree. There are two types of removals, illustrated in Fig. 1 and determined by which additional node is removed with the maximal keeperless subtree. See Ref. [1] for additional details of the pruning procedure, along with an explanation of why the two types of removals must be chosen in this way.

For our present result, consider an arbitrary canonical LOCC protocol represented as a canonical LOCC tree. We want to count the number of extreme rays in this tree. The first step will be to prune the tree as

A leaf node terminates a branch and so has no children. A subtree consists of a node in the tree, which is the root of that subtree, along with all descendants of that root node, where a descendant of a given node is a node that can be reached by starting at the given node and repeatedly proceeding from parent to child. An ancestor is defined similarly, but in this case, one repeatedly proceeds in the opposite direction, from child to parent.

described in [1], after which we rearrange the remaining nodes as follows: If a node is an extreme ray and at least one of its children is not extreme, swap positions of these two nodes, which moves the extreme node closer to the leaves of the tree. If both children are non-extreme, just choose either one to swap with its parent. Continue this process until no extreme node has a child that is not extreme, which means that any descendant of an extreme node must itself be extreme.

The resulting tree remains full binary and every extreme node lies in a subtree within which every node is extreme. Using integer index s, denote each maximal such subtree as T_s. If for given s, T_s has l_s leaf nodes, then as it is still full binary, it also has $2l_s - 1$ nodes in total, each of which is extreme. Suppose there are $\mathcal{S}$ of these subtrees. Then the total number of extreme nodes in this tree is equal to the total number of nodes in the collection of these subtrees, which is

$$\sum_{s=1}^{\mathcal{S}}(2l_s - 1) = 2\sum_{s=1}^{\mathcal{S}} l_s - \mathcal{S} \leq 2N - \mathcal{S}, \tag{2}$$

where we have used the fact that the total number N of leaf nodes is at least $\sum_s l_s$ (this sum can be strictly less than N if there is one or more subtrees that have no extreme rays in them at all, since in this case the leaves in these subtrees are not counted in the sum). Even though no two leaves are the same $\mathcal{K}_j$, it is still possible that some extreme rays are repeated at different nodes in this tree.[3] However, since every extreme ray appears at least once in the tree, the number of extreme rays is no greater than the number of extreme nodes, which is itself no greater than the quantity $2N - \mathcal{S}$ on the right-hand side of (2). Therefore, we have that

$$\sum_{\alpha=1}^{P} e_\alpha \leq 2N - \mathcal{S}. \tag{3}$$

If we can find the smallest possible value of $\mathcal{S}$, this will give a good upper bound on the total number of distinct extreme rays. Recall from [1] that the root node of the original tree is always present in the pruned tree and is not extreme. It should be clear that this node is still the root of the entire pruned and rearranged, final tree, implying $\mathcal{S} \geq 2$. In fact $\mathcal{S} = 2$ is possible, occurring when the root is the only non-extreme node in the pruned tree, and then no re-arrangement is necessary. In this case, $\sum_\alpha e_\alpha \leq 2(N-1)$, and we recover Theorem 1.

It turns out, however, that $\mathcal{S} = 2$ is not always possible, depending on how many parties are involved in the protocol. We will presently show that the number of leaf nodes in any one of these subtrees cannot exceed 2^{P-1}. Now, $\mathcal{S}$ is minimized when each subtree has this maximum number of leaf nodes, which occurs for these full binary subtrees when every branch has the same maximum height (height is the number of edges between the root and the leaf). The height of these subtrees is limited by the fact that every node in each of them is extreme, along with the fact that extreme α-nodes have no α-node descendants. The latter point is true of the original tree, by Lemma 5 of [1], and as is pointed out there, this remains true for the pruned tree. It also applies to the final, rearranged tree, since our rearrangement, like the pruning, does not create new descendants of any extreme node, but rather only turns some of its descendants into non-descendants. Therefore, no branch in these subtrees can have more than one α-node, for each of the P parties α, which directly implies there are no more than P nodes along any branch within any one of these subtrees, whose height h must therefore satisfy $h \leq P - 1$. It is well-known for a binary tree with l leaves and height h that $l \leq 2^h$ [30], so we can conclude that the number of leaves in any one of these subtrees cannot exceed 2^{P-1}. Since there are a total of N leaves in the full collection of these subtrees, there must be at least $N/2^{P-1}$ subtrees in this collection. Hence,

$$\mathcal{S} \geq \left\lceil \frac{N}{2^{P-1}} \right\rceil, \tag{4}$$

where $\lceil x \rceil$ is the smallest integer not less than x, and from (3) we have

$$\sum_{\alpha=1}^{P} e_\alpha \leq 2N - \left\lceil \frac{N}{2^{P-1}} \right\rceil, \tag{5}$$

[3] For example, it may be that $\mathcal{K}_1^{(1)} = \mathcal{K}_2^{(1)}$ is a (single) extreme ray, and these operators appear as two different leaves, one being the unique $\mathcal{K}_1$ leaf, the other being the unique $\mathcal{K}_2$ leaf. In this case, both these leaf nodes represent the same extreme ray in the first party's set of rays, and the number of extreme nodes in the tree is strictly greater than the number of extreme rays.

Combining this with Theorem 1, we have

Theorem 2. *For any finite-round LOCC protocol of P parties implementing a separable measurement corresponding to the N distinct POVM elements $\{\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \ldots \otimes \mathcal{K}_j^{(P)}\}_{j=1}^N$, it must be that*

$$\sum_{\alpha=1}^{P} e_\alpha \leq 2N - \lceil 2N\delta \rceil , \tag{6}$$

where $\delta = \max\left(N^{-1}, 2^{-P}\right)$, 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. The upper bound in (6) *can be achieved with equality for any finite N and P.*

We showed in [1] how the upper bound can be achieved when $N \leq 2^P$. The discussion above indicates how it can be done for all finite N. First consider the special case that $N = 2^{P-1}n$ with integer $n \geq 3$. One party measures first with n distinct outcomes. For each of her outcomes, each of the other $P-1$ parties measures once with a two-outcome measurement along every branch, conditioning their measurements on the previous parties' outcomes. As a result, descended from each of the n outcomes of that initial measurement, there is a full binary subtree having 2^{P-1} leaf nodes and $2^P - 1$ nodes. This gives a total of $N = 2^{P-1}n$ leaves in the entire tree, which also has a total of $\left(2^P - 1\right) n = 2N(1-\delta)$ nodes, not counting the root of the tree. The parties can choose their measurements so that all of their local outcomes are distinct from each other, and so that each such outcome is extreme in the cone of its collection of local outcomes. Then every node in the tree is extreme apart from the root of the tree, and the bound is achieved with equality.

