Local approximation for perfect discrimination of quantum states

Scott M. Cohen *

Department of Physics, Portland State University, Portland, Oregon 97201, USA

(Received 20 August 2022; accepted 15 December 2022; published 3 January 2023)

Quantum state discrimination involves identifying a given state out of a set of possible states. When the states are mutually orthogonal, perfect state discrimination is always possible using a global measurement. In the case of multipartite systems when the parties are constrained to use multiple rounds of local operations and classical communication (LOCC), perfect state discrimination is often impossible even with the use of *asymptotic LOCC*, wherein an error is allowed but must vanish in the limit of an infinite number of rounds. Utilizing our recent results on asymptotic LOCC, we derive a lower bound on the error probability for LOCC discrimination of any given set of mutually orthogonal pure states. Informed by the insights gained from this lower bound, we are able to prove necessary conditions for perfect state discrimination by asymptotic LOCC. We then illustrate by example the power of these necessary conditions in significantly simplifying the determination of whether perfect discrimination of a given set of states can be accomplished arbitrarily closely using LOCC. The latter examples include a proof that perfect discrimination by asymptotic LOCC is impossible for any *minimal* unextendible product basis (UPB), where minimal means that for the given multipartite system no UPB with a smaller number of states can exist. We also give a simple proof that what has been called *strong nonlocality without entanglement* is considerably stronger than had previously been demonstrated.

DOI: 10.1103/PhysRevA.107.012401

I. INTRODUCTION

Nonlocality in quantum physics is a concept that has long intrigued researchers. Recognizing that this concept can mean different things in different contexts, Griffiths [1] has drawn a distinction between the use of the term nonlocality to describe the properties of quantum systems, on the one hand, and nonlocal influences between systems, on the other. The latter is a subject that continues to be widely debated, even to the present day.[1] Nonlocal properties of quantum systems are less controversial, but there are at times differing conceptions of what they entail. One such example, wherein a set of quantum states can exhibit nonlocal properties even when no one of those states is itself nonlocal, has received a great deal of attention in recent years. This property, first discovered over 20 years ago in the seminal work of Ref. [2], is commonly referred to as nonlocality without entanglement (NLWE) and arises in the context of quantum state discrimination [3–7], wherein a party or parties are tasked with determining in which one of a known set of states their shared system had been prepared. Quantum state discrimination is a key paradigm in quantum information processing and quantum computing [8], and can also play a role in any experiment for which there exists enough *a priori* information to narrow down the possible outcomes of that experiment.

When the set of states consists only of product states, having no entanglement [9] and therefore exhibiting no nonlocal properties individually, it may still turn out that, taken as a set, the collection does indeed behave nonlocally. As shown in Ref. [2], a particular set of mutually orthogonal product states on a 3×3 system cannot be perfectly discriminated when the parties are restricted to multiple rounds of measuring their local part of the system and communicating their outcomes to the other parties—a process known as local operations and classical communication (LOCC)—even though this can be easily accomplished by a single global measurement on the entire system taken as a whole. It is in this sense that the set of states exhibits nonlocality: When the system is measured locally it behaves differently than when it is measured globally.

The proof of NLWE given in Ref. [2] involved a long, complicated argument. The reason was that their aim was not simply to exclude the possibility of perfect local discrimination of the states, which is actually quite easily shown, but importantly, that the parties could not even approach accomplishing this task arbitrarily closely. We believe the latter definition of NLWE is the proper one to follow, and we will do so throughout this paper: A set of mutually orthogonal product states exhibits NLWE if and only if perfect discrimination of that set is impossible even when an error is allowed but must vanish in the limit of an infinite number of rounds. By not allowing for this vanishing error, one overlooks the fact that any measurement will be subject to experimental imperfections—that nothing is ever accomplished perfectly in the real world. As a consequence of these unavoidable imperfections, it is more appropriate to ask whether or not a task can be accomplished arbitrarily closely and, if not, the amount of error that is impossible to avoid. Many of us over the years have failed to clearly understand the important distinction that considering infinite-round protocols, alone, is not the same as allowing for vanishing error. In the former approach, it

*cohensm52@gmail.com

[1]While we have not studied this issue in depth, we do lean in the direction of Griffiths's view that there is no evidence for these nonlocal influences.

would be sufficient to show that no party can make a first local measurement without destroying orthogonality of the set (see, for example, Appendix B of Ref. [10]): If no one can start the protocol, they cannot continue it indefinitely (or at all). This approach fails to consider all possible *sequences* of LOCC protocols of steadily increasing number of rounds, wherein as one proceeds through the sequence, the error incurred might become smaller and smaller, approaching zero asymptotically. To better understand what is missed, let us consider how one may think about these things.

LOCC protocols are commonly viewed as a tree graph with a single root node representing the situation before any party has measured. From the root node, the tree branches to multiple nodes, each one representing an outcome of the first measurement, which is local, being implemented by only one party. From each of these nodes, the tree continues to branch to more nodes, each set of *child* nodes of a given *parent* node representing outcomes of the local measurement performed at that stage of the protocol. A finite branch of the tree starts at the root and continues until it reaches a node that has no children, denoted as a *leaf* node. In the limit of an infinite number of rounds, there may be branches that never terminate and are of infinite length. As shown in Ref. [11], each branch (finite or infinite) corresponds directly to a continuous path of product operators through a particular subset of operator space. Significantly, for a given protocol, each such path is *piecewise local*, which means that it consists of straight line segments along which the product operator changes only in one party's local part. For example, on a bipartite system, this might be represented as $[(1-x)\mathcal{A}+x\mathcal{A}']\otimes\mathcal{B}$, which is a line stretching from $\mathcal{A}\otimes\mathcal{B}$ to $\mathcal{A}'\otimes\mathcal{B}$ as x ranges from 0 to 1, $\mathcal{A}'$ corresponding to one outcome of a local measurement by Alice, $\mathcal{A}$ being the cumulative effect of Alice's actions up to (and preceding) this latest measurement. Only the A part changes; the B part remains unchanged. This piecewise local property applies even to infinite branches, which then consist of many (an infinite number of) infinitesimally short pieces.

To understand why only considering individual infinite-round protocols overlooks possibilities, let us recall how we learned about integrals in our introductory calculus classes: Any curve can be approximated arbitrarily closely by a piecewise constant curve, and this provides a way to approximate the area under the original curve. In the limit that the number of constant pieces goes to infinity, the piecewise constant curve asymptotically approaches the original curve, which in general is *not* piecewise constant. Similarly, there exist sequences of LOCC protocols for which each protocol in the sequence corresponds to piecewise local paths in operator space, but for which the limit of this sequence corresponds to paths which are *not* piecewise local. In particular, it may well be that the limit of a sequence of LOCC protocols corresponds to an initial measurement that is not local, and such sequences are *not* excluded by simply demonstrating that the only initial *local* measurement that does not destroy orthogonality of the original set is a measurement for which all outcomes are proportional to the identity operator (a *trivial* measurement). Instead, as we will see below, it is sufficient to show that any nontrivial initial *separable* measurement operator that is arbitrarily close to $I_{\mathcal{H}}$ destroys orthogonality (see Corollary 1).

In an effort to ensure these ideas are clear, let us divide the class of infinite-round protocols into two distinct subclasses [12]. The first subclass involves sequences of protocols where each subsequent protocol in a given sequence differs from the preceding protocol simply by adding more rounds of communication, but without changing the local measurements implemented in earlier rounds. Since the earlier rounds are unchanged, the branches remain piecewise local even in the infinite limit. Thus, one obtains a valid LOCC protocol in this limit, albeit one having an infinite number of rounds, so this subclass may be seen as being a part of LOCC. The second subclass includes limits of sequences in which measurements made at the earlier rounds are changed from one protocol in the sequence to the next. This subclass must be included to obtain the asymptotic LOCC discussed above, and its inclusion gives rise to the topological closure of LOCC, which we denote as $\overline{\text{LOCC}}$ in the sequel. By changing those earlier rounds, the branches need not correspond to piecewise local paths in the infinite limit (see the comparison to limits of piecewise constant curves in the preceding paragraph) and as such, in this limit, one may fail to obtain a valid LOCC protocol.

Let us review the main result, Theorem 1, of Ref. [11], where we consider a measurement to be a positive operator valued measure (POVM) consisting of a set of positive semidefinite operators, E_j, known as POVM elements. Note that $\mathcal{M}\in\overline{\text{LOCC}}$ means there exists a sequence of LOCC protocols, the nth such protocol implementing measurement $\mathcal{M}_n$, such that $\lim_{n\to\infty}\mathcal{M}_n=\mathcal{M}$.

Theorem 1 of Ref. [11]. If $\mathcal{M}\in\overline{\text{LOCC}}$, with measurement $\mathcal{M}$ consisting of POVM elements E_j, then for each j, there exists a continuous, monotonic path of product operators from $\mathcal{I}_{\mathcal{H}}$ to a point on the (half-open) line segment $(0,E_j]$, and this path lies entirely within the geometric object, $\mathcal{Z}_{\mathcal{M}}=\sum_j[0,E_j]$, which is known as a *zonotope*.

An alternative, but equivalent, definition of the zonotope just introduced is $\mathcal{Z}_{\mathcal{M}}:=\{z|z=\sum_j c_jE_j,\ 0\leqslant c_j\leqslant 1\,\forall j\}$. In addition, by *monotonic*, we mean that the trace of the product operators is nonincreasing along these paths. These paths, which need not themselves be piecewise local, are found as the limit of a sequence of piecewise local paths, the latter being associated with that sequence of LOCC protocols, the limit of which implements $\mathcal{M}$. Of course, without the restriction that the paths lie within $\mathcal{Z}_{\mathcal{M}}$, these paths would always exist. That is, there are always such paths between any pair of product operators. For example, one path from $\mathcal{A}\otimes\mathcal{B}$ to $\mathcal{A}'\otimes\mathcal{B}'$ would be $[(1-x)\mathcal{A}+x\mathcal{A}']\otimes\mathcal{B}$ followed by $\mathcal{A}'\otimes[(1-y)\mathcal{B}+y\mathcal{B}']$. As is amply illustrated by the examples in Ref. [11], however, there are many measurements for which there are no paths of product operators starting at $I_{\mathcal{H}}$ and lying within $\mathcal{Z}_{\mathcal{M}}$. It is worth noting that those examples were drawn from well-studied cases of local state discrimination, for which much of the work in Ref. [11] involved determining the most general separable measurement $\mathcal{M}$ capable of perfectly discriminating the given set, and then showing that the requisite paths of product operators within $\mathcal{Z}_{\mathcal{M}}$ do not exist. Here, we simplify things by finding ways

to reach these conclusions for given sets of states without the need to know anything about what measurements can accomplish the task successfully. Another observation is that since the paths considered here are continuous and starting at $I_{\mathcal{H}}$, they require the existence of a positive semidefinite product operator lying within $\mathcal{Z}_{\mathcal{M}}$ at every distance, R, from $I_{\mathcal{H}}$ in the range $0 \leqslant R \leqslant d(I_{\mathcal{H}}, E_j)$, with $d(X, Y)$ the distance between (normalized operators) X and Y. Suppose such continuous paths do not exist. Then it seems a reasonable guess that the error incurred by any LOCC protocol used for implementing the desired POVM will be in some way related to how far away from $\mathcal{Z}_{\mathcal{M}}$ one must stray in order to find such paths, and in an attempt to lower bound this error, one may then consider, for each R, how far it is from $\mathcal{Z}_{\mathcal{M}}$ to the nearest positive semidefinite product operator. This is part of the motivation for the present work, in which we prove a result that is similar, but not quite identical, to what we have just conjectured. Our result differs from the ideas just described in one very important aspect: in order to know the distance of an operator from $\mathcal{Z}_{\mathcal{M}}$, one needs to know the measurement, $\mathcal{M}$. It turns out that knowledge of what measurement(s) might be successful is not needed; all we need to know is the set of states one is setting out to discriminate.

