Multicopy Adaptive Local Discrimination: Strongest Possible Two-Qubit Nonlocal Bases

Manik Banik
School of Physics, IISER Thiruvananthapuram, Vithura, Kerala 695551, India

Tamal Guha, Mir Alimuddin, and Guruprasad Kar
Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata 700108, India

Saronath Halder
Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211019, India

Some Sankar Bhattacharya
Department of Computer Science, The University of Hong Kong, Pokfulam Road 999077, Hong Kong

(Received 19 November 2020; accepted 5 May 2021; published 28 May 2021)

Ensembles of composite quantum states can exhibit nonlocal behavior in the sense that their optimal discrimination may require global operations. Such an ensemble containing N pairwise orthogonal pure states, however, can always be perfectly distinguished under an adaptive local scheme if $(N-1)$ copies of the state are available. In this Letter, we provide examples of orthonormal bases in two-qubit Hilbert space whose adaptive discrimination require three copies of the state. For this composite system, we analyze multicopy adaptive local distinguishability of orthogonal ensembles in full generality which, in turn, assigns varying nonlocal strength to different such ensembles. We also come up with ensembles whose discrimination under an adaptive separable scheme require less numbers of copies than adaptive local schemes. Our construction finds important application in multipartite secret sharing tasks and indicates toward an intriguing superadditivity phenomenon for locally accessible information.

DOI: 10.1103/PhysRevLett.126.210505

Introduction.—The second quantum revolution aims to harness individual quantum systems for storing, transferring, and manipulating information [1]. In many of the information protocols, the elementary step is reliable decoding of the classical information encoded in some physical system. When involved systems are quantum, several interesting observations appear that, otherwise, are not present in the classical world. For instance, the classical message encoded in the states of a composite quantum system may not be completely retrieved under local quantum operations and classical communications (LOCC) among the spatially separated subsystems. Such a set of states is called nonlocal as their optimal discrimination requires global operation(s) on the composite system. In a seminal paper [2], Bennett *et al.* provided examples of orthonormal bases in $(\mathbb{C}^3)^{\otimes 2}$ and $(\mathbb{C}^2)^{\otimes 3}$ that are not perfectly distinguishable under LOCC. These examples are quite striking as they contain only product states and, hence, introduced the phenomenon of "quantum nonlocality without entanglement." For the simplest multipartite system $(\mathbb{C}^2)^{\otimes 2}$, an example of a LOCC indistinguishable ensemble was first identified in [3]. Unlike the examples of Bennett *et al.*, an orthogonal ensemble in $(\mathbb{C}^2)^{\otimes 2}$ must contain entangled state(s) for local indistinguishability [4]. Historically, a difference between global and local distinguishability for a two-qubit ensemble containing only product states was conjectured by Peres and Wootters [5]. Importantly, Peres-Wootters' ensemble contains nonorthogonal states, and recently, their conjecture has been proven to be true [6]. The results in [2–5] initiated a plethora of studies on the local state discrimination problem that turn out to be deeply interlinked with quantum entanglement theory (see [7–24] and references therein). Subsequently, local indistinguishability has been identified as a crucial primitive for cryptography protocols, such as quantum data hiding [25–27] and quantum secret sharing [28–30]; it also underlies the nonzero gap between single-shot and multishot classical capacities of noisy quantum channels [31] and has been shown to have foundational appeal [32–34]. The mathematical difficulty of characterizing the class of LOCC operations [35] motivates researchers to address the state discrimination problem with a larger class of operations, namely, separable superoperator (SEP) and/or the set of operations that map positive partial transposition (PPT) states to PPT states [36–40].

The problem of local discrimination discussed so far considers identifying the unknown state from a single copy of the system. Given many copies of the state $|\psi_i\rangle^{\otimes k}$, the probability of knowing the state $|\psi_i\rangle$ and,

consequently, guessing the classical message 'i' increases; $|\psi\rangle_i$ is sampled from some known ensemble $\mathcal{E}_N \equiv \{p_i, |\psi_i\rangle | p_i\rangle 0 \,\&\, \sum p_i = 1\}_{i=1}^N$. If there is no limitation on the number k, then the state can be identified exactly even without any prior knowledge from which ensemble it is sampled. This fact, known as local tomography, has been axiomatized by many authors in physical reconstruction of Hilbert space quantum theory [41–43]. However, given the prior knowledge of the orthogonal pure states ensemble $\mathcal{E}_N$, only $(N-1)$ copies are sufficient for perfect local discrimination [8,16]. In this multicopy scenario, the parties are allowed to invoke adaptive as well as nonadaptive strategies for discrimination.

Definition 1.—(Local adaptive strategy) Given multiple copies of the state in an adaptive strategy, each of the copies are addressed individually, and the maximal possible information regarding the unknown state is extracted through LOCC. Depending on the knowledge obtained from the former copies, strategies on the later copies are modified adaptively.