If the last measurement along a single branch of the preceding protocol is omitted, this removes two leaf nodes, but the node that was the parent of those two removed leaves becomes a new leaf, so N is decreased by one to $N = 2^{P-1}n - 1$. At the same time, the total number of nodes is decreased by two, as is the total number of extreme rays. Now, $\lceil 2N\delta \rceil = \left\lceil 2N/2^P \right\rceil$ doesn't change when N decreases by one, so the upper bound in (6) also decreases by two, and is again achieved with equality. This process can be continued sequentially, at each step omitting a single measurement in the same chosen subtree. The quantity $\lceil 2N\delta \rceil$ remains unchanged as N decreases by one and the number of extreme rays decreases by two, with the upper bound always being achieved with equality, until there is only one node left in that subtree. When that subtree's last node is removed, N has decreased by 2^{P-1} in all, which is the point at which $\lceil 2N\delta \rceil$ decreases by one. This last removal decreases N by one, the number of extreme rays also by one, and the upper bound by one, so the upper bound is again achieved with equality. At this point we are effectively back where we started but with one less outcome in the first party's initial measurement, so start again omitting measurements in another subtree. By continuing this process even into the last remaining subtree, we see that the bound is tight for any finite N.

Let us now turn to the case of a separable measurement having an infinite number of distinct POVM elements. Begin by choosing an ordering of these POVM elements. Let $e_{\alpha N}$ be the number of distinct extreme rays for party α in the first N of those POVM elements. Define the density of extreme rays as

$$\mathcal{D}_e = \lim_{N\to\infty} \frac{1}{N} \sum_{\alpha=1}^{P} e_{\alpha N}, \tag{7}$$

and we only include in the sum on the right, those parties for which at least one of its local operators is not proportional to the identity. This quantity, $\mathcal{D}_e$, depends on the ordering chosen. Then we have the following theorem.

Theorem 3. *For any finite-round LOCC protocol of P parties implementing a separable measurement corresponding to an infinite number of distinct POVM elements $\{\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \ldots \otimes \mathcal{K}_j^{(P)}\}$, there exists an ordering of those POVM elements such that*

$$\mathcal{D}_e \leq 2(1 - 2^{-P}). \tag{8}$$

There exist separable measurements with an infinite number of distinct POVM elements for which the upper bound in (8) *can be achieved with equality.*

The proof is given in Appendix A. The idea is that the LOCC protocol that implements the measurement induces an ordering for which $\mathcal{D}_e$ satisfies the bound. One first prunes and rearranges the tree in a way similar to what was done for finite N, and then the leaves of the resulting tree can be enumerated. This enumeration provides the desired ordering. Actually, there is a great deal of freedom in choosing this enumeration, so our proof actually demonstrates that there are an infinite number of orderings for which (8) is satisfied, and we can strengthen Theorem 3 to some degree as follows.

Theorem 4. *Consider any finite-round LOCC protocol of P parties implementing a separable measurement corresponding to an infinite number of distinct POVM elements $\{\mathcal{K}_j = \mathcal{K}_j^{(1)} \otimes \ldots \otimes \mathcal{K}_j^{(P)}\}$. Then, for any finite integer M, and for any choice and ordering of the first M of these POVM elements, there exists an ordering of the remaining POVM elements such that $\mathcal{D}_e \leq 2(1-2^{-P})$.*

The proof of this result is included in Appendix A.

One can show that the bound in (8) is tight by the following discussion, which closely mirrors that given above on how to achieve the upper bound with equality in the case of finite N. The first party makes an initial measurement with an infinite number of outcomes, each of which is followed by a sequence of $P-1$ (one for each of the other parties) two-outcome measurements along every branch. This means each outcome of that initial measurement has descended from it 2^{P-1} leaf nodes and a total of 2^P-1 nodes in its descendant subtree. Choose these measurements such that all nodes are extreme rays and distinct from each other—this is not difficult to do—and then order the POVM elements in the overall separable measurement by following a right-to-left enumeration of the leaves of this LOCC tree. Considering the subtrees descendant from the rightmost $\mathcal{S}$ outcomes of the initial measurement, one has $N = 2^{P-1}\mathcal{S}$ leaf nodes and $(2^P-1)\mathcal{S}$ extreme rays for all P parties. As $\mathcal{S} \to \infty$, also $N \to \infty$, and we see that $\mathcal{D}_e$ of (7) is equal to $(2^P-1)/2^{P-1} = 2(1-2^{-P})$ for this P-round LOCC protocol, saturating the upper bound in (8).

III. APPLICATION TO RANK-1 MEASUREMENTS

For finite-N measurements in which every operator is rank-1, it is a simple process to apply Theorem 2 to determine if these measurements are candidates for LOCC. Each rank-1 product operator is a product of rank-1 local operators, and rank-1 operators, being extreme rays in the full set of positive semidefinite operators, are necessarily extreme in any subset of that full set. Therefore, one need only count the number of distinct local operators in these measurements, and then violation of the bound in Theorem 2 automatically rules out any possibility of implementation by finite-round LOCC.