The remainder of the paper is organized as follows: In Sec. II, we use the insights of Ref. [11] to derive a lower bound on the probability of error, p_{err}, in locally discriminating any mutually orthogonal set of pure states. We allow for limits of sequences of protocols, discussed above, going beyond LOCC itself to include $\overline{\text{LOCC}}$. These arguments demonstrate that $p_{\text{err}} > 0$ implies the set of states cannot be perfectly discriminated within $\overline{\text{LOCC}}$, which would require asymptotically vanishing error. Unfortunately, we have found this lower bound to be difficult to compute. Nonetheless, in Sec. III we use the insights gleaned from this lower bound to prove two theorems providing necessary conditions that a given set of states can be perfectly discriminated within $\overline{\text{LOCC}}$, and then in Sec. IV we give examples where these theorems easily demonstrate that this is impossible. We also show that perfect discrimination within $\overline{\text{LOCC}}$ is impossible when the set of states is an unextendible product basis with the minimal number of states for the associated multipartite Hilbert space. Finally, we end with our conclusions.

II. ERROR PROBABILITY FOR DISCRIMINATING ANY SET OF ORTHOGONAL PURE STATES BY $\overline{\text{LOCC}}$

In this section, we begin by considering the error incurred in using LOCC to discriminate a set $\mathcal{S}$ of N orthogonal pure states on Hilbert space $\mathcal{H}$: $\mathcal{S} = \{\eta_m, |\Psi_m\rangle\}$, given with *a priori* probabilities $\eta_m > 0$, $\sum_m \eta_m = 1$, and $\langle\Psi_m|\Psi_n\rangle = \delta_{mn}$. For an arbitrary set of orthogonal states $|\Psi_m\rangle$, not necessarily a complete basis of the Hilbert space, there will generally be a number of possible global measurements that perfectly discriminate those states. In general, however, when these states describe a multipartite system, there may be constraints on the actions the parties are able to perform, and under such circumstances, any given global measurement, $\mathcal{M}_g$, may be impossible. Instead, the parties may be restricted to using LOCC in their efforts to discriminate the state, and they may be forced to utilize a different measurement, say,

$$\mathcal{M}_Q = \left\{ Q_i \middle| \sum_i Q_i = I_{\mathcal{H}}, Q_i \geqslant 0 \right\}. \tag{1}$$

It may be that $\mathcal{M}_Q$ can be implemented by LOCC, at least arbitrarily closely: $\mathcal{M}_Q \in \overline{\text{LOCC}}$. If not, then the question arises, how well can the parties do in discriminating the state if they are able to perform the best possible LOCC measurement, $\mathcal{M}_Q$?

Define P_R to be the set of positive semidefinite product operators acting on $\mathcal{H}$ and lying at a distance R from the identity operator $I_{\mathcal{H}}$ [distances *between normalized operators* are measured using the Frobenius norm, defined above Eq. (4), below], and also define

$$\Pi = \sum_m \sqrt{\eta_m}\Psi_m, \tag{2}$$

with $\Psi_m = |\Psi_m\rangle\langle\Psi_m|$. Then, in Appendix A, we prove the following theorem.

Theorem 1. Given any set of mutually orthogonal pure states, the probability of error for local state discrimination of this set is lower bounded as

$$p_{\text{err}} \geqslant \frac{1}{2} \max_R \min_{\substack{Q\in\mathcal{P}_R \\ z\in\mathcal{Z}_\Psi}} \left\| \frac{\Pi Q \Pi - z}{\text{Tr}(\Pi^2 Q)} \right\|^2, \tag{3}$$

where $\|\cdot\|$ is the Frobenius norm, and $\max_R$ is taken over the range $0 \leqslant R \leqslant \sqrt{(D-1)/D}$ (see Appendix A for details). With $\mathcal{Z}_\Psi := \{z | z = \sum_m c_m \Psi_m,\ 0 \leqslant c_m \leqslant 1\ \forall m\}$, it is straightforward to see that the minimum over $z \in \mathcal{Z}_\Psi$ is achieved at $z = \sum_m \eta_m \langle\Psi_m|Q|\Psi_m\rangle\Psi_m$. Note that the definition of $\mathcal{Z}_\Psi$ closely adheres to how $\mathcal{Z}_{\mathcal{M}}$ was defined above for a measurement $\mathcal{M}$, even though the set of operators, Ψ_m, does not in general constitute a complete measurement. When $p_{\text{err}} = 0$ and the set of states can be perfectly discriminated using $\overline{\text{LOCC}}$, then operator Π effectively takes the paths of Ref. [11], which are associated with an actual complete measurement $\mathcal{M}$ and lie within $\mathcal{Z}_{\mathcal{M}}$, projecting (and scaling, by the η_m) them into $\mathcal{Z}_\Psi$. Thus, we obtain continuous paths of operators that lie entirely within $\mathcal{Z}_\Psi$ (these need not be product operators after they are projected by Π into $\mathcal{Z}_\Psi$; see Sec. III, below for further details), and this is why we need not know $\mathcal{Z}_{\mathcal{M}}$ or the optimal measurement, $\mathcal{M}$, that is to be used. Given this observation, it would seem to make sense to consider measurements $\mathcal{M}$ such that $\mathcal{Z}_\Psi \subseteq \mathcal{Z}_{\mathcal{M}}$ whenever possible, although it is not entirely clear this would necessarily minimize the error.

Calculating this lower bound on p_{err} appears to be extremely challenging in practice. Approaching this problem analytically is prohibitively difficult except for the smallest systems, that is, for two qubits, in which case it is *merely* very challenging. For the latter case, we have been able to show for discriminating the four Bell states [8] by LOCC—when they are given with equal *a priori* probabilities, $\eta_m = 1/4$—that our lower bound is $p_{\text{err}} = 1/4$, which is just a factor of 2 smaller than the known optimal strategy [13]. That this is the correct order of magnitude may be seen as an encouraging sign. Calculating this lower bound does not appear to fall into any of the classes that admit an efficient numerical approach, however. Therefore, one would need access to significant

computational resources to obtain a result with a high degree of confidence that it is truly a lower bound. Therefore, in the next section, we will obtain powerful necessary conditions for the possibility of perfect state discrimination by $\overline{\text{LOCC}}$ of any given set of mutually orthogonal pure states. Note that the *a priori* probabilities, $\eta_m > 0$, are only relevant to the question of the amount of error incurred and not to whether or not perfect discrimination is possible.

III. NECESSARY CONDITIONS FOR PERFECT STATE DISCRIMINATION BY $\overline{\text{LOCC}}$

Our first necessary condition is obtained as follows. If there exists R such that the quantity maximized over R in Eq. (3) is nonvanishing, then $p_{\text{err}} > 0$—or alternatively (recalling the perspective of the result of Ref. [11]), the required continuous paths of product operators whose projection by Π lies entirely within $\mathcal{Z}_\Psi$ do not exist—then perfect discrimination of the set of states by $\overline{\text{LOCC}}$ is impossible.

Theorem 2. Given a set of mutually orthogonal quantum states, $\{|\Psi_m\rangle\}$, if for any fixed state $|\Psi_n\rangle$, no continuous path of positive semidefinite product operators, say $Q_i(s)$, exists such that the following two conditions hold, then this set of states cannot be perfectly discriminated within $\overline{\text{LOCC}}$:

(1) The path begins at $I_\mathcal{H}$ and ends at some fixed positive semidefinite product operator, Q_i, where $\Pi Q_i \Pi \propto \Psi_n$, and index i will generally depend on index n.

(2) For every s, $Q_i(s)$ is diagonal in the (partial) basis of the $|\Psi_m\rangle$.

Note that the condition that $Q_i(s)$ is diagonal in the $|\Psi_m\rangle$ is equivalent to $\Pi Q_i(s)\Pi$ lying within $\mathcal{Z}_\Psi$.

Proof. Suppose there exists measurement $\mathcal{M}_Q \in \overline{\text{LOCC}}$ as in Eq. (1) that perfectly discriminates the given set of states. Then by Theorem 1 of Ref. [11], for each $Q_i \in \mathcal{M}$, there exists a continuous path of product operators $Q_i(s)$ extending from $I_\mathcal{H}$ to Q_i and lying entirely within $\mathcal{Z}_\mathcal{M}$. Furthermore, each $Q_i \geqslant 0$ identifies without error one of the states in the set, say, Ψ_n, or in other words, $\text{Tr}(Q_i\Psi_m) = \delta_{mn}q_{in}$, which, since $\Psi_n \geqslant 0$ as well, means that $Q_i\Psi_m = 0 = \Psi_m Q_i$ for all $m \neq n$. This implies that $\Pi Q_i \Pi = q_{in}\Psi_n$, for the given fixed n, with $q_{in} \geqslant 0$. Now, from the proof of Theorem 1 in Ref. [11], we know that $Q_i(s) = \sum_j c_{ij}(s)Q_j$ with $c_{ij}(s) \geqslant 0$. This leads to $\Pi Q_i(s)\Pi = \sum_j c_{ij}(s)\Pi Q_j \Pi = \sum_j \sum_m q_{jm}c_{ij}(s)\Psi_m \in \mathcal{Z}_\Psi$. Since the path terminates at Q_i, and as we have seen, $\Pi Q_i \Pi \propto \Psi_n$ for some n, the proof of this theorem is complete. ■

We will use this theorem in the next section to prove that no unextendible product basis consisting of the minimal number of states can be perfectly discriminated using $\overline{\text{LOCC}}$. First, noting that we can write our positive semidefinite path of operators as $Q(s) = K(s)^\dagger K(s)$, the condition in Theorem 2 that $Q(s)$ is diagonal in the partial basis of the $|\Psi_m\rangle$ is equivalent to orthogonality of the new states, $K(s)|\Psi_m\rangle$. Thus, we have the following corollary to Theorem 2.

Corollary 1. If a given set of mutually orthogonal quantum states, $|\Psi_m\rangle$, can be perfectly discriminated within $\overline{\text{LOCC}}$, then there exists a continuous path of product operators, $K(s)$, such that for every s, the states $K(s)|\Psi_m\rangle$ remain orthogonal along the entire path.

Notice how this generalizes the observation, discussed here in the Introduction, that the initial, local measurement in any LOCC protocol must preserve orthogonality of the states. Here we see instead that for $\overline{\text{LOCC}}$, orthogonality is preserved along entire continuous paths of operators, and also that while $K(s)$ must be a product (separable measurement) operator, this path need not be piecewise local, so need not correspond to a series of local measurements.

The proof of the next result will use an extension of the notion, introduced in Ref. [14], of partitions of the states of an unextendible product basis (UPB) among the various parties. Note, however, that this theorem is general, being applicable to any set of states, not just UPBs. Let us review these ideas before proceeding to the theorem itself.

An UPB is a set, $\mathcal{S}$, of N mutually orthogonal product states on multipartite Hilbert space $\mathcal{H}$ such that there is no other product state on $\mathcal{H}$ that is orthogonal to all the original N states in the UPB. In principle, a complete product basis of $\mathcal{H}$ is unextendible, but one is usually only concerned with *partial* bases, such that the N states do not span the complete space $\mathcal{H}$. The following lemma was proved in Ref. [14].

Lemma 1 [14]. Let π be a partition of $\mathcal{S}$ into P disjoint subsets equal to the number of parties: $\mathcal{S} = S_1 \cup S_2 \cup \cdots \cup S_P$. Let $r_\alpha = \text{rank}\{|\psi_j^{(\alpha)}\rangle : |\Psi_j\rangle \in S_\alpha\}$ be the local rank of subset S_α as seen by the αth party. Then $\mathcal{S}$ is extendible if and only if there exists a partition π such that for all $\alpha = 1, \ldots, P$, the local rank of the αth subset is less than the dimensionality of the αth party's Hilbert space. That is to say, $\mathcal{S}$ is extendible if and only if there exists π such that for all α, $r_\alpha < d_\alpha$.

The partitioning introduced in this lemma can be understood as a way of distributing "the job of being orthogonal to a new product state" [15] among the various parties. If, for every such partition, at least one party's local states—say party α with set of local states S_α—span the full local Hilbert space, then there is no state orthogonal to all the states in S_α, and party α fails to fulfill its role of being orthogonal to an additional product state. If for every partition at least one party fails in this role, then there is no additional product state orthogonal to all the states in $\mathcal{S}$. In other words, under these circumstances, the original set is unextendible.

We are now ready to prove our second necessary condition for perfect state discrimination by $\overline{\text{LOCC}}$.

Theorem 3. Consider any mutually orthogonal set of product states $\mathcal{S} = \{|\Psi_j\rangle = \bigotimes_\alpha |\psi_j^{(\alpha)}\rangle\}$. For each party α, define the subset of all index pairs, $J_\alpha = \{(i,j)|\langle\psi_i^{(\alpha)}|\psi_j^{(\alpha)}\rangle = 0;\ \langle\psi_i^{(\beta)}|\psi_j^{(\beta)}\rangle \neq 0\ \forall \beta \neq \alpha\}$. If for every party α the set of dyads, $\{|\psi_i^{(\alpha)}\rangle\langle\psi_j^{(\alpha)}|\}_{(i,j)\in J_\alpha}$, spans a space of dimension $d_\alpha^2 - 1$, then this set of product states cannot be perfectly discriminated within $\overline{\text{LOCC}}$.