Such adaptive strategies have already been studied extensively in quantum channel discrimination [44–46] and in noise estimation [47,48]. Perfect local discrimination of any orthogonal ensemble $\mathcal{E}_N$ is possible with $(N-1)$ copies under such adaptive schemes. The known examples of the nonlocal ensemble, however, do not even require $(N-1)$ copies for perfect discrimination. In fact, the authors in Ref. [2] found no example where more than two copies of the unknown state are needed for perfect discrimination, and thus, they laid down the question: "Are there any sets of states, entangled or not, for which some finite number (greater than 2) of copies of the state is necessary for distinguishing the states reliably?" Even after more than two decades, to the best of our knowledge, there is no conclusive answer to this question. In the present Letter, we address this question and show that, indeed, there exist ensembles of orthogonal pure states for a composite system that require more than two copies of the state for perfect local discrimination under adaptive strategies. Our explicit constructions form orthonormal bases for two-qubit Hilbert space. We, in-fact, completely characterize the two-qubit ensembles that require three copies of the state for perfect local discrimination under adaptive strategies. Interestingly, we also find ensembles that require three copies of the state for perfect discrimination under adaptive LOCC, whereas two copies suffice if adaptive SEP protocols are followed. Multicopy consideration of the local state discrimination problem establishes the "more nonlocality with less entanglement" phenomenon for $(\mathbb{C}^2)^{\otimes 2}$ ensembles, which was earlier reported for ensembles in $(\mathbb{C}^3)^{\otimes 2}$ [9]. Our study indicates an intriguing superadditivity phenomenon for the locally accessible information of multisite quantum ensembles, and we discuss a practical application of the present constructions in a multipartite secret sharing task.

Results.—Throughout the Letter, we follow the standard notations used in the quantum information community. For instance, $\{|0\rangle, |1\rangle\}$ is the computational basis (eigenkets of the Pauli σ_z operator) of $\mathbb{C}^2$, and $|ab\rangle$ stands for the short hand notation of the bipartite state $|a\rangle_A \otimes |b\rangle_B \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$. Given the single copy of the state, the authors in [4] have analyzed LOCC distinguishability of orthogonal ensembles in $(\mathbb{C}^2)^{\otimes 2}$. Here, we will analyze their multicopy local distinguishability. We will explore the case where Alice and Bob follow adaptive protocols for discrimination. An ensemble of three orthogonal pure states (of an arbitrary composite system) is always two-copy distinguishable under adaptive LOCC [8,16]. Therefore, we will focus on the ensembles $\mathcal{E}_4 = \{|\psi_i\rangle\}_{i=1}^4 \subset (\mathbb{C}^2)^{\otimes 2}$, where $\langle\psi_i|\psi_j\rangle = \delta_{ij}$. Throughout the Letter, we will consider that the states are uniformly sampled from the ensemble. Given multiple copies, while discriminating such a set under adaptive protocol, the following three situations can arise: (a) the states can be discriminated after acting on the first copy at an early stage of the protocol, (b) the protocol on the first copy results in a conclusion that the given state belongs to the group $\mathcal{G}_l \equiv \{|\psi_l\rangle\}$ or in its complement group $\mathcal{G}_l^{\mathsf{C}} \coloneqq \mathcal{E}_4 \backslash \mathcal{G}_l$, for some $l \in \{1, \ldots, 4\}$, and (c) the protocol on the first copy results in a conclusion that the state belongs to the group $\mathcal{G}_{ij} \equiv \{|\psi_i\rangle, |\psi_j\rangle\}$ for some $i, j \in \{1, \ldots, 4\}$ with $i \neq j$. In the second and third cases, the discrimination has to be completed from the subsequent copies. This leads us to our first result.

Theorem 1.—An orthogonal ensemble $\mathcal{E}_4 \subset (\mathbb{C}^2)^{\otimes 2}$ is two-copy distinguishable under adaptive LOCC protocol if and only if one of the following is satisfied: (i) The set is one-copy distinguishable and a second copy is not at all required (trivial case). (ii) The protocol on the first copy leads to a conclusion that the given state belongs to a group $\mathcal{G}_l$ or $\mathcal{G}_l^{\mathsf{C}}$ for some $l \in \{1, \ldots, 4\}$ such that $\mathcal{G}_l^{\mathsf{C}}$ contains no more than one entangled state. (iii) The protocol on the first copy leads to a conclusion that the given state belongs to the group $\mathcal{G}_{ij}$ for some $i, j \in \{1, \ldots, 4\}$ with $i \neq j$, such that the projectors $\mathbb{P}_{ij}$ and $\mathbb{P}_{ij}^{\mathsf{C}}$ are separable, where $\mathbb{P}_{ij} \coloneqq |\psi_i\rangle\langle\psi_i| + |\psi_j\rangle\langle\psi_j|$ and $\mathbb{P}_{ij}^{\mathsf{C}} \coloneqq \mathbf{I}_4 - \mathbb{P}_{ij}$.