Rank-1 measurements arise in the context of quantum state discrimination of a full basis of any multipartite Hilbert space. When the basis is mutually orthogonal, the only[4] measurement that can perfectly discriminate the set of states consists of rank-1 projectors onto the states of that basis. When the basis is non-orthogonal, it may still be the case that an *optimal* measurement consists of rank-1 operators. Clearly, these measurement operators must be product for there to be any hope of accomplishing this task by LOCC, and if they are product, Theorem 2 further restricts what may be possible. Examples illustrating the usefulness of Theorem 2 are given in the following two subsections.

A. Domino states

A well-known example of perfect discrimination of a full product basis where our results can be profitably applied is that of Bennett, et. al., which was the first demonstration of the existence of separable measurements that are not LOCC [4]. This set of nine states on a 3×3 system, often referred to as domino states, is (omitting normalization factors)

$$\begin{array}{lll} |\Psi_1\rangle = |1\rangle|1\rangle & |\Psi_2\rangle = |0\rangle(|0\rangle+|1\rangle) & |\Psi_3\rangle = |0\rangle(|0\rangle-|1\rangle) \\ |\Psi_4\rangle = |2\rangle(|1\rangle+|2\rangle) & |\Psi_5\rangle = |2\rangle(|1\rangle-|2\rangle) & |\Psi_6\rangle = (|1\rangle+|2\rangle)|0\rangle \\ |\Psi_7\rangle = (|1\rangle-|2\rangle)|0\rangle & |\Psi_8\rangle = (|0\rangle+|1\rangle)|2\rangle & |\Psi_9\rangle = (|0\rangle-|1\rangle)|2\rangle. \end{array} \qquad (9)$$

[4] We restrict to measurements acting only on the original Hilbert space. While enlarging the Hilbert space creates the possibility of using other measurements, these other measurements are effectively identical to the "only" measurement discussed here; see Lemma 5 of [2]. Therefore, enlarging the Hilbert space does not allow accomplishment by LOCC of a task that is impossible by LOCC acting only on the original Hilbert space.

There are seven distinct local states for each of the $P = 2$ parties, so the $N = 9$ separable measurement that perfectly discriminates these states involves seven distinct rank-1 local projectors on each side. This means that whereas $e_1 = 7 = e_2$ and $e_1+e_2 = 14$, the upper bound on this sum in Theorem 2 is $2N - \lceil N/2^{P-1} \rceil = 13$. Hence, this measurement violates Theorem 2, implying directly (the well-known result) that this set of states cannot be perfectly discriminated by finite-round LOCC. The same conclusion immediately follows for any set of "rotated domino states" [12], for which an arbitrary rotation is applied to each pair of superposition states (such as $|0\rangle + |1\rangle \to \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$, $|0\rangle - |1\rangle \to \sin(\theta)|0\rangle - \cos(\theta)|1\rangle$). Note that for the result we had obtained previously in [1], in which $\delta = N^{-1}$ instead of the value $\delta = 2^{-P} > N^{-1}$ used here, we have a bound of $2(N-1) = 16$, which does not allow a conclusion to be drawn for these states (rotated or not). Therefore, these examples demonstrate the usefulness of the extension obtained in the present paper.

B. Unambiguous state discrimination on two qubits

Here, we provide a class of unambiguous state discrimination problems that can be optimally solved by a unique[4] separable measurement that cannot be implemented by finite-round LOCC, this latter conclusion requiring our generalization to Theorem 2, because the conditions of Theorem 1 do not allow for a conclusion to be reached. For unambiguous state discrimination of a set of states $\{|\Phi_j\rangle\}_{j=1}^N$, we require a positive operator-valued measure, or POVM, whose first N elements Π_k satisfy

$$\langle \Phi_j|\Pi_k|\Phi_j\rangle = p_j \delta_{jk}, \tag{10}$$

and one last element

$$\Pi_{N+1} = I - \sum_{k=1}^{N} \Pi_k \geq 0, \tag{11}$$

which represents the inconclusive outcome of the measurement. Consider the following set of four linearly independent states on two qubits, $\mathcal{S} = \{\eta_j, |\Phi_j\rangle\}$, each given with *a priori* probability η_j,

$$\begin{aligned}
|\Phi_1\rangle &= \frac{1}{\sqrt{|\beta_3|^2 + |\alpha_3\beta_1|^2}} \left(\beta_3^*\beta_1^*|00\rangle + \beta_3^*\alpha_1^*|01\rangle - \alpha_3^*\beta_1^*|10\rangle\right), \\
|\Phi_2\rangle &= \frac{1}{\sqrt{|\beta_3|^2 + |\alpha_3\beta_1|^2}} \left(\beta_3^*\beta_1^*|00\rangle - \beta_3^*\alpha_1^*|01\rangle - \alpha_3^*\beta_1^*|10\rangle\right), \\
|\Phi_3\rangle &= |10\rangle, \\
|\Phi_4\rangle &= |11\rangle,
\end{aligned} \tag{12}$$

where for $j = 1, 3$ we require that $\alpha_j \neq 0$, $\beta_j \neq 0$, and $|\alpha_j|^2 + |\beta_j|^2 = 1$, and we also require that $|\alpha_1| \leq |\beta_1|$ and $\eta_1 = \eta_2$. Finally, we apply one additional restriction to these coefficients, which as shown in Appendix B, will ensure there is a unique measurement that is optimal for unambiguously discriminating these states. This final restriction is,

$$\left(1 - \left|\frac{\alpha_1\beta_3}{\beta_1}\right|^2\right)^2 \geq \frac{\eta_3}{4\eta_1}\left|\frac{\alpha_3}{\beta_1}\right|^2 \left(|\beta_3|^2 + |\alpha_3\beta_1|^2\right). \tag{13}$$

We note that these restrictions leave a wide range of allowed values for the coefficients.