Throughout the remainder of this paper, we will refer to kets $|\psi_j^{(\alpha)}\rangle$ as the *local states* on $\mathcal{H}_\alpha$. The idea of the proof is that when these dyads span a space of dimension $d_\alpha^2 - 1$, there is one and only one operator orthogonal to all of them, that being the identity operator, I_α. If this is true for all parties, there can be no global product operator that is orthogonal to all these global dyads and is close to but not proportional to $I_\mathcal{H}$, and then by Theorem 1, perfect discrimination by $\overline{\text{LOCC}}$ is impossible.

Proof. We extend the notion of partitioning to the set of dyads $\mathcal{D} = \{|\Psi_i\rangle\langle\Psi_j|\}_{j\neq i}$. Let $\hat{\pi}$ be such a partition, yielding $\mathcal{D} = D_1 \cup D_2 \cup \cdots \cup D_P$, which we will understand as a way to distribute the "job of being orthogonal" to a product operator $Q = \bigotimes_\alpha Q^{(\alpha)}$. That is, given $\hat{\pi}(s)$, $\mathrm{Tr}(Q^{(\alpha)}(s)|\psi_i^{(\alpha)}\rangle\langle\psi_j^{(\alpha)}|) = 0$ for all $|\Psi_i\rangle\langle\Psi_j| \in D_\alpha$.

By Theorem 2, if the states of $\mathcal{S}$ can be perfectly discriminated within $\overline{\mathrm{LOCC}}$, then there exists a continuous path of positive semidefinite product operators $Q(s)$ such that for every s, $Q(s)$ is diagonal in the partial basis of the states in $\mathcal{S}$: $\langle\Psi_i|Q(s)|\Psi_j\rangle = \delta_{ij}\langle\Psi_i|Q(s)|\Psi_i\rangle$. Now, for each distinct s, one may assign a different partition $\hat{\pi}(s)$ to distribute the orthogonality job. However, given that there is a finite number of states, N, there is also a finite number of dyads, $N(N-1)$, and thus there is a finite number of distinct partitions that can be used here. If, for any given partition, each (and every) party α is given a set of dyads spanning a subspace of dimension $d_\alpha^2 - 1$, then for that partition there is one and only one operator $Q^{(\alpha)}$ orthogonal to all of that party's dyads, and thus there is one and only one operator Q orthogonal to all the multipartite dyads, $|\Psi_i\rangle\langle\Psi_j|$ for $j \neq i$. Given there are a finite number of partitions, there are then only a finite number of operators orthogonal to all the multipartite dyads, and there cannot be a continuous path of operators from $I_\mathcal{H}$ to anywhere. Indeed, given that the dyads have been distributed according to the index sets J_α, each of these local dyads is traceless, and thus orthogonal to the identity operator, I_α. Thus, for each such partition, the only operator orthogonal to these dyads is $Q(s) = I_\mathcal{H}$, which is a *point* and not a *path* that leaves $I_\mathcal{H}$, as is required.

There are two points that need clarification here. First, partitioning dyads according to J_α omits dyads, which are therefore not given to any of the parties. As already noted elsewhere, this is not an issue for our proof because including those additional dyads can only *increase* the space spanned by the dyads given to any given party, and so can only further constrain operators $Q^{(\alpha)}(s)$ orthogonal to these local dyads. The second point is that there are many partitions that do not conform to J_α. For example, there will generally be partitions such that dyad $|\Psi_i\rangle\langle\Psi_j|$ is given to party α even when the corresponding local states on α are not themselves orthogonal. As explained in the next paragraph, we will not need to consider any of these other partitions.

The reason we can restrict consideration to those partitions that follow J_α is that these are the only ones relevant for small enough s. Let us see why this is so. Since this path of operators starts at $Q(0) = I_\mathcal{H}$, then by continuity, there exists $Q(s)$ for small enough s which is arbitrarily close to $I_\mathcal{H}$. If $\langle\psi_i^{(\beta)}|\psi_j^{(\beta)}\rangle \neq 0$, then for small enough s, $\langle\psi_i^{(\beta)}|Q^{(\beta)}(s)|\psi_j^{(\beta)}\rangle$ is also nonvanishing, and $|\psi_i^{(\beta)}\rangle\langle\psi_j^{(\beta)}|$ is not orthogonal to $Q^{(\beta)}(s)$. To see this formally, one may measure distances between operators on $\mathcal{H}_\beta$ by the Frobenius norm, $\|X\| = \sqrt{\sum_{k,l}|X_{kl}|^2} \geqslant |\langle\psi_i^{(\beta)}|X|\psi_j^{(\beta)}\rangle|$ for some fixed i, j (no sum).[2]

[2]This inequality is obvious when $\langle\psi_i^{(\beta)}|\psi_j^{(\beta)}\rangle = 0$, and it is straightforward to show that $\|X\| \geqslant |\langle\psi_i^{(\beta)}|X|\psi_j^{(\beta)}\rangle|$ also holds for any nonorthogonal pair of states.

Then, for $|\langle\psi_i^{(\beta)}|\psi_j^{(\beta)}\rangle| = r \gg \epsilon > 0$ and $Q^{(\beta)}(s)$ within ϵ of I_β, we have

$$\begin{aligned}\epsilon > \|I_\beta - Q^{(\beta)}(s)\| &\geqslant \left|\langle\psi_i^{(\beta)}|(I_\beta - Q^{(\beta)}(s))|\psi_j^{(\beta)}\rangle\right| \\ &= \left|r - \langle\psi_i^{(\beta)}|Q^{(\beta)}(s)|\psi_j^{(\beta)}\rangle\right|, \end{aligned} \tag{4}$$

implying that $|\langle\psi_i^{(\beta)}|Q^{(\beta)}(s)|\psi_j^{(\beta)}\rangle| \approx r \gg \epsilon > 0$ and $Q^{(\beta)}(s)$ is not orthogonal to the corresponding dyad, $|\psi_j^{(\beta)}\rangle\langle\psi_i^{(\beta)}|$. If $\langle\psi_i^{(\beta)}|\psi_j^{(\beta)}\rangle \neq 0$ for all $\beta \neq \alpha$, then the job of $|\Psi_j\rangle\langle\Psi_i|$ being orthogonal to $Q(s)$ for small enough s must be assigned to party α, and this completes the proof. ∎

As a simple illustration of how this works, consider the set of two-qubit states, which can be perfectly discriminated by LOCC, $\mathcal{S} = \{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|+\rangle, |1\rangle|-\rangle\}$, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. For the second party, we have the index set $J_2 = \{(1,2),(2,1),(3,4),(4,3)\}$. The corresponding dyads are $\{|0\rangle\langle 1|, |1\rangle\langle 0|, |+\rangle\langle -|, |-\rangle\langle +|\}$. This set spans a space of dimension $d_2^2 - 1 = 3$, indicating there is a unique local operator orthogonal to the entire set, that being the identity operator I_2. Thus, there is no product operator $A \otimes B$ close to $I_\mathcal{H}$ that *does not destroy orthogonality* of the original set $\mathcal{S}$, except possibly those with $B \propto I_2$. Looking at the first party, $J_1 = \{(1,3),(2,3),(1,4),(2,4),(3,1),(3,2),(4,1),(4,2)\}$, with corresponding dyads, $\{|0\rangle\langle 1|, |1\rangle\langle 0|\}$, which span a space of dimension only $2 < d_1^2 - 1$. This leaves party 1 with a range of possible measurement operators close to the identity (anything diagonal in the standard basis is acceptable) and, as is fairly obvious, this party can indeed initiate a successful LOCC protocol.

If the local parts of dyads $|\Psi_m\rangle\langle\Psi_n|$, $m \neq n$, are to span a subspace of dimension $d_\alpha^2 - 1$ for each party α, there must be enough pairs of states in the original set to distribute to all parties, $N(N-1) \geqslant \sum_\alpha (d_\alpha^2 - 1) =: T$. This provides a lower bound on the number of states, $N \geqslant \lceil \frac{1}{2} + \sqrt{T + \frac{1}{4}} \rceil$, which is smaller than the minimal number of states in a UPB on the same system. However, we do not know if there exist sets of states that achieve this new lower bound while still exhibiting NLWE, or if a larger number is needed.

Additional examples illustrating the power of these ideas will be found in the next section.

IV. APPLICATIONS

In this section, we illustrate the results of the preceding one with a few explicit examples.

A. The rotated domino states and the Tiles UPB

It is perhaps worth showing how easy it can sometimes be to prove that certain sets of states cannot be perfectly discriminated within $\overline{\mathrm{LOCC}}$. Let us begin with two well-known sets of states for which this has previously been proven [6,11] using more—sometimes, much, much more—complicated arguments. The rotated domino states are [2]

$$\begin{aligned}|\Psi_1\rangle &= |1\rangle \otimes |1\rangle, \\ |\Psi_2\rangle &= |0\rangle \otimes (\cos\theta_1|0\rangle + \sin\theta_1|1\rangle), \\ |\Psi_3\rangle &= |0\rangle \otimes (\sin\theta_1|0\rangle - \cos\theta_1|1\rangle), \\ |\Psi_4\rangle &= (\cos\theta_2|0\rangle + \sin\theta_2|1\rangle) \otimes |2\rangle,\end{aligned}$$

$$
\begin{aligned}
|\Psi_5\rangle &= (\sin\theta_2|0\rangle - \cos\theta_2|1\rangle)\otimes|2\rangle,\\
|\Psi_6\rangle &= |2\rangle\otimes(\cos\theta_3|1\rangle + \sin\theta_3|2\rangle),\\
|\Psi_7\rangle &= |2\rangle\otimes(\sin\theta_3|1\rangle - \cos\theta_3|2\rangle),\\
|\Psi_8\rangle &= (\cos\theta_4|1\rangle + \sin\theta_4|2\rangle)\otimes|0\rangle,\\
|\Psi_9\rangle &= (\sin\theta_4|1\rangle - \cos\theta_4|2\rangle)\otimes|0\rangle,
\end{aligned}
\tag{5}
$$

with $0 < \theta_j \leqslant \pi/4$. We can easily show these states cannot be perfectly discriminated using $\overline{\text{LOCC}}$.

Theorem 4. The rotated domino states of Eq. (5) cannot be perfectly discriminated using $\overline{\text{LOCC}}$.

Proof. We will use Theorem 3, so identify for the first party, $J_1 \supset \{(3,9),(5,7),(3,7),(4,5),(8,9)\}$, corresponding to dyads,

$$
\begin{aligned}
&|0\rangle(\sin\theta_4\langle 1| - \cos\theta_4\langle 2|), && (\sin\theta_4|1\rangle - \cos\theta_4|2\rangle)\langle 0|,\\
&|2\rangle(\sin\theta_2\langle 0| - \cos\theta_2\langle 1|), && (\sin\theta_2|0\rangle - \cos\theta_2|1\rangle)\langle 2|,\\
&|0\rangle(\langle 2|, && (|2\rangle\langle 0|,\\
&(\cos\theta_2|0\rangle + \sin\theta_2|1\rangle)(\sin\theta_2\langle 0| - \cos\theta_2\langle 1|), && (\cos\theta_4|1\rangle + \sin\theta_4|2\rangle)(\sin\theta_4\langle 1| - \cos\theta_4\langle 2|),
\end{aligned}
\tag{6}
$$

and the Hermitian conjugates of the last pair of dyads are omitted, as they are not needed. To readily show these are linearly independent, consider

$$
\begin{aligned}
0 = {} & c_1|0\rangle(\sin\theta_4\langle 1| - \cos\theta_4\langle 2|) + c_2(\sin\theta_4|1\rangle - \cos\theta_4|2\rangle)\langle 0| + c_3|2\rangle(\sin\theta_2\langle 0| - \cos\theta_2\langle 1|)\\
& + c_4(\sin\theta_2|0\rangle - \cos\theta_2|1\rangle)\langle 2| + c_5|0\rangle\langle 2| + c_6|2\rangle\langle 0| + c_7(\cos\theta_2|0\rangle + \sin\theta_2|1\rangle)(\sin\theta_2\langle 0| - \cos\theta_2\langle 1|)\\
& + c_8(\cos\theta_4|1\rangle + \sin\theta_4|2\rangle)(\sin\theta_4\langle 1| - \cos\theta_4\langle 2|).
\end{aligned}
\tag{7}
$$

It is very easy to show that this is satisfied if and only if all the coefficients vanish. The 0,0 matrix element of Eq. (7) gives $c_7 = 0$ and the 2,2 element gives $c_8 = 0$. Then, each off-diagonal element shows that one of the remaining c_j vanishes, and this encompasses all of them. Thus, $c_j = 0$ for all j, and these eight dyads are linearly independent. Since there is a symmetry between the parties, then by Theorem 3, this completes the proof. ■

Notice that while $|\Psi_1\rangle$ is needed to make this set a full basis, it does not appear in any of the dyads of Eq. (6). Therefore, the set still cannot be perfectly discriminated within $\overline{\text{LOCC}}$ even if this state is omitted.

Next, consider the states of the Tiles UPB, which is a subset of the dominoes (unrotated, all $\theta_j = \pi/4$), except with $|\Psi_1\rangle$ replaced by $|F\rangle$:

$$
\begin{aligned}
|F\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)\otimes(|0\rangle + |1\rangle + |2\rangle),\\
|\Psi_3\rangle &= \frac{1}{\sqrt{2}}|0\rangle\otimes(|0\rangle - |1\rangle),\\
|\Psi_5\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\otimes|2\rangle,\\
|\Psi_7\rangle &= \frac{1}{\sqrt{2}}|2\rangle\otimes(|1\rangle - |2\rangle),\\
|\Psi_9\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)\otimes|0\rangle.
\end{aligned}
\tag{8}
$$

We have the following.

Theorem 5. The Tiles UPB of Eq. (8) cannot be perfectly discriminated using $\overline{\text{LOCC}}$.

Proof. In this case, we can use six of the same dyads as were used for the (rotated) dominoes, the ones in the first three rows of Eq. (6) (but with $\theta_j = \pi/4$, as noted above). Then, instead of those in the fourth row there, include the local (on the first party) parts of $|\Psi_5\rangle\langle F|$ and $|\Psi_9\rangle\langle F|$. By following the same argument as was just used in the proof of the preceding theorem, it is easily seen that these are eight linearly independent dyads. Since there is again a symmetry between the parties, the proof is complete. ■

B. "Strong" quantum nonlocality without entanglement

We now turn to the results of Ref. [16] concerning what they have denoted as strong nonlocality without entanglement. We have argued in the Introduction that these results are perhaps not as strong as claimed or, at least, as one might wish them to be. The authors of that paper have not proved that the sets of states discussed in their paper exhibit NLWE, according to how we believe NLWE should be understood, and therefore they have also not proved that they exhibit a stronger version of NLWE, as is their claim. Here, we show that for the first of their sets of states (on a tripartite system), their claims are nonetheless correct, that this set does exhibit NLWE, and we also show that it demonstrates NLWE across all bipartite cuts, therefore also exhibiting the stronger version of NLWE.

Defining $|j \pm k\rangle = (|j\rangle \pm |k\rangle)/\sqrt{2}$, the set of states on a $3\times 3\times 3$ system, given in Eq. (4) of Ref. [16] as an example of what they call strong nonlocality without entanglement, is

$$
\begin{aligned}
&|\Psi_{1\pm}\rangle = |1\rangle|2\rangle|1 \pm 2\rangle, && |\Psi_{4\pm}\rangle = |1\rangle|3\rangle|1 \pm 3\rangle,\\
&|\Psi_{7\pm}\rangle = |2\rangle|3\rangle|1 \pm 2\rangle, && |\Psi_{10\pm}\rangle = |3\rangle|2\rangle|1 \pm 3\rangle,
\end{aligned}
\tag{9}
$$

and cyclic permutations of the local states in Eq. (9)—so that, for example, $|\Psi_{2\pm}\rangle = |2\rangle|1 \pm 2\rangle|1\rangle$, and generally $|\Psi_{3j+k,\pm}\rangle$ is obtained by permuting the local states in $|\Psi_{3j+1,\pm}\rangle$ $k-1$ times—along with $|i\rangle|i\rangle|i\rangle$, $i = 1,2,3$. We now demonstrate that this set of states does indeed exhibit strong NLWE, according to our definition. First, we show that this set exhibits NLWE.

Theorem 6. The set of states in Eq. (4) of Ref. [16] cannot be perfectly discriminated within $\overline{\text{LOCC}}$.

Proof. We wish to apply Theorem 3. Toward that end, we seek orthogonal pairs of local states on the first party, such that the corresponding pairs on the other parties are not orthogonal. By simple inspection, one easily finds there are many index pairs which satisfy this condition. We only need to find enough dyads to span a subspace of dimension $d_\alpha^2 - 1$; including more index pairs means more dyads, which cannot shrink the subspace that they span. Select index pairs, $(1+, 2+)$, $(1+, 10+)$, $(2+, 5+)$, $(3+, 3-)$, and $(6+, 6-)$, which lead to ten distinct dyads (including Hermitian conjugates) that (as explained in the proof of Theorem 3) must be given to the first party, those dyads being $|i\rangle\langle j|$ for all $i \neq j$ and $|1+i\rangle\langle 1-i|$, $i = 2, 3$. Since we need only eight linearly independent dyads, we omit the two other dyads that appear, which are $|1-i\rangle\langle 1+i|$, $i = 2, 3$. Consider

$$0 = \sum_{i=1}^{3} \sum_{\substack{j=1 \\ j\neq i}}^{3} c_{ij}|i\rangle\langle j| + c_1'|1+2\rangle\langle 1-2| + c_2'|1+3\rangle\langle 1-3|. \tag{10}$$

It is almost trivial to show that this is satisfied if and only if all coefficients vanish. First, take the $\langle 2|\cdots|2\rangle$ and $\langle 3|\cdots|3\rangle$ matrix elements of Eq. (10), yielding $0 = c_1'$ and $0 = c_2'$, respectively. Then, the $\langle i|\cdots|j\rangle$ matrix element for all $j \neq i$ leads to the conclusion that $c_{ij} = 0$ as well, and we are done. The chosen eight dyads are linearly independent, and by the symmetry between the three parties, we have verified that the conditions for Theorem 3 hold for the states of Eq. (9). ∎

We can also use Theorem 3 to prove this set cannot be discriminated by $\overline{\text{LOCC}}$ even if two of the parties get together and make joint measurements on their combined (two) parts of the tripartite system.

Theorem 7. The set of states in Eq. (4) of Ref. [16] exhibits *true* strong nonlocality without entanglement.

Proof. Since their combined parts have dimension equal to $d_{BC} = 9$, the proof here is slightly more challenging than that for Theorem 6, since we need to demonstrate there are $d_{BC}^2 - 1 = 80$ linearly independent dyads. Selecting this many dyads out of the hundreds to choose from is difficult to do by hand, but it is easy to write a short computer program that will perform this task for us. We do, indeed, find that there are 80 linearly independent dyads satisfying the conditions of Theorem 3. Given that we have already shown that for any one party there are $d_A^2 - 1 = 8$ linearly independent such dyads, then because of symmetry between the parties, this completes the proof. ∎

Thus, we have shown that this set of states demonstrates what we consider to be a significantly stronger "nonlocality" than was originally shown by the authors of Ref. [16].

We note that the above proof of NLWE, in the case that one views it as a tripartite system, requires only eight linearly independent dyads for each party, and it turns out that a much reduced set of states still exhibits NLWE. It is straightforward to show that the reduced set of 12 states, $|\Psi_{1\pm}\rangle$, $|\Psi_{2\pm}\rangle$, $|\Psi_{3\pm}\rangle|\Psi_{10\pm}\rangle$, $|\Psi_{11\pm}\rangle$, $|\Psi_{12\pm}\rangle$, still exhibits nonlocality without entanglement. We have checked numerically, and it turns out that this reduced set does not exhibit (our version of) strong nonlocality without entanglement. However, omitting only the three states $|i\rangle|i\rangle|i\rangle$, $i = 1, 2, 3$ does leave a strongly nonlocal set.

As another illustration of the power of Theorem 3, we use it in Appendix C to prove that GenTiles1 [14], a bipartite UPB on an $n \times n$ system for any even $n \geqslant 4$, cannot be perfectly discriminated by $\overline{\text{LOCC}}$, a result we first obtained recently in Ref. [11], where it was necessary to first determine the most general separable POVM that perfectly discriminates the set. Here, by using Theorem 3, we are able to avoid a great deal of effort since, with this approach, one need not know anything about what measurements will succeed; all one needs to know is the set of states itself.

C. Unextendible product bases consisting of the minimal number of states

We will show in this section that every unextendible product basis (UPB) [14] consisting of the minimal number of states—which we will refer to as a *minimal UPB*—cannot be discriminated perfectly by $\overline{\text{LOCC}}$. (There is a paper [17] purporting to prove that this is true for *any* unextendible product basis. We believe their proof is wrong, probably in various places, and explain our reasons for this belief in Appendix D.) When the UPB is on P parties each having local Hilbert space $\mathcal{H}_\alpha$ of dimension d_α, the minimal number of states is given as $N = \sum_\alpha (d_\alpha - 1) + 1$ [14].

We start by showing that for a minimal UPB, every set of d_α of the local states making up this UPB is linearly independent.

Lemma 1. A set of $N = \sum_\alpha (d_\alpha - 1) + 1$ pure product states on P parties is an unextendible product basis if and only if, for every α, every set of d_α of the local states on $\mathcal{H}_\alpha$, of dimension d_α, is linearly independent.

The proof can be found in Appendix E. The following lemma will also play an important role.

Lemma 2. Suppose $|\psi_k^{(\alpha)}\rangle$ and linearly independent set $\{|\phi_{kl}^{(\alpha)}\rangle\}_{l=1}^{d_\alpha}$ are states on $\mathcal{H}_\alpha$ of dimension d_α. If operator X is orthogonal to each of the d_α dyads, $|\psi_k^{(\alpha)}\rangle\langle\phi_{kl}^{(\alpha)}|$, for fixed k and $l = 1, 2, \ldots, d_\alpha$, then X has rank strictly smaller than d_α.

Proof. Orthogonality of X to each of the dyads means

$$\left\langle \phi_{kl}^{(\alpha)} \middle| X \middle| \psi_k^{(\alpha)} \right\rangle = 0, \tag{11}$$

for all l. Note that states $|\phi_{kl}^{(\alpha)}\rangle$ constitute a complete basis of $\mathcal{H}_\alpha$ for each k, so that any state $|\Phi^{(\alpha)}\rangle \in \mathcal{H}_\alpha$ can be written as a linear combination of the $|\phi_{kl}^{(\alpha)}\rangle$. Multiply Eq. (11) by arbitrary complex numbers, μ_l, and sum over l to obtain $\langle\Phi^{(\alpha)}|X|\psi_k^{(\alpha)}\rangle = 0$. Since $|\Phi^{(\alpha)}\rangle$ is arbitrary, this means that $X|\psi_k^{(\alpha)}\rangle = 0$, so X cannot be full rank, and this completes the proof. ∎

Now we are ready to prove our desired result, as codified in the following theorem.

Theorem 8. Given any unextendible product basis on P parties, $\mathcal{S} = \{|\Psi_m\rangle = \bigotimes_\alpha |\psi_m^{(\alpha)}\rangle\}$, having the minimal number of states, $N = \sum_\alpha (d_\alpha - 1) + 1$, with the αth local Hilbert space $\mathcal{H}_\alpha$ having dimension d_α, then this set of N multipartite states cannot be perfectly discriminated within $\overline{\text{LOCC}}$.

Proof. According to Theorem 2 of the previous section, if a set of N orthogonal states $|\Psi_m\rangle$ can be perfectly discriminated by $\overline{\text{LOCC}}$, then there exists a continuous path of product

operators, $Q(s)$, starting from $I_{\mathcal{H}}$, such that $\langle\Psi_m|Q(s)|\Psi_n\rangle = 0$ for all $m \neq n$. Restated in terms of dyads, we have that $Q(s)$ must be orthogonal to $N(N-1) = N\sum_\alpha (d_\alpha - 1)$ dyads $|\Psi_n\rangle\langle\Psi_m|$ for all $m \neq n$. Let us drop the parameter s and focus on understanding the conditions under which $Q = \bigotimes_\alpha Q^{(\alpha)}$ is orthogonal to all these dyads associated with the states of a minimal UPB. More specifically, since we require a continuous path starting at $I_{\mathcal{H}}$, there must be part of this path that consists of full-rank operators, so let us restrict to the case that Q, and therefore each $Q^{(\alpha)}$, is full rank.