Since the states of (12) form a basis of the full Hilbert space, the only operators satisfying (10) are those proportional to a projector onto one of the reciprocal set of states, $\{|\Psi_k\rangle\}$, which are uniquely determined by the condition

$$\langle \Psi_k|\Phi_j\rangle = \delta_{jk}. \tag{14}$$

For the states of (12), the (generally non-normalized) reciprocal set consists of

$$
\begin{aligned}
|\Psi_1\rangle &= q|0\rangle\left(\alpha_1|0\rangle + \beta_1|1\rangle\right),\\
|\Psi_2\rangle &= q|0\rangle\left(\alpha_1|0\rangle - \beta_1|1\rangle\right),\\
|\Psi_3\rangle &= \left(\frac{\alpha_3}{\beta_3}|0\rangle + |1\rangle\right)|0\rangle,\\
|\Psi_4\rangle &= |11\rangle,
\end{aligned}
\tag{15}
$$

where $q = \sqrt{|\beta_3|^2 + |\alpha_3\beta_1|^2}\Big/ (2\alpha_1^*\beta_1^*\beta_3^*)$. Therefore, the first four POVM elements in any measurement that succeeds in unambiguously discriminating $\mathcal{S}$ must be proportional to a projector onto one of these states. That is, our measurement consists of operators

$$
\begin{aligned}
\Pi_k &= p_k\left[\Psi_k\right],\ k = 1,\ldots,4\\
\Pi_5 &= I - \sum_{k=1}^{4} p_k\left[\Psi_k\right],
\end{aligned}
\tag{16}
$$

and we have defined $[\psi] = |\psi\rangle\langle\psi|$. Optimization of our measurement consists of minimizing the probability of obtaining an inconclusive result, where this probability is given by

$$
p_5 = \sum_{j=1}^{4}\eta_j\langle\Phi_j|\Pi_5|\Phi_j\rangle = 1 - \sum_{j=1}^{4}\eta_j p_j,
\tag{17}
$$

and we have used (14) to obtain the final expression in the preceding equation. Thus, we wish to maximize $\sum_j \eta_j p_j$ subject to the constraint that $\Pi_5 \geq 0$.

From (15) and the second line of (16), we can write Π_5 in the computational basis as

$$
\Pi_5 = \begin{pmatrix}
1 - |q\alpha_1|^2(p_1+p_2) - |\alpha_3/\beta_3|^2 p_3 & -|q|^2\alpha_1\beta_1^*(p_1-p_2) & -p_3\alpha_3/\beta_3 & 0\\
-|q|^2\alpha_1^*\beta_1(p_1-p_2) & 1 - |q\beta_1|^2(p_1+p_2) & 0 & 0\\
-p_3\alpha_3^*/\beta_3^* & 0 & 1-p_3 & 0\\
0 & 0 & 0 & 1-p_4
\end{pmatrix}.
\tag{18}
$$

Now, $\Pi_5 \geq 0$ if and only if every one of its principal minors is non-negative. To begin with, it is clear that $p_4 \leq 1$ and $p_1 + p_2 \leq 1/|q\beta_1|^2$. Since all principal minors are either independent of p_4 or proportional to $1-p_4$, we see (unsurprisingly, since $|\Phi_4\rangle$ is orthogonal to all other $|\Phi_j\rangle$) that $p_4 = 1$ is always achievable, no matter what values are taken by the other p_j.

Let us first consider what happens when $p_1+p_2 = 1/|q\beta_1|^2$. Then, the $(1,2)$ principal minor (that involving the first and second rows and columns) is negative unless $p_1 = p_2 = 1/2|q\beta_1|^2$, which must therefore hold. From the $(1,3)$ principal minor, we then have that

$$
\begin{aligned}
p_3 &\leq \frac{|\beta_3|^2\left[1 - |q\alpha_1|^2(p_1+p_2)\right]}{1 - |q\alpha_1\beta_3|^2(p_1+p_2)}\\
&= \frac{|\beta_3|^2\left(1 - |\alpha_1/\beta_1|^2\right)}{1 - |\alpha_1\beta_3/\beta_1|^2} \equiv \hat{p}_3.
\end{aligned}
\tag{19}
$$

Note that since $|\beta_3| < 1$, the upper bound in this expression is strictly less than unity, and one can readily check that Π_5 is positive semidefinite when p_3 saturates this bound. When this is the case, we have that

$$
p_5 = 1 - \frac{\eta_1}{|q\beta_1|^2} - \frac{\eta_3|\beta_3|^2\left(1 - |\alpha_1/\beta_1|^2\right)}{1 - |\alpha_1\beta_3/\beta_1|^2} - \eta_4.
\tag{20}
$$

In fact, it turns out that for these choices of the p_j, $\Pi_5 = [\pi_5]\otimes[0]$ is a rank-1 product operator, where

$$
|\pi_5\rangle = \mu|0\rangle + \nu|1\rangle,
\tag{21}
$$

with

$$\mu = e^{i\theta}\sqrt{1-|\alpha_1/\beta_1|^2-|\alpha_3/\beta_3|^2\,\hat{p}_3},$$
$$\nu = e^{i\phi}\sqrt{1-\hat{p}_3}. \tag{22}$$

Up to an unimportant overall phase, we may choose $\theta = 0$, and then $-\phi$ must be the same as the phase of α_3/β_3, yielding a unique POVM for these choices of the p_j. We can show, see Appendix B, that the value of p_5 cannot be less than that given in (20), and that this value of p_5 requires that $p_1+p_2 = 1/|q\beta_1|^2$. Therefore, the foregoing choices of the p_j yield the unique, optimal measurement for unambiguous discrimination of the states in (12), which is a manifestly separable measurement, as all POVM elements are product operators. Hence, separable measurements are as good as global ones for this task. On the other hand, we can use Theorem 2 to immediately see that this separable measurement cannot be implemented by finite-round LOCC. Since each of the Π_j is a rank-1 product operator, each is a tensor product of two operators that are themselves each an extreme ray in the full convex cone of positive operators for their respective spaces. Therefore, we can simply count the number of distinct such operators to obtain the desired number of extreme rays, e_1 and e_2. For the first party, we have operators $[0]$, $[\pi_3]$, $[1]$, and $[\pi_5]$, where $|\pi_3\rangle = \alpha_3|0\rangle + \beta_3|1\rangle$, so $e_1 = 4$. Similarly for the second party, we have operators $[\pi_1]$, $[\pi_2]$, $[0]$, and $[1]$, with $|\pi_1\rangle = \alpha_1|0\rangle+\beta_1|1\rangle$ and $|\pi_2\rangle = \alpha_1|0\rangle - \beta_1|1\rangle$, so $e_2 = 4$, as well. The measurement consists of $N = 5$ distinct operators, so we have a violation of the conditions of Theorem 2 with $8 = e_1 + e_2 > 3N/2 = 7.5$. On the other hand, $2(N-1) = 8$, so the conditions of Theorem 1 are not violated. Hence, while Theorem 1 is not strong enough to allow a conclusion to be drawn about the LOCC implementation of this measurement, Theorem 2 tells us that it is indeed impossible by finite-round LOCC. As the α_j, β_j are constrained only by the conditions given below (12), we thus have a continuous class of optimal unambiguous state discrimination problems each achievable by a separable measurement, but for which Theorem 2 tells us directly that this is impossible by finite-round LOCC. Since Theorem 1 is too weak to allow a conclusion to be drawn, these examples demonstrate the importance of the extension to Theorem 2. Note also that this class includes a wide range of possible *a priori* probabilities for each set of the other coefficients defining the set $\mathcal{S}$.