We may partition the dyads among the parties, again as a way to distribute the job of "being orthogonal" to Q. First, suppose in a given such partition, party α is given less than $N(d_\alpha - 1)$ distinct dyads to which $Q^{(\alpha)}$ must be orthogonal. Then, there must be another party, say, β, that has been given at least $N(d_\beta - 1) + 1$ distinct dyads to which $Q^{(\beta)}$ must be orthogonal. Each of these dyads is of the form $|\psi_k^{(\beta)}\rangle\langle\psi_l^{(\beta)}|$, for some k, l. Since there are only N distinct kets $|\psi_k^{(\beta)}\rangle$ to choose from, there must be at least one k such that $|\psi_k^{(\beta)}\rangle$ is the ket appearing in d_β of the distinct dyads. Otherwise, there is no way to account for all $N(d_\beta - 1) + 1$ dyads partitioned to this party. Then, by Lemma 1 we see that this set of bras, $\langle\psi_l^{(\beta)}|$, spans $\mathcal{H}_\beta$, so by Lemma 2, $Q^{(\beta)}$ is not full rank. Therefore, since we are seeking full rank Q, we may restrict to partitions that give no one party, α, less than $N(d_\alpha - 1)$ distinct dyads.

On the other hand, if any party α is given more than $N(d_\alpha - 1)$ distinct dyads, then by the same argument just given, Q cannot be full rank. Therefore, any partition allowing for full rank Q must distribute exactly $N(d_\alpha - 1)$ distinct dyads to party α, for every α.

For any such partition allowing for Q to have full rank, we will next identify a set of $d_\alpha^2 - 1$ linearly independent dyads distributed to party α, for all α. This implies that for any partition consistent with full rank Q, there is at most one possible Q orthogonal to all $d_\alpha^2 - 1$ dyads. Since all of these dyads are orthogonal to $I_{\mathcal{H}}$, operators proportional to the latter are the only ones of full rank orthogonal to all these dyads and, as such, satisfying the constraint that $\Pi Q \Pi$ is diagonal in the (partial) basis of the $|\Psi_m\rangle$. Therefore, there can be no *continuous* path of product operators starting from $I_{\mathcal{H}}$ and satisfying this constraint. Therefore, the proof will be complete once we demonstrate the linear independence of $d_\alpha^2 - 1$ of the (local) dyads, for each partition and for each α.

Note that since there are $P \geqslant 2$ parties (and there are no UPBs on a two-qubit system), then for all α, $N > d_\alpha + 1$, so there are $N(d_\alpha - 1) > (d_\alpha + 1)(d_\alpha - 1) = d_\alpha^2 - 1$ dyads distributed to each party, α. In Appendix F, we show that the following set of dyads is linearly independent:

$$\begin{aligned}
&\left|\psi_1^{(\alpha)}\right\rangle\!\left\langle\psi_l^{(\alpha)}\right|,\ l = d_\alpha + 1, \ldots, 2d_\alpha - 1,\\
&\left|\psi_l^{(\alpha)}\right\rangle\!\left\langle\psi_1^{(\alpha)}\right|,\ l = d_\alpha + 1, \ldots, 2d_\alpha - 1,\\
&\left|\psi_k^{(\alpha)}\right\rangle\!\left\langle\phi_{kl}^{(\alpha)}\right|,\ k = 2, \ldots, d_\alpha;\ l = 1, \ldots, d_\alpha - 1,
\end{aligned} \tag{12}$$

where each $|\phi_{kl}^{(\alpha)}\rangle$ is one of the $|\psi_m^{(\alpha)}\rangle$, $m \neq k$; for each k, no two of the $|\phi_{kl}^{(\alpha)}\rangle$ correspond to the same m; and in the last line, the $|\psi_k^{(\alpha)}\rangle$ are specifically chosen to be distinct from the $|\psi_l^{(\alpha)}\rangle$, $l = d_\alpha + 1, \ldots, 2d_\alpha - 1$. Note that such a set of dyads always exists for any minimal UPB and for every partition: as argued above, each $|\psi_m^{(\alpha)}\rangle$ appears as the ket in $d_\alpha - 1$ distinct dyads given to party α, so any choice of $|\psi_1^{(\alpha)}\rangle$ appears with $d_\alpha - 1$ of the $|\psi_l^{(\alpha)}\rangle$; and since $P \geqslant 2$, we have $N \geqslant 2(d_\alpha - 1) + 1$, so there are more than the needed $d_\alpha - 1$ *other* states remaining to be chosen as the $|\psi_k^{(\alpha)}\rangle$, $k = 2, \ldots, d_\alpha$, on the third line, each of which appear in $d_\alpha - 1$ distinct dyads, which provides for the $|\phi_{kl}^{(\alpha)}\rangle$. As discussed in the preceding paragraph, this completes the proof. ■

V. CONCLUSIONS

In summary, we have applied the insights of Ref. [11] to the problem of quantum state discrimination using local operations and classical communication wherein an error is allowed but must vanish in the asymptotic limit. We obtained a lower bound on the probability of error under these circumstances and found that this lower bound provides an estimate of the correct order of magnitude relative to the known optimal error for discriminating the four Bell states. We then proved new necessary conditions that a set of mutually orthogonal states can be perfectly discriminated by $\overline{\text{LOCC}}$, and provided examples illustrating the power of these conditions, which greatly simplify what has previously been an extremely arduous task—that of determining whether a set of states can be discriminated with error that is vanishingly small. While for quantum state discrimination by $\overline{\text{LOCC}}$, the approach given in Ref. [11] required knowledge of the precise measurement the parties were trying to implement, a key advance attained here is that they only need to know the set of states they are tasked with discriminating, nothing more.

The work we have presented here and in Ref. [11] opens up a wide range of questions for further study. Since the numerical evaluation of our lower bound, Eq. (3), appears to be difficult, it would be of interest for experts to develop methods of addressing this problem. At present, the greatest lower bound that we are aware of for the domino states [2] is $p_{\text{err}} \geqslant 1.9 \times 10^{-8}$ [6]. As such, it would be interesting to know how our lower bound compares to this (perhaps surprisingly) small value.

Other avenues for further exploration include applying the ideas of Ref. [11] to (i) strengthen those results by demonstrating the need not only for continuous paths to individual measurement outcomes, but to all outcomes of a given measurement simultaneously, which we believe we have found a way to do; (ii) find ways of determining when a quantum channel can be implemented by $\overline{\text{LOCC}}$, a goal we also believe we are well on the way to achieving; and, finally, (iii) determine a lower bound on the error incurred when implementing a given quantum channel by $\overline{\text{LOCC}}$, say, for example, to transform one entangled state to another.

ACKNOWLEDGMENT

We wish to thank Dan Stahlke and Jeff Kidder for helpful discussions.

APPENDIX A: PROOF OF THEOREM 1

We begin by considering the error incurred by using any given POVM, $\mathcal{M}_Q$ as in Eq. (1), to discriminate the set of states $\mathcal{S}$, for the moment without the restriction to LOCC. Note that with $\Pi = \sum_m \sqrt{\eta_m}\Psi_m$, we have that $\mathrm{Tr}(\Pi^2) = \sum_m \eta_m \mathrm{Tr}(\Psi_m) = \sum_m \eta_m = 1$, and for any complete POVM, $\{Q_i\}$, $\sum_i \mathrm{Tr}(Q_i\Pi^2) = \mathrm{Tr}(\Pi^2) = 1$. In addition, $\Pi\Psi_m\Pi = \eta_m\Psi_m$. Defining $\widehat{Q}_i = \Pi Q_i \Pi \geqslant 0$, we have

$$
\begin{aligned}
p_{\mathrm{err}} &= 1 - \sum_i \max_m \eta_m \mathrm{Tr}(Q_i\Psi_m) = \sum_i [\mathrm{Tr}(\Pi Q_i \Pi) - \max_m \mathrm{Tr}(Q_i \Pi \Psi_m \Pi)] \\
&= \sum_i [\mathrm{Tr}(\widehat{Q}_i) - \max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)] \\
&\geqslant \sum_i \left[\frac{\mathrm{Tr}(\widehat{Q}_i) + \max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)}{2\mathrm{Tr}(\widehat{Q}_i)}\right][\mathrm{Tr}(\widehat{Q}_i) - \max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)] \\
&= \sum_i \frac{1}{2\mathrm{Tr}(\widehat{Q}_i)}([\mathrm{Tr}(\widehat{Q}_i)]^2 - [\max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)]^2) \\
&\geqslant \sum_i \frac{1}{2\mathrm{Tr}(\widehat{Q}_i)}\left[\mathrm{Tr}\big(\widehat{Q}_i^2\big) - \sum_m (\mathrm{Tr}(\widehat{Q}_i\Psi_m))^2\right] \\
&= \sum_i \frac{1}{2\mathrm{Tr}(\widehat{Q}_i)}\mathrm{Tr}\big(\widehat{Q}_i^2 - 2z_i\widehat{Q}_i + z_i^2\big) \\
&= \sum_i \frac{\mathrm{Tr}(\widehat{Q}_i)}{2}\left\|\frac{\widehat{Q}_i - z_i}{\mathrm{Tr}(\widehat{Q}_i)}\right\|^2 .
\end{aligned}
\tag{A1}
$$

The third line follows from the fact that $\max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m) \leqslant \mathrm{Tr}(\widehat{Q}_i)$, while the fifth line follows from the fact that $\mathrm{Tr}(\widehat{Q}_i^2) \leqslant [\mathrm{Tr}(\widehat{Q}_i)]^2$ for any $\widehat{Q}_i \geqslant 0$, and that $0 \leqslant [\max_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)]^2 \leqslant \sum_m [\mathrm{Tr}(\widehat{Q}_i\Psi_m)]^2$. In the sixth line, we introduce $z_i = \sum_m \mathrm{Tr}(\widehat{Q}_i\Psi_m)\Psi_m$, from which the equality to the preceding line follows from the fact that $\mathrm{Tr}(\Psi_m\Psi_n) = \delta_{mn}$. Finally, in the seventh line, we introduce the definition of the Frobenius norm, which is $\|M\|^2 = \mathrm{Tr}(M^\dagger M) = \sum_{k,l} |M_{kl}|^2$.

Let us now restrict to $\mathcal{M}_Q \in \mathrm{LOCC}_{\mathbb{N}}$, implemented by any finite-round LOCC protocol. We will represent each such protocol as a tree graph consisting of an arbitrary number of finite branches, each branch itself consisting of a sequence of nodes. Each node α corresponds to a POVM element $\tilde{Q}_\alpha$ as described elsewhere, and each such element, once normalized to unit trace, lies at a distance $\tilde{R}_\alpha$ from the similarly normalized identity operator,

$$
\tilde{R}_\alpha = \left\| \frac{I_{\mathcal{H}}}{D} - \frac{\tilde{Q}_\alpha}{\mathrm{Tr}(\tilde{Q}_\alpha)} \right\|, \tag{A2}
$$

with D the overall dimension of $\mathcal{H}$. Since it is straightforward to show that any refinement of a given measurement into rank-1 operators does not increase the error probability, we may assume that the outcomes of $\mathcal{M}_Q$ are all rank-1 operators, in which case the leaf nodes, l, of the LOCC protocol all lie at a distance $\tilde{R}_l = \sqrt{(D-1)/D}$. That is, every branch of the protocol terminates at this distance from $\mathcal{I}_{\mathcal{H}}$.

We will use the following lemma to inform a truncation of LOCC protocols (see below). Define $\Delta(Q, z) = \|(\Pi Q \Pi - z)/\mathrm{Tr}(\Pi Q \Pi)\| = \|(\widehat{Q} - z)/\mathrm{Tr}(\widehat{Q})\|$ and $\Delta(Q) := \min_{z\in\mathcal{Z}_\Psi} \Delta(Q, z)$, where z is an element of zonotope $\mathcal{Z}_\Psi$, defined in the main text. Note for later reference that every element of $\mathcal{Z}_\Psi$ is diagonal in the (partial) basis of the $|\Psi_m\rangle$. Then we have the following.

Lemma 3. Consider the set $\mathcal{P}_R$ of all positive semidefinite product operators acting on $\mathcal{H}$ and lying at distance R from the identity operator $I_{\mathcal{H}}$, in the sense of Eq. (A2), and suppose that no operator in that set lies closer than Δ_R to zonotope $\mathcal{Z}_\Psi$. That is,

$$
\Delta_R = \min_{\substack{Q\in\mathcal{P}_R \\ z\in\mathcal{Z}_\Psi}} \Delta(Q, z) = \min_{Q\in\mathcal{P}_R} \Delta(Q). \tag{A3}
$$

Suppose, in addition, there exists node $\tilde{Q}_p$, parent of its child node $\tilde{Q}_s$, both lying along a branch of a LOCC protocol implementing measurement $\mathcal{M}_Q$ and such that $\tilde{R}_p \leqslant R$ and $\tilde{R}_s \geqslant R$. Then, $\Delta(\tilde{Q}_p) \geqslant \Delta_R$ or $\Delta(\tilde{Q}_s) \geqslant \Delta_R$, or both.

Proof. As noted in the main text, the minimum over $z \in \mathcal{Z}_\Psi$ is achieved at $z = \sum_m \mathrm{Tr}(\widehat{Q}\Psi_m)\Psi_m = \sum_m \eta_m \mathrm{Tr}(Q\Psi_m)\Psi_m$, for any Q, so in the basis of states $|\Psi\rangle$, $\widehat{Q} - z$ is the same as $\widehat{Q}$ but with its diagonal elements set to zero (note that states $|\Psi_m\rangle$ may constitute an incomplete basis here, but this is not a problem since with the use of Π in its definition, the support of $\widehat{Q}$ is confined to the span of that incomplete basis).

Consider the line segment, $Q(x) = (1-x)\tilde{Q}_p + x\tilde{Q}_s$, $0 \leqslant x \leqslant 1$, which connects $\tilde{Q}_p$ to $\tilde{Q}_s$. Since this is a continuous function of x, and since $\tilde{R}_p \leqslant R$ and $\tilde{R}_s \geqslant R$, there exists y in the range $0 \leqslant y \leqslant 1$ such that $Q(y)$ is at distance R from $I_{\mathcal{H}}$, again in the sense of Eq. (A2). $Q(y) \in \mathcal{P}_R$ because we are considering a LOCC protocol, for which $\tilde{Q}_p$ and $\tilde{Q}_s$ differ only in one party's local operator. To prove the lemma, assume $\Delta(\tilde{Q}_p) < \Delta_R$ and $\Delta(\tilde{Q}_s) < \Delta_R$, which we will see leads to the

condition that $\Delta(Q(y)) < \Delta_R$, contradicting the definition of Δ_R as the minimum over $Q \in \mathcal{P}_R$. We have

$$\Delta(Q(y)) = \min_z \left\| \frac{\widehat{Q}(y) - z}{\mathrm{Tr}(\widehat{Q}(y))} \right\| = \left\| \frac{\widehat{Q}(y) - z(y)}{\mathrm{Tr}(\widehat{Q}(y))} \right\|, \tag{A4}$$

with $\widehat{Q}(y) = \Pi Q(y) \Pi$ and

$$\begin{aligned} z(y) &= \sum_m \mathrm{Tr}(\widehat{Q}(y)\Psi_m)\Psi_m \\ &= (1-y)\sum_m \mathrm{Tr}(\widehat{Q}_p\Psi_m)\Psi_m + y\sum_m \mathrm{Tr}(\widehat{Q}_s\Psi_m)\Psi_m \\ &= (1-y)z_p + yz_s, \end{aligned} \tag{A5}$$

where $\widehat{Q}_{p,s} = \Pi \tilde{Q}_{p,s} \Pi$, and z_p, z_s are defined in analogy to $z(y)$. This gives

$$\begin{aligned} [\mathrm{Tr}(\widehat{Q}(y))]^2 \Delta(Q(y))^2 &= \|(1-y)(\widehat{Q}_p - z_p) + y(\widehat{Q}_s - z_s)\|^2 \\ &= (1-y)^2 [\mathrm{Tr}(\widehat{Q}_p)]^2 \Delta_p^2 \\ &\quad + y^2 [\mathrm{Tr}(\widehat{Q}_s)]^2 \Delta_s^2 + 2y(1-y) \\ &\quad \times \mathrm{Tr}([\widehat{Q}_p - z_p][\widehat{Q}_s - z_s]). \end{aligned} \tag{A6}$$

Noting that the inner product of unit vectors cannot exceed unity, we have that

$$\begin{aligned} \mathrm{Tr}\big([\widehat{Q}_p - z_p][\widehat{Q}_s - z_s]\big) &\leqslant \sqrt{\mathrm{Tr}([\widehat{Q}_p - z_p]^2)\mathrm{Tr}([\widehat{Q}_s - z_s]^2)} \\ &= \mathrm{Tr}(\widehat{Q}_p)\mathrm{Tr}(\widehat{Q}_s)\Delta_p\Delta_s, \end{aligned} \tag{A7}$$

and then from Eq. (A6) that

$$[\mathrm{Tr}(\widehat{Q}(y))]^2 \Delta(Q(y))^2 \leqslant [(1-y)\mathrm{Tr}(\widehat{Q}_p)\Delta_p + y\mathrm{Tr}(\widehat{Q}_s)\Delta_s]^2. \tag{A8}$$

By assumption, $\Delta_p < \Delta_R$ and $\Delta_s < \Delta_R$. This leads to the conclusion that

$$\begin{aligned} [\mathrm{Tr}(\widehat{Q}(y))]^2 \Delta(Q(y))^2 &< [(1-y)\mathrm{Tr}(\widehat{Q}_p) + y\mathrm{Tr}(\widehat{Q}_s)]^2 \Delta_R^2 \\ &= [\mathrm{Tr}(\widehat{Q}(y))]^2 \Delta_R^2, \end{aligned} \tag{A9}$$

or $\Delta(Q(y)) < \Delta_R$, a contradiction. This completes the proof. ■

This lemma provides a way to truncate a given finite-round LOCC protocol such that every branch that reaches a distance $R \leqslant \sqrt{(D-1)/D}$ from $I_{\mathcal{H}}$ is left with a (new) leaf node, $\tilde{Q}_\alpha$, for which $\Pi \tilde{Q}_\alpha \Pi$ is a distance of at least Δ_R from $\mathcal{Z}_\Psi$. Recall that, since we can restrict consideration to rank-1 measurements, all leaf nodes lie at distance $R = \sqrt{(D-1)/D}$, and every branch corresponds to a continuous path starting at distance $R = 0$. Therefore, for each branch, identify the *first* node $\tilde{Q}_\alpha$ that is a distance at least R from $I_{\mathcal{H}}$. Truncate this branch at its parent Q_p, unless $\tilde{Q}_\alpha$ is at a distance equal to R or $\Delta_p < \Delta_R$, in either of which cases, truncate at $\tilde{Q}_\alpha$, for which the lemma tells us $\Delta_\alpha \geqslant \Delta_R$. Now we have a truncated tree for which

$$\Delta_\alpha = \left\| \frac{\Pi \tilde{Q}_\alpha \Pi - \tilde{z}_\alpha}{\mathrm{Tr}(\tilde{Q}_\alpha)} \right\| \geqslant \Delta_R \tag{A10}$$

for all leaf nodes, $\tilde{Q}_\alpha$, in the truncation, and $\tilde{z}_\alpha = \sum_m \eta_m \mathrm{Tr}(\tilde{Q}_\alpha \Psi_m)\Psi_m$. Each such leaf node has a set of descendants in the original protocol, which we index as $\mathcal{L}_\alpha = \{l | Q_l$ is a leaf node descendant of $\tilde{Q}_\alpha$ in the original protocol$\}$, unless $\tilde{Q}_\alpha$ is itself a leaf node in the original protocol, in which case we instead define $\mathcal{L}_\alpha = \{l | Q_l$ is *the* leaf node $\tilde{Q}_\alpha$ in the original protocol$\}$. Then, $\tilde{Q}_\alpha = \sum_{l \in \mathcal{L}_\alpha} Q_l$, and from Eq. (A1) we have

$$\begin{aligned} p_{\mathrm{err}} &\geqslant \sum_l \frac{\mathrm{Tr}(\Pi^2 Q_l)}{2} \left\| \frac{\Pi Q_l \Pi - z_l}{\mathrm{Tr}(\Pi^2 Q_l)} \right\|^2 \\ &\geqslant \sum_\alpha \sum_{l \in \mathcal{L}_\alpha} \frac{\|\Pi Q_l \Pi - z_l\|^2}{2\mathrm{Tr}(\Pi^2 Q_l)} \\ &= \sum_\alpha \frac{\left\| \sum_{i \in \mathcal{L}_\alpha} (\Pi Q_l \Pi - z_l) \right\|^2}{2 \sum_{i \in \mathcal{L}_\alpha} \mathrm{Tr}(\Pi^2 Q_l)} \\ &= \sum_\alpha \frac{\left\| \Pi \tilde{Q}_\alpha \Pi - \tilde{z}_\alpha \right\|^2}{2\mathrm{Tr}(\Pi^2 \tilde{Q}_\alpha)} \\ &= \sum_\alpha \frac{\mathrm{Tr}(\Pi^2 \tilde{Q}_\alpha)}{2} \Delta_\alpha \\ &\geqslant \sum_\alpha \frac{\mathrm{Tr}(\Pi^2 \tilde{Q}_\alpha)}{2} \Delta_R \\ &= \frac{1}{2} \min_{\substack{Q \in \mathcal{P}_R \\ z \in \mathcal{Z}_\Psi}} \left\| \frac{\Pi Q \Pi - z}{\mathrm{Tr}(\Pi^2 Q)} \right\|^2, \end{aligned} \tag{A11}$$

where the second line (and, slightly indirectly, last line) follows since the sum over leaves descended from all of the $\tilde{Q}_\alpha$ includes all leaves in the original protocol; the step going from line 2 to line 3 is proven in Appendix B; and $\tilde{z}_\alpha$ is defined below Eq. (A10). The second-to-last line follows from Lemma 3, while the last line is a result of the fact that $\tilde{Q}_\alpha$ is a product operator (since it is an intermediate outcome of a LOCC protocol), along with $\sum_\alpha \tilde{Q}_\alpha = I_{\mathcal{H}}$.

Thus, we have derived the expression in Theorem 1, which lower-bounds p_{err} for any finite number of rounds, r. Since

this result is independent of r, it continues to hold in the limit $r \to \infty$, and this completes the proof.

APPENDIX B: PROOF OF LINE 3 IN EQ. (A11)

Here we prove that

$$\sum_{l\in\mathcal{L}_\alpha} \frac{\|\widehat{Q}_l - z_l\|^2}{\mathrm{Tr}(\widehat{Q}_l)} \geqslant \frac{\|\sum_{l\in\mathcal{L}_\alpha}(\widehat{Q}_l - z_l)\|^2}{\sum_{l\in\mathcal{L}_\alpha}\mathrm{Tr}(\widehat{Q}_l)}, \tag{B1}$$

with $\widehat{Q}_l = \Pi Q_l \Pi$. Let $t_l = \mathrm{Tr}(\widehat{Q}_l) > 0$. Then, defining $M^{(l)} = \widehat{Q}_l - z_l$ and denoting its matrix elements in any chosen basis as $M^{(l)}_{\mu\nu}$, consider

$$\begin{aligned}\mathcal{S} &\equiv \sum_{l\in\mathcal{L}_\alpha} \frac{\|\widehat{Q}_l - z_l\|^2}{\mathrm{Tr}(\widehat{Q}_l)} - \frac{\left\|\sum_{l\in\mathcal{L}_\alpha}(\widehat{Q}_l - z_l)\right\|^2}{\sum_{l\in\mathcal{L}_\alpha}\mathrm{Tr}(\widehat{Q}_l)} \\ &= \sum_{l\in\mathcal{L}_\alpha} \frac{\sum_{\mu\nu}\left|M^{(l)}_{\mu\nu}\right|^2}{t_l} - \frac{\sum_{\mu\nu}\left|\sum_{l\in\mathcal{L}_\alpha} M^{(l)}_{\mu\nu}\right|^2}{\sum_{l\in\mathcal{L}_\alpha} t_l} \equiv \sum_{\mu\nu}\mathcal{S}_{\mu\nu}.\end{aligned} \tag{B2}$$