IV. CONCLUSIONS

In summary, we have proved a necessary condition for any finite-round LOCC protocol, which provides an upper bound on the number of extreme rays appearing in the collection of POVM elements associated with a separable measurement, see Theorem 2 and the accompanying discussion. We have shown that the upper bound in Theorem 2 is tight for all measurements having a finite number of distinct POVM elements by providing examples of measurements for which the upper bound is achieved with equality. This has been further extended in Theorems 3 and 4 to cover cases of measurements with an infinite number of distinct POVM elements, and the bound in this case can also be achieved with equality. These results extend a previous result obtained in [1], restated here as Theorem 1, but the corresponding upper bound in that theorem is tight only when there are relatively few distinct POVM elements.

In Section III, we have shown that the well-known separable measurement of [4] violates the necessary condition of Theorem 2, providing one more way of showing that this measurement cannot be implemented by finite-round LOCC. We also introduced a new class of unambiguous state discrimination problems, each of which can be optimally discriminated by a separable measurement, but for which Theorem 2 implies they cannot be optimally discriminated by finite-round LOCC. In all these cases, the corresponding separable measurement does not violate the condition of Theorem 1, demonstrating the importance of the extension obtained in Theorem 2.

We have conjectured elsewhere that Theorem 1 also applies to infinite-round LOCC protocols, and we continue to believe this conjecture holds. Similarly, we also believe that Theorem 2 holds for infinite-round protocols, but we have yet to find a proof. We feel less confident this will also be the case for Theorems 3 and 4, though it is certainly a possibility. If these conjectures turn out to be true, we will have found yet another way of proving that there is a finite gap between what can be achieved by the separable measurement which successfully distinguishes the nine states of [4], as opposed to what can be achieved by LOCC. We will also then have shown a similar finite gap for each example in the class of optimal unambiguous discrimination problems introduced in Sec. III.

Acknowledgments — We would like to thank Li Yu and Dan Stahlke for very helpful discussions. This work has been supported in part by the National Science Foundation through Grant No. 1205931.

Appendix A: Proof of Theorems 3 and 4

Our proof of Theorems 3 and 4 will be very similar to that of Theorem 2, except that we will not start with a canonical LOCC tree, since such a tree, being full binary, would require the infinite-leaf tree to have infinite height, whereas we wish to work with trees of finite height. According to Lemmas 2 and 4 of [17], we may nonetheless assume that our LOCC tree is such that every nonleaf node has at least two children and that, of the POVM elements labeling its children, no two are proportional to each other.

Although the following lemma applies only to trees with a finite number of leaf nodes, it will play an important role in our arguments.

Lemma 5. *For any tree of height h in which every nonleaf node has at least two children, the ratio of the total number of nodes n to the number of leaf nodes l in the tree satisfies*

$$\frac{n}{l} \leq 2\left(1-2^{-(h+1)}\right), \tag{A1}$$

as long as l, and hence n, is finite.

Proof. The proof is by induction on the height h. For $h=1$, the tree has a root node and $l \geq 2$ leaf nodes, for a total of $n = l+1$ nodes in all. Then, $n/l = 1+1/l \leq 3/2 = 2\left(1-2^{-(h+1)}\right)$. Now assume (A1) holds for $h = H-1$, and let us show that it then holds for $h = H$. Let T_H be a tree of height H obtained from T_{H-1} by adding children to some of the leaf nodes of T_{H-1}. Those leaf nodes to which we do not add children are terminal at $H-1$, let there be t_{H-1} of these terminal leaves. If we add the number of leaf nodes from T_H to the total number of nodes in T_{H-1}, we overcount the total number of nodes in T_H because those terminal leaves have been counted twice. Therefore, the total number of nodes in T_H is $n_H = n_{H-1} + l_H - t_{H-1}$. In addition, since we consider only trees for which each nonleaf node has at least two children, we have $l_H \geq 2\left(l_{H-1} - t_{H-1}\right) + t_{H-1} = 2l_{H-1} - t_{H-1}$. Hence, defining $x = t_{H-1}/l_{H-1}$, we have

$$\begin{aligned}\frac{n_H}{l_H} &= 1 + \frac{n_{H-1} - t_{H-1}}{l_H} \leq 1 + \frac{n_{H-1} - t_{H-1}}{2l_{H-1} - t_{H-1}} = 1 + \frac{n_{H-1}/l_{H-1} - x}{2-x} \\ &\leq 1 + \frac{2\left(1-2^{-H}\right) - x}{2-x} = 2 - \frac{2^{-(H-1)}}{2-x} \leq 2 - 2^{-H} = 2\left(1-2^{-(H+1)}\right),\end{aligned} \tag{A2}$$

where the first inequality on the second line is by the induction assumption, and this completes the proof.■

Proof of Theorem 3. Consider any finite-round LOCC tree implementing a separable measurement defined by the infinite set of POVM elements $\{\mathcal{K}_j\}$. This tree has an infinite number of leaf nodes, at least one for each $\mathcal{K}_j$. We prune this tree following the technique of [1], except that if at any stage of this process we are removing a subtree whose root has more than one sibling, then we simply remove that subtree without removing an additional nonleaf node (since in [1] the tree was full binary, the subtrees considered there always had one and only one sibling; it was then necessary to remove an extra nonleaf node in order to keep the tree full binary; see [1] for details). If that subtree has only one sibling, then remove it according to the rules used in [1]. The pruning is complete when there is one and only one leaf for each of the $\mathcal{K}_j$. According to this procedure, every nonleaf node in the resulting tree still has at least two children.