We will show that each term, $\mathcal{S}_{\mu\nu}$, is non-negative. To simplify notation, let us replace $l \in \mathcal{L}_\alpha$ by l and take the restriction on the sums as implicit. Multiply by $\sum_j t_j > 0$ and $\prod_k t_k > 0$ to obtain

$$\begin{aligned}\mathcal{S}_{\mu\nu} &= \sum_j t_j \sum_l \left|M^{(l)}_{\mu\nu}\right|^2 \prod_{k\neq l} t_k - \left|\sum_l M^{(l)}_{\mu\nu}\right|^2 \prod_k t_k \\ &= \sum_l \left(\prod_{k\neq l} t_k\right)\left(\sum_{j\neq l} t_j + t_l\right)\left|M^{(l)}_{\mu\nu}\right|^2 - \sum_l \left(\left|M^{(l)}_{\mu\nu}\right|^2 + \sum_{j\neq l} M^{(l)*}_{\mu\nu} M^{(j)}_{\mu\nu}\right)\prod_k t_k \\ &= \sum_l \left(\prod_{k\neq l} t_k\right)\sum_{j\neq l} t_j \left|M^{(l)}_{\mu\nu}\right|^2 - \sum_l \sum_{j\neq l} M^{(l)*}_{\mu\nu} M^{(j)}_{\mu\nu} \prod_k t_k \\ &= \sum_l \sum_{j\neq l} \left(\prod_{k\neq l,j} t_k\right)\left[t_j^2 \left|M^{(l)}_{\mu\nu}\right|^2 - t_l t_j M^{(l)*}_{\mu\nu} M^{(j)}_{\mu\nu}\right] \\ &= \frac{1}{2}\sum_l \sum_{j\neq l} \left(\prod_{k\neq l,j} t_k\right)\left[t_j^2 \left|M^{(l)}_{\mu\nu}\right|^2 - t_l t_j M^{(l)*}_{\mu\nu} M^{(j)}_{\mu\nu} + t_l^2 \left|M^{(j)}_{\mu\nu}\right|^2 - t_j t_l M^{(j)*}_{\mu\nu} M^{(l)}_{\mu\nu}\right] \\ &= \frac{1}{2}\sum_l \sum_{j\neq l} \left(\prod_{k\neq l,j} t_k\right)\left|t_j M^{(l)}_{\mu\nu} - t_l M^{(j)}_{\mu\nu}\right|^2,\end{aligned} \tag{B3}$$

which is manifestly non-negative. Therefore, each $\mathcal{S}_{\mu\nu} \geqslant 0$ implies that $\mathcal{S} \geqslant 0$ as well, and this completes the proof.

APPENDIX C: GenTiles1 CANNOT BE PERFECTLY DISCRIMINATED BY $\overline{\mathrm{LOCC}}$

As an illustration of how these results may be applied, we use Theorem 3 to prove that GenTiles1 [14], a bipartite UPB on an $n \times n$ system for any even $n \geqslant 4$, cannot be perfectly discriminated by $\overline{\mathrm{LOCC}}$, a result we obtained recently in Ref. [11]. The states in this UPB are

$$\begin{aligned}|V_{km}\rangle &= \frac{1}{\sqrt{n}}|k\rangle \otimes \sum_{j=0}^{\frac{n}{2}-1} \omega^{jm}|j + k + 1 \ (\mathrm{mod}\ n)\rangle, \\ |H_{km}\rangle &= \frac{1}{\sqrt{n}}\sum_{j=0}^{\frac{n}{2}-1} \omega^{jm}|j + k \ (\mathrm{mod}\ n)\rangle \otimes |k\rangle, \\ |F\rangle &= \frac{1}{n}\sum_{ij=0}^{n-1} |i\rangle \otimes |j\rangle,\end{aligned} \tag{C1}$$

with $\omega = e^{4\pi i/n}$, $m = 1, \ldots, n/2 - 1$, and $k = 0, \ldots, n-1$. Notice that the system is symmetric under interchange of parties, so if we can show there exists a set of dyads, each of which is traceless on one party but not on the other, and which on the first party spans a subspace of dimension $n^2 - 1$, then this will also hold for the other party, and then by Theorem 3, we will have demonstrated the desired result. The local states on the first party are

$$\begin{aligned}|h_{km}\rangle &= \sum_{j=0}^{\frac{n}{2}-1} \omega^{jm}|j + k \ (\mathrm{mod}\ n)\rangle, \\ |f\rangle &= \sum_{j=0}^{n-1} |j\rangle,\end{aligned} \tag{C2}$$

along with the standard basis states, $|i\rangle$.

Following a bit of guesswork and playing around numerically looking for patterns on systems with several smallish values of n, we have identified the following set of $n^2 - 1$ linearly independent, traceless dyads on the

first party:

$$\begin{aligned}
&(1)\ |i\rangle\langle j|\ \ i,j=0,\ldots,n-1;\ \ j\neq i, i+\frac{n}{2}(\mathrm{mod} n),\\
&(2)\ |f\rangle\langle h_{km}| \text{ and } |h_{km}\rangle\langle f|\ k=0, m=1,\ldots,\frac{n}{2}-1 \text{ and } k=1, m=1;\ \text{and } |f\rangle\langle h_{k1}|\ \ k=2,\ldots,\frac{n}{2},\\
&(3)\ |h_{km}\rangle\langle h_{kl}|\ \ k=1, m=1, l=2,\ldots,\frac{n}{2}-1 \text{ and } k=1, m=2, l=1,\\
&(4)\ |h_{01}\rangle\langle n/2|.
\end{aligned} \tag{C3}$$

Set 1 corresponds to orthogonality of $|H_{im}\rangle$, $|H_{jl}\rangle$, which are not orthogonal on the second party for at least some values of m, l—these are $n(n-2)$ dyads. Set 2 corresponds to orthogonality of $|F\rangle$, $|H_{km}\rangle$, which again, are not orthogonal on the second party—these are $2(n/2-1)+2+n/2-1=3n/2-1$. Set 3 is for $|H_{km}\rangle$, $|H_{kl}\rangle$ (same k)—$n/2-1$ dyads. Set 4 is for H_{01}, $|V_{\frac{n}{2}}m\rangle$—which is one last dyad. The total number of these dyads is n^2-1, as required, and none of these are orthogonal on the second party. They are linearly independent if there is no set of nonzero coefficients satisfying the following equation:

$$\begin{aligned}
0=&\sum_{\substack{i,j=0\\ j\neq i,i+n/2\ (\mathrm{mod}\ n)}} c_{ij}|i\rangle\langle j|+\sum_{m=1}^{n/2-1}(f_{0m}|f\rangle\langle h_{0m}|+f'_{0m}|h_{0m}\rangle\langle f|)+f_{11}|f\rangle\langle h_{11}|+f'_{11}|h_{11}\rangle\langle f|\\
&+\sum_{k=2}^{n/2} f_{k1}|f\rangle\langle h_{k1}|+\sum_{m=2}^{n/2-1} g_{1m}|h_{11}\rangle\langle h_{1m}|+g_{21}|h_{12}\rangle\langle h_{11}|+h|h_{01}\rangle\langle n/2|.
\end{aligned} \tag{C4}$$

We next show that this latter equation is satisfied if and only if all its coefficients vanish, which proves that the set of dyads listed in Eqs. (C3) are linearly independent, spanning a space of dimension n^2-1. By the symmetry of the parties for GenTiles1, this conclusion holds for the second party, as well. Thus, by Theorem 3, GenTiles1 cannot be perfectly discriminated within $\overline{\mathrm{LOCC}}$ for any value of n.

We start by taking the $\langle n/2+l|\cdots|n/2+l\rangle$ matrix elements of Eqs. (C3) for $l=1,\ldots,n/2-1$. Since for these values of l, $\langle n/2+l|h_{km}\rangle=0$ for $k=0,1$, and since the terms involving c_{ij} only include nondiagonal dyads ($j\neq i$), these matrix elements of Eq. (C4) yield

$$0=\sum_{k=2}^{n/2} f_{k1}\langle h_{k1}|n/2+l\rangle=\sum_{k=l+1}^{n/2} f_{k1}\omega^{k-l}, \tag{C5}$$

and we have used the facts that $\langle h_{k1}|n/2+l\rangle$ vanishes unless $k\leqslant n/2+l\leqslant k+n/2-1$ (mod n), in which case it is equal to $\omega^{k-n/2-l}$, and $\langle i|f\rangle=1$ for all i. Beginning with $l=n/2-1$, this reduces to $f_{n/2,1}=0$. Then, $l=n/2-2$ yields $f_{n/2-1,1}=0$, and continuing on step-by-step, reducing l by unity each time, we find that $f_{k1}=0$ for all $k=2,\ldots,n/2$.

Noting that the terms involving c_{ij} also do not include $j=i+n/2$ (mod n), we next take $\langle n/2|\cdots|0\rangle$ to obtain

$$0=\sum_{m=1}^{n/2-1} f_{0m}+f'_{11}\omega^{-1}, \tag{C6}$$

and then $\langle n/2+l|\cdots|l\rangle$, $l=1,\ldots,n/2-1$, to obtain

$$0=\sum_{m=1}^{n/2-1} f_{0m}\omega^{-ml}+f_{11}\omega^{1-l}. \tag{C7}$$

Using $\sum_{l=0}^{n/2-1}\omega^{-ml}=0$ for all $m\neq 0$, we can add Eq. (C6) to the sum of all versions (different l) of Eq. (C7) to obtain $f'_{11}=f_{11}\omega^2$. Similarly, from $\langle 0|\cdots|n/2\rangle$ we get

$$0=\sum_{m=1}^{n/2-1} f'_{0m}+f_{11}\omega+h, \tag{C8}$$

and from $\langle l|\cdots|n/2+l\rangle$, $l=1,\ldots,n/2-1$,

$$0=\sum_{m=1}^{n/2-1} f'_{0m}\omega^{ml}+f'_{11}\omega^{l-1}=\sum_{m=1}^{n/2-1} f'_{0m}\omega^{ml}+f_{11}\omega^{l+1}. \tag{C9}$$

Adding Eq. (C8) and all $n/2-1$ instances of Eq. (C9) leaves $h=0$.

Looking now at the diagonal element, $\langle 0|\cdots|0\rangle$, we have

$$0=\sum_{m=1}^{n/2-1}(f_{0m}+f'_{0m}). \tag{C10}$$

Adding Eq. (C10) and all instances of Eq. (C7) and Eq. (C9), we obtain

$$0=\sum_{l=0}^{n/2-1}\sum_{m=1}^{n/2-1}(f_{0m}\omega^{-ml}+f'_{0m}\omega^{ml})+\sum_{l=1}^{n/2-1} f_{11}\omega(\omega^l+\omega^{-l}), \tag{C11}$$

which reduces to $0=-2f_{11}\omega$, so $f_{11}=0$, implying [see below Eq. (C7)] $f'_{11}=0$. Now Eq. (C7) can be written (with $f_{11}=0$) as $M\vec{f}_0=\vec{0}$, with the elements of $\vec{f}_0$ being $(\vec{f}_0)_m=f_{0m}$, and those of M are given by $M_{lm}=\omega^{-ml}$, $m,l\neq 0$. If we add a column of all ones to obtain matrix M', then it is straightforward to see that $M'M'^{\dagger}$ is proportional to the $(n/2-1)$-dimensional identity operator. Thus, the rank of M'

is $n/2-1$. However, the sum of all columns of M' vanishes, implying that the column rank of M' is the same as that of M. This, in turn, implies that the rank of M is also $n/2-1$, so M is invertible. Therefore, we have that $\vec{f}_0 = \vec{0}$, and $f_{0m} = 0$ for all $m = 1, \ldots, n/2-1$.

Similarly, Eq. (C9) can be written as $M\vec{f}_0' = 0$, with the same M and $(\vec{f}_0')_m = f_{0m}'$, and thus $f_{0m}' = 0$ for all $m = 1, \ldots, n/2-1$, as well. Thus, the only nonzero coefficients left are the c's and g's.

For the g's, consider all remaining diagonal elements of our constraint equations, those not previously used in the preceding arguments, $\langle l|\cdots|l\rangle$, $l = 1, \ldots, n/2-1$. Given our preceding results, these yield

$$0 = \sum_{m=2}^{n/2-1} g_{1m}\omega^{-(m-1)l} + g_{21}\omega^{l}. \tag{C12}$$

Defining $\vec{g}^T = (g_{21}\, g_{1,n/2-1}\, g_{1,n/2-2} \cdots g_{13}\, g_{12})$, this last equation may be written as $M^*\vec{g}$, with M the same matrix as has appeared above. Therefore, each entry of $\vec{g}$ vanishes, and the only nonzero coefficients remaining are the c_{ij}.

That is,

$$0 = \sum_{\substack{i,j=0 \\ j\neq i, i+n/2 \pmod n}} c_{ij}|i\rangle\langle j|, \tag{C13}$$

and it is clear that $c_{ij} = 0$ for all remaining i, j, as well. Thus, we have that Eq. (C4) can be satisfied if and only if all of the coefficients appearing there vanish, showing that the set of dyads in Eq. (C3) is linearly independent, which is what we set out to prove.

APPENDIX D: WHY REFERENCE [17] IS WRONG

Here we argue that the results of Ref. [17] purporting to prove that any unextendible product basis exhibits NLWE is wrong. It is probably wrong in various places, including the assumption that A in their Eq. (4), the key part of which reads as

$$\max_{i\neq j}(2\lambda^2\delta'\langle\phi_i|A|\phi_j\rangle + \lambda^2\delta'^2\langle\phi_i|A^\dagger A|\phi_j\rangle) > \max_{i\neq j} 2\lambda^2\delta'\langle\phi_i|A|\phi_j\rangle,$$

must be a positive semidefinite operator: $E = \lambda(I+\delta' A)$ is positive semidefinite, but there is no apparent reason why A needs to be. It is all well and good to use the polar decomposition of $S = EU$ to obtain $E \geqslant 0$, but this implies $S = \lambda(U+\delta' A')$, and there is no reason that (with the starting point being S) the polar decomposition of A' should yield the same U as that for S. Put more simply, $E \geqslant 0$ being close to (proportional to) the identity operator only means that the operator A, seen above, is small; to maintain generality, one must allow for indefinite (and even negative semidefinite) A. In other words, it is wrong to assume that A is positive semidefinite. More importantly, the inequality in their Eq. (4) is unjustified, even if one maximizes over the absolute value of the off-diagonal matrix element of $E^\dagger E$, instead of (as it is written in their paper) maximizing over the off-diagonal matrix element itself (which may not be a real number, implying that this maximization makes no sense). The reason is that off-diagonal elements of positive semidefinite operators (such as $A^\dagger A$ in this equation) need not be positive (this problem arises even when considering the absolute value of the off-diagonal matrix element, as we have just suggested must be done). Indeed, these off-diagonal elements may well be complex numbers. Therefore, the inequality in their Eq. (4) could very easily be in the opposite direction, thus failing to provide the *critical* lower bound on the degree to which the states remain orthogonal.

The argument given in Ref. [17] has been criticized previously [7] for a different technical point, a criticism that we do not understand. We do take issue with that same technical point, however, but for different reasons. Below Eq. (16) of Ref. [17], for the case $c_N \to 0$, the claim that Eqs. (5) and (6) lead to $\epsilon \to 0$ appears to have no basis. It is not entirely clear how they arrive at this conclusion, but they seem to be assuming that if the off-diagonal elements of $O(N)$ all vanish, then its diagonal elements must all be equal to each other, an assumption for which we see no justification. In any case, if their Eq. (4) is wrong, as we have suggested above, then it is almost certain that the analogous Eq. (15) is also wrong, calling into question the validity of the critical Eq. (16).

Finally, given the fact that there are several apparent erroneous assumptions made in the proof—along with numerous apparent typographical errors and omissions of detailed explanations of their reasoning—one is left with little confidence in their conclusions, even if one could follow the proof in detail, which is not an easy task.

APPENDIX E: PROOF OF LEMMA 1

Proof. We prove the "only if" direction by way of contradiction. Thus, suppose we have a minimal UPB and there exists party α and a linearly *dependent* set of d_α local states, say, $\{|\psi_m^{(\alpha)}\rangle\}_{m=1}^{d_\alpha}$. Then, there exists a partition of the entire set of N states such that $\{|\Psi_m\rangle\}_{m=1}^{d_\alpha}$ are placed with party α, and all the other parties, β, are each given $d_\beta - 1$ states. Note that for every party, the local states corresponding to this partition fail to span the entire local Hilbert space. Therefore, for each party β, we can identify one additional local state, $|\phi^{(\beta)}\rangle$ orthogonal to all the $d_\beta - 1$ local states apportioned to party β for $\beta \neq \alpha$, and since the d_α local states partitioned to party α also do not span the local Hilbert space, we can do the same for party α with state $|\phi^{(\alpha)}\rangle$. Taking the tensor product of these P local states, we obtain a product state $\bigotimes_\mu |\phi^{(\mu)}\rangle$, orthogonal to all N of the original states of the UPB, extending the UPB and contradicting the fact that it is a UPB to begin with. This completes the proof of the "only if" part.

To prove the other direction, simply notice that, for every partition of the states among the parties, there is at least one party that is given at least d_α local states. By assumption, the set of states given to that party is linearly independent, spanning $\mathcal{H}_\alpha$, and thus, there can be no state on $\mathcal{H}_\alpha$ orthogonal to those d_α local states. Therefore, one cannot extend the original set of states by adding one more orthogonal product state. That is, the set is unextendible. ∎

APPENDIX F: LINEAR INDEPENDENCE OF DYADS FOR THEOREM 8

Here, we show that the set of dyads in Eq. (12) is linearly independent. To this end, consider

$$0=\sum_{l=1}^{d_\alpha-1}\left(\sum_{k=2}^{d_\alpha}c_{kl}\big|\psi_k^{(\alpha)}\big\rangle\big\langle\phi_{kl}^{(\alpha)}\big|+c_{1l}\big|\psi_1^{(\alpha)}\big\rangle\big\langle\psi_{d_\alpha+l}^{(\alpha)}\big|+c_{d_\alpha+1,l}\big|\psi_{d_\alpha+l}^{(\alpha)}\big\rangle\big\langle\psi_1^{(\alpha)}\big|\right). \tag{F1}$$

Since according to Lemma 1, $|\psi_k^{(\alpha)}\rangle$, $k=1,\ldots,d_\alpha$, are a basis of $\mathcal{H}_\alpha$, we may expand

$$\big|\psi_{d_\alpha+l}^{(\alpha)}\big\rangle=\sum_{k=1}^{d_\alpha}\mu_{kl}\big|\psi_k^{(\alpha)}\big\rangle, \tag{F2}$$

and then Eq. (F1) becomes

$$0=\sum_{l=1}^{d_\alpha-1}\left[\sum_{k=2}^{d_\alpha}\big|\psi_k^{(\alpha)}\big\rangle\big(c_{kl}\big\langle\phi_{kl}^{(\alpha)}\big|+c_{d_\alpha+1,l}\mu_{kl}\big\langle\psi_1^{(\alpha)}\big|\big)+\big|\psi_1^{(\alpha)}\big\rangle\left(\sum_{k=1}^{d_\alpha}c_{1l}\mu_{kl}^*\big\langle\psi_k^{(\alpha)}\big|+c_{d_\alpha+1,l}\mu_{1l}\big\langle\psi_1^{(\alpha)}\big|\right)\right]. \tag{F3}$$

Since $|\psi_k^{(\alpha)}\rangle$, $k=1,\ldots,d_\alpha$, are linearly independent, each of their coefficients in the preceding equation must vanish separately. That is,

$$0=\sum_{l=1}^{d_\alpha-1}\big(c_{kl}\big\langle\phi_{kl}^{(\alpha)}\big|+c_{d_\alpha+1,l}\mu_{kl}\big\langle\psi_1^{(\alpha)}\big|\big),\ k=2,\ldots,d_\alpha, \tag{F4}$$

and

$$0=\sum_{l=1}^{d_\alpha-1}\left(\sum_{k=1}^{d_\alpha}c_{1l}\mu_{kl}^*\big\langle\psi_k^{(\alpha)}\big|+c_{d_\alpha+1,l}\mu_{1l}\big\langle\psi_1^{(\alpha)}\big|\right)=\sum_{l=1}^{d_\alpha-1}\left[\sum_{k=2}^{d_\alpha}c_{1l}\mu_{kl}^*\big\langle\psi_k^{(\alpha)}\big|+(c_{d_\alpha+1,l}\mu_{1l}+c_{1l}\mu_{1l}^*)\big\langle\psi_1^{(\alpha)}\big|\right]. \tag{F5}$$

Noting that the set of d_α states $\{\langle\psi_1^{(\alpha)}|,\{\langle\phi_{kl}^{(\alpha)}|\}_{l=1}^{d_\alpha-1}\}$ is also linearly independent for each k, the coefficients of these states must each vanish in Eq. (F4), implying $c_{kl}=0$ for all $k=2,\ldots,d_\alpha$ and all $l=1,\ldots,d_\alpha-1$. In addition,

$$\sum_{l=1}^{d_\alpha-1}c_{d_\alpha+1,l}\mu_{kl}=0,\ k=2,\ldots,d_\alpha. \tag{F6}$$

Considering Eq. (F2), we find

$$\sum_{l=1}^{d_\alpha-1}c_{d_\alpha+1,l}\big|\psi_{d_\alpha+l}^{(\alpha)}\big\rangle=\sum_{k=1}^{d_\alpha}\sum_{l=1}^{d_\alpha-1}c_{d_\alpha+1,l}\mu_{kl}\big|\psi_k^{(\alpha)}\big\rangle=\left(\sum_{l=1}^{d_\alpha-1}c_{d_\alpha+1,l}\mu_{1l}\right)\big|\psi_1^{(\alpha)}\big\rangle, \tag{F7}$$

and we have used Eq. (F6). This implies linear dependence of the d_α states $|\psi_1^{(\alpha)}\rangle$ and $|\psi_{d_\alpha+l}^{(\alpha)}\rangle$, $l=1,\ldots,d_\alpha-1$, a contradiction, unless $c_{d_\alpha+1,l}$ vanishes for all l. These results reduce Eq. (F5) to

$$0=\sum_{l=1}^{d_\alpha-1}c_{1l}\left(\sum_{k=2}^{d_\alpha}\mu_{kl}^*\big\langle\psi_k^{(\alpha)}\big|+\mu_{1l}^*\big\langle\psi_1^{(\alpha)}\big|\right). \tag{F8}$$

Once again, the coefficient of each $|\psi_k^{(\alpha)}\rangle$ must vanish separately, implying $\sum_l c_{1l}\mu_{kl}=0$ for all k. Similarly to what we just did in Eq. (F7), consider

$$\sum_{l=1}^{d_\alpha-1}c_{1l}^*\big|\psi_{d_\alpha+l}^{(\alpha)}\big\rangle=\sum_{k=1}^{d_\alpha}\sum_{l=1}^{d_\alpha-1}c_{1l}^*\mu_{kl}\big|\psi_k^{(\alpha)}\big\rangle=0, \tag{F9}$$

and we have used Eq. (F8). This implies that the set of $d_\alpha-1$ states in the sum on the left is linearly dependent, which contradicts Lemma 1 unless $c_{1l}=0$ for all l.

Collecting all these results, we see that the sum of d_α^2-1 dyads in Eq. (F1) vanishes if and only if each of the c_{mn} appearing there vanishes identically. That is, those d_α^2-1 dyads constitute a linearly independent set. As argued in the paragraph preceding Eq. (12), this completes the proof.

[1] R. B. Griffiths, Found. Phys. **41**, 705 (2011).
[2] 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).
[3] J. A. Bergou, J. Phys.: Conf. Ser. **84**, 012001 (2007).
[4] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
[5] E. Chitambar and M.-H. Hsieh, J. Math. Phys. **55**, 112204 (2014).
[6] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, Commun. Math. Phys. **323**, 1121 (2013).
[7] M. Kleinmann, H. Kampermann, and D. Bruß, Phys. Rev. A **84**, 042326 (2011).
[8] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[9] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[10] S. M. Cohen, Phys. Rev. A **75**, 052313 (2007).
[11] S. M. Cohen, Phys. Rev. A **105**, 022207 (2022).
[12] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Commun. Math. Phys. **328**, 303 (2014).
[13] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, IEEE Trans. Inf. Theory **61**, 3593 (2015).
[14] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Commun. Math. Phys. **238**, 379 (2003).
[15] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[16] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Phys. Rev. Lett. **122**, 040403 (2019).
[17] S. De Rinaldis, Phys. Rev. A **70**, 022309 (2004).