The next step is to rearrange the resulting tree in the same way we did for the finite-N case, exchanging an extreme node with one of its non-extreme children, if there is one, and continuing this process until no extreme node has a non-extreme descendant. The tree that remains has all its extreme nodes in subtrees within which every node is extreme, and just as in the finite-N case, these subtrees can have height no greater than $P-1$.

Choose any one of these subtrees and set $\mathcal{S}=1$. If this is a finite subtree we can include it in its entirety from the outset, so add another subtree to the collection and increment $\mathcal{S}$. If instead it is an infinite subtree, we will need to count its nodes using some kind of a limiting procedure. Hence for each infinite subtree, instead of starting with the entire subtree, add it in as a "skeleton" of itself, one which is a full binary tree. Any such skeleton will do, as long as every branch in it is also a branch in the original subtree. These skeletons may be obtained from their corresponding subtree by removing all but two children from every node that has more than two, while also removing the complete branches descended from those removed children. At each subsequent step, include another subtree in the collection and increment $\mathcal{S}$. At the same time, for each skeleton of an infinite subtree T_s, add a full binary branch to that skeleton, by which we mean a branch for which every nonleaf node has two children, where the added branch is either one that was in the original T_s, or a skeleton of one that was. Add these skeletal branches in the order indicated by index s, starting at the infinite subtree with smallest s and proceeding to the one with next smallest s, and so on. Continue this process of adding subtrees and branches indefinitely. In the limit of an infinite number of steps of this procedure, each T_s will be fully reconstructed and every subtree will be included in the collection. If all subtrees are finite, there will be an infinite number of subtrees to include, one at each step. Otherwise, there may be a finite or infinite number of subtrees to include, but reconstruction of the infinite subtrees will always require an infinite number of steps. In any case, at each step of this infinitely long process, we have a finite number $\mathcal{S}$ of subtrees, each having l_s leaf nodes and n_s nodes in total, with both l_s and n_s finite.

We need to identify a precise ordering of the $\mathcal{K}_j$. Such an ordering may be obtained directly from the procedure described above of including more and more subtrees, while at the same time reconstructing each infinite subtree in a step-by-step fashion. In fact, this procedure generates an infinite number of such orderings. The index s, which can be assigned arbitrarily, provides a kind of coarse-grained order for the $\mathcal{K}_j$, indicating when each finite subtree is added, when each infinite one is begun as a skeleton, and also the order in which each additional skeletal branch is added to those infinite subtrees previously begun. There still remains the task of ordering the set of $\mathcal{K}_j$ within each of these "coarse-grained" objects. Note that each of the $\mathcal{K}_j$ appears in one and only one of the subtrees (recall that the pruned tree has one and only one appearance of each $\mathcal{K}_j$), so this fine-grained ordering will be unambiguous. For each skeletal branch then, choose any ordering that has the $\mathcal{K}_j$ that appear within it ordered one right after another, which then ensures that there is no more than one branch at a time in the entire collection of (partially reconstructed) subtrees that is not full binary. This means that at each step of this procedure, every nonleaf node in the entire collection has at least two children, except those nodes in the branch that is presently being constructed.[5]

At any given point, let s_* denote the one subtree that has a branch that is not yet partially completed to full binary. Let δn be the number of nodes on the skeletal branch in this subtree that is presently being constructed and is not yet part of a full binary skeleton, and let δl be the corresponding number of leaves. Given that these branches have height no greater than $P-1$, then the number of leaf nodes in the skeletal branch that is not yet full binary must satisfy $\delta l \leq 2^{P-1}$. Define $n_C = n_{s_*} - \delta n$ and $l_C = l_{s_*} - \delta l$. Then since n_C, l_C count the nodes and leaves that lie in branches for which every nonleaf node has at least two children, we have from Lemma 5 that $n_C/l_C \leq 2\left(1-2^{P-1}\right)$. Now, each time one adds a leaf, one adds no more than P nodes, strictly fewer than this if that leaf is attaching to a subtree already begun. Therefore, $\delta n/\delta l \leq P$.

Define $N = \sum_s l_s$, which is the number of distinct $\mathcal{K}_j$ appearing in the collection of subtrees at this stage of the process. The total number of extreme rays appearing in this collection is no greater than the total number of nodes, $\sum_\alpha e_{\alpha N} \leq \sum_s n_s$. Then, for any ordering as described above, we have

$$
\begin{aligned}
\frac{1}{N}\sum_\alpha e_{\alpha N} &\leq \sum_{s=1}^{\mathcal{S}} n_s \Big/ \sum_{s=1}^{\mathcal{S}} l_s \\
&= \sum_{s\neq s_*}^{\mathcal{S}} l_s \left(\frac{n_s}{l_s}\right) \Big/ \sum_{s=1}^{\mathcal{S}} l_s + l_C \left(\frac{n_C}{l_C}\right) \Big/ \sum_{s=1}^{\mathcal{S}} l_s + \delta l \left(\frac{\delta n}{\delta l}\right) \Big/ \sum_{s=1}^{\mathcal{S}} l_s \\
&\leq 2\left(1-2^{-P}\right)\left(\sum_{s\neq s_*}^{\mathcal{S}} l_s + l_C\right) \Big/ \sum_{s=1}^{\mathcal{S}} l_s + P\delta l \Big/ \sum_{s=1}^{\mathcal{S}} l_s \\
&= 2\left(1-2^{-P}\right) + \left(P-2+2^{-(P-1)}\right)\delta l \Big/ \sum_{s=1}^{\mathcal{S}} l_s \\
&\leq 2\left(1-2^{-P}\right) + \left(P-2+2^{-(P-1)}\right)2^{P-1} \Big/ \sum_{s=1}^{\mathcal{S}} l_s .
\end{aligned}
\tag{A3}
$$

---

[5] To be more precise about this, for each new subtree, start with any one leaf that was at the end of a branch of height $h \leq P-1$, the same as that of the original subtree, adding this solitary leaf along with its $h-1$ ancestors, one of which is the root of that subtree. The next leaf is chosen as one whose branch attaches to that preceding branch (which will add no more than $h-1$ nodes to this subtree, including that leaf, since it must share at least one node with the preceding branch to which it attaches). Subsequent leaves are chosen to attach to this same skeleton in a way such that no node in it has more than two children, and this continues until every nonleaf node has two. Then, move on to the next subtree. If a subtree has already been started, then it has a full binary skeleton already present, so add any additional leaf to start the next skeleton. This leaf attaches to that full binary skeleton at a node that already had at least two children, so will now have more than two, but in general, this new leaf will have ancestors that have only one child node. Continue adding leaves to the skeleton consisting of that leaf and its ancestors until it is also full binary, and then move on to the next subtree, continuing this process indefinitely.

where the third line follows from Lemma 5, which tells us that $n_s/l_s \leq 2\left(1-2^{-P}\right)$ for all $s \neq s_*$ and that $n_C/l_C \leq 2\left(1-2^{-P}\right)$, along with the fact that $\delta n/\delta l \leq P$, as argued above. The last line follows from $\delta l \leq 2^{P-1}$, which was also argued above. Now as $\mathcal{S} \to \infty$, $N = \sum_{s=1}^{\mathcal{S}} l_s \to \infty$. Hence in this limit, we see that the second term in the last line approaches zero, and we recover $\mathcal{D}_e \leq 2\left(1-2^{-P}\right)$. This completes the proof of Theorem 3. ■

Proof of Theorem 4. Theorem 4 follows almost immediately from the proof of Theorem 3. For any ordering of the first M of the $\mathcal{K}_j$, fill in the subtrees constructed from those M leaves until they are full binary. Then, for the remaining leaves, continue precisely as described in the proof of Theorem 3. The result follows directly. ■

Appendix B: Proof of optimality for the measurement found at the end of Sec. III B

We wish to show that the probability p_5 given in (20) is optimal for unambiguous discrimination of the states in (12), and that the measurement found at the end of that section, having $p_1 = p_2 = 1/2\,|q\beta_1|^2$ and $p_3 = \hat{p}_3$ is the unique optimal measurement. To do this, let us consider all other measurements, for which we can write

$$\begin{aligned} p_1 &= \frac{1+\delta_1}{2\,|q\beta_1|^2}, \\ p_2 &= \frac{1+\delta_2}{2\,|q\beta_1|^2}, \end{aligned} \tag{B1}$$

and then Π_5 becomes

$$\Pi_5 = \begin{pmatrix} 1-|\alpha_1/\beta_1|^2\,[1+(\delta_1+\delta_2)/2] - |\alpha_3/\beta_3|^2 p_3 & -\alpha_1(\delta_1-\delta_2)/2\beta_1 & -p_3\alpha_3/\beta_3 & 0 \\ -\alpha_1^*(\delta_1-\delta_2)/2\beta_1^* & -(\delta_1+\delta_2)/2 & 0 & 0 \\ -p_3\alpha_3^*/\beta_3^* & 0 & 1-p_3 & 0 \\ 0 & 0 & 0 & 1-p_4 \end{pmatrix}. \tag{B2}$$

We first notice immediately that $\Pi_5 \geq 0$ implies that $\delta_1+\delta_2 \leq 0$, and if $\delta_1+\delta_2 = 0$, then it also implies that $\delta_1 = 0 = \delta_2$, in which case we are back to the measurement found in Sec. III B. We are trying to determine if there exists a measurement different from, but which performs at least as well as, the one of Sec. III B. Therefore, let us assume that $\delta_1+\delta_2 < 0$ and see if there exists p_3, δ_1, δ_2 such that this new measurement does at least as well as the previous one, which translates to the condition,

$$1 - \frac{\eta_1}{|q\beta_1|^2} - \frac{\eta_3|\beta_3|^2\left(1-|\alpha_1/\beta_1|^2\right)}{1-|\alpha_1\beta_3/\beta_1|^2} \geq 1 - \frac{\eta_1}{|q\beta_1|^2} - \frac{\eta_1\left(\delta_1+\delta_2\right)}{2\,|q\beta_1|^2} - \eta_3 p_3, \tag{B3}$$

or

$$p_3 \geq \frac{|\beta_3|^2\left(1-|\alpha_1/\beta_1|^2\right)}{1-|\alpha_1\beta_3/\beta_1|^2} - \frac{\eta_1\left(\delta_1+\delta_2\right)}{2\eta_3\,|q\beta_1|^2}. \tag{B4}$$

However, from the $(1,3)$ principal minor of (B2), we also have that

$$p_3 \leq \frac{|\beta_3|^2\left(1-|q\alpha_1|^2\,(p_1+p_2)\right]}{1-|q\alpha_1\beta_3|^2\,(p_1+p_2)} = \frac{|\beta_3|^2\left(1-|\alpha_1/\beta_1|^2\,[1+\left(\delta_1+\delta_2\right)/2]\right)}{1-|\alpha_1\beta_3/\beta_1|^2\,[1+\left(\delta_1+\delta_2\right)/2]}. \tag{B5}$$

We thus have that the right-hand side of (B4) can be no greater than that of (B5), a condition which reduces to

$$\left(\delta_1+\delta_2\right)|\alpha_1\alpha_3\beta_3|^2 \leq \frac{\left(\delta_1+\delta_2\right)\eta_1}{|q|^2\eta_3}\left(1-|\alpha_1\beta_3/\beta_1|^2\right)\left(1-|\alpha_1\beta_3/\beta_1|^2\,[1+\left(\delta_1+\delta_2\right)/2]\right). \tag{B6}$$

Since by assumption, $\delta_1+\delta_2<0$, this can be rearranged to give

$$\frac{(\delta_1+\delta_2)}{2}\left|\frac{\alpha_1\beta_3}{\beta_1}\right|^2 \geq 1-\left|\frac{\alpha_1\beta_3}{\beta_1}\right|^2-\frac{\eta_3\left|q\alpha_1\alpha_3\beta_3\right|^2}{\eta_1\left(1-\left|\alpha_1\beta_3/\beta_1\right|^2\right)}. \tag{B7}$$

This is impossible, since the left-hand side of this is negative but by (13), the right-hand side is non-negative. We can therefore conclude that there is no measurement that does as well as that found at the end of Sec. III B, which is therefore the unique optimal measurement for unambiguously discriminating the states of (12). This is the result we set out to prove, so we are done.

---

[1] S. M. Cohen, "Necessary condition for local quantum operations and classical communication with extensive violation by separable operations," Phys. Rev. A **90**, 012336 (2014).

[2] S. M. Cohen, "Class of unambiguous state discrimination problems achievable by separable measurements but impossible by local operations and classical communication," Phys. Rev. A **91**, 012321 (2015).

[3] E. M. Rains, "Rigorous treatment of distillable entanglement," Phys. Rev. A **60**, 173 (1999).

[4] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum nonlocality without entanglement," Phys. Rev. A **59**, 1070 (1999).

[5] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases, uncompletable product bases, and bound entanglement," Commun. Math. Phys. **238**, 379 (2003).

[6] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases and bound entanglement," Phys. Rev. Lett. **82**, 5385 (1999).

[7] J. Niset and N. J. Cerf, "Multipartite nonlocality without entanglement in many dimensions," Phys. Rev. A **74**, 052103 (2006).

[8] E. Chitambar and R. Duan, "Nonlocal entanglement transformations achievable by separable operations," Phys. Rev. Lett. **103**, 110502 (2009).

[9] Dan Stahlke and Robert B. Griffiths, "Entanglement requirements for implementing bipartite unitary operations," Phys. Rev. A **84**, 032316 (2011).

[10] R. Duan, Y. Feng, Y. Xin, and M. Ying, "Distinguishability of quantum states by separable operations," arXiv:0705.0795v2 [quant-ph] (2007).

[11] Masato Koashi, Fumitaka Takenaga, Takashi Yamamoto, and Nobuyuki Imoto, "Quantum nonlocality without entanglement in a pair of qubits," arXiv:0709.3196 [quant-ph] (2007).

[12] Andrew M. Childs, Debbie Leung, Laura Mančinska, and Maris Ozols, "A framework for bounding nonlocality of state discrimination," Communications in Mathematical Physics **323**, 1121–1153 (2013).

[13] Eric Chitambar, Wei Cui, and Hoi-Kwong Lo, "Entanglement monotones for w-type states," Phys. Rev. A **85**, 062316 (2012).

[14] Eric Chitambar, Wei Cui, and Hoi-Kwong Lo, "Increasing entanglement monotones by separable operations," Phys. Rev. Lett. **108**, 240504 (2012).

[15] Vlad Gheorghiu and R. B. Griffiths, "Entanglement transformations using separable operations," Phys. Rev. A **76**, 032310 (2007).

[16] S. M. Cohen, "When a quantum measurement can be implemented locally, and when it cannot," Phys. Rev. A **84**, 052322 (2011).

[17] S. M. Cohen, "Local quantum protocols for separable measurements with many parties," Phys. Rev. A **87**, 052135 (2013).

[18] I.D. Ivanovic, "How to differentiate between non-orthogonal states," Physics Letters A **123**, 257 (1987).

[19] D. Dieks, "Overlap and distinguishability of quantum states," Physics Letters A **126**, 303 (1988).

[20] A. Peres, "How to differentiate between non-orthogonal states," Physics Letters A **128**, 19 (1988).

[21] Anthony Chefles, "Unambiguous discrimination between quantum states," Physics Letters A **69**, 339–347 (1998).

[22] Anthony Chefles, "Condition for unambiguous state discrimination using local operations and classical communication," Phys. Rev. A **69**, 050307 (2004).

[23] Jonathan Walgate and A.J. Scott, "Generic local distinguishability and completely entangled subspaces," J. Phys. A: Math. Theor. **41**, 375305 (2008).

[24] Somshubhro Bandyopadhyay and Jonathan Walgate, "Local distinguishability of any three quantum states," J. Phys. A: Math. Theor. **42**, 072002 (2009).

[25] Runyao Duan, Yuan Feng, Zhengfeng Ji, and Mingsheng Ying, "Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication," Phys. Rev. Lett. **98**, 230502 (2007).

[26] Yi-Xin Chen and Dong Yang, "Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communications," Phys. Rev. A **65**, 022320 (2002).

[27] Zhengfeng Ji, Hongen Cao, and Mingsheng Ying, "Optimal conclusive discrimination of two states can be achieved locally," Phys. Rev. A **71**, 032323 (2005).
[28] Eric Chitambar, Runyao Duan, and Min-Hsiu Hsieh, "When do local operations and classical communication suffice for two-qubit state discrimination?" IEEE Trans. Inf. Theory **60**, 1549 (2014).
[29] Clifford A. Shaffer, *Data Structures and Algorithm Analysis in C++*, 3rd ed. (Dover, E-book, 2011) Chap. 5.
[30] Edward A. Bender and S. Gill Williamson, *Lists, Decisions and Graphs* (E. A. Bender and S. G. Williamson, http://cseweb.ucsd.edu/ gill/BWLectSite/, 2010).