Proof of Theorem 1.—For perfect discrimination, after the protocol on the first copy, either the state is discriminated straightaway [case (i)] or some states (at least one) must be eliminated [the other two cases]. In case (ii), if the protocol on the first copy leads to the conclusion that the given set is in some group $\mathcal{G}_l$, then the discrimination is done. If it leads to a conclusion in the complement group $\mathcal{G}_l^{\mathsf{C}}$ (which will be the case with some nonzero probability), then the unknown state needs to be distinguished from the second copy. Recall that three orthogonal states in $(\mathbb{C}^2)^{\otimes 2}$ can be exactly locally distinguished if and only if at least two of those states are product states [4] and, hence, leading us to assertion (ii). In case (iii), if the protocol on the first

copy leads to a conclusion that the unknown state belongs in either some group $\mathcal{G}_{ij}$ or in its complement group $\mathcal{G}_{ij}^{\complement}$, then protocol on the second copy perfectly succeeds, as two orthogonal states (in any dimension) can always be exactly locally distinguished [8]. Suppose that there is some LOCC protocol on the first copy that leads us to this desired conclusion. Such a protocol will perfectly distinguish the density operators $\rho := \frac{1}{2}\mathbb{P}_{ij}$ and $\rho^{\perp} := \frac{1}{2}\mathbb{P}_{ij}^{\complement}$. Recall that two rank-two orthogonal density operators ρ, $\rho^{\perp} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ are LOCC distinguishable if and only if the projectors onto the supports of each of the mixed states are separable [17] and, hence, leads us to assertion (iii).

To complete the argument, let us consider that, after the protocol on the first copy, none of the states is eliminated, rather, the knowledge regarding the ensemble gets updated, i.e., the uniform ensemble $\mathcal{E}_4 \equiv \{1/4, |\psi_i\rangle\}$ ends up in some nonuniform ensemble $\mathcal{E}_4' \equiv \{p_i, |\psi_i\rangle | p_i \neq 0 \, \forall \, i\}$. In such a case, the ensemble $\mathcal{E}'$ must be discriminated from the second copy of the state. According to Theorem 4 of Ref. [4], this can be done if and only if all four states are product. This is because Theorem 4 of Ref. [4] (and, also, the other theorems therein) is independent of the prior probability distributions. This completes the proof. ∎

Given the above theorem, naturally, the question arises which orthogonal ensembles of $(\mathbb{C}^2)^{\otimes 2}$ are two-copy distinguishable under adaptive LOCC. As an immediate corollary of Theorem 1, first, we have the following result (Proof provided in the Supplemental Material [49]).

Corollary 1.—Any orthogonal ensemble of $(\mathbb{C}^2)^{\otimes 2}$ containing no more than two entangled states is two-copy distinguishable under adaptive LOCC.

Ensembles having more than two entangled states can not be in category (i) or category (ii) of Theorem 1. However, they can be in category (iii). For instance, consider the orthonormal basis $\mathcal{B}^{[\theta]}$ with basis states

$$|\phi_\theta^+\rangle := S_\theta|00\rangle + C_\theta|11\rangle, \qquad |\phi_\theta^-\rangle := C_\theta|00\rangle - S_\theta|11\rangle,$$
$$|\psi_\theta^+\rangle := S_\theta|01\rangle + C_\theta|10\rangle, \qquad |\psi_\theta^-\rangle := C_\theta|01\rangle - S_\theta|10\rangle,$$

where $S_\theta \equiv \sin\theta$ & $C_\theta \equiv \cos\theta$ with $0 \leq \theta \leq \pi/2$. All the states are entangled whenever $\theta \neq 0, \pi/2$ and, in particular, $\theta = \pi/4$ corresponds to the maximally entangled basis or Bell basis. These entangled bases are two-copy distinguishable under adaptive LOCC. The protocol goes as follows: on the first copy, both Alice and Bob perform σ_z measurement on their part of the composite system and compare their measurement results. Correlated outcomes imply that the given state belongs to the group $\mathcal{G}_{|\phi\rangle} \equiv \{|\phi_\theta^+\rangle, |\phi_\theta^-\rangle\}$ whereas anticorrelated outcomes imply that it is from the group $\mathcal{G}_{|\psi\rangle} \equiv \{|\psi_\theta^+\rangle, |\psi_\theta^-\rangle\}$. The result of Walgate *et al.* [8] assures perfect local distinguishability of the states from the second copy. Now, let us construct another orthonormal basis

$$\mathcal{A}_\gamma^{[\alpha,\beta]} \equiv \left\{ \begin{array}{ll} |a_1\rangle := |\phi_\alpha^-\rangle, & |a_3\rangle := S_\gamma|\phi_\alpha^+\rangle + C_\gamma|\psi_\beta^+\rangle \\ |a_2\rangle := |\psi_\beta^-\rangle, & |a_4\rangle := C_\gamma|\phi_\alpha^+\rangle - S_\gamma|\psi_\beta^+\rangle \end{array} \right\},$$

with $\alpha, \beta, \gamma \in [0, \pi/2]$. Whenever $\alpha, \beta \neq 0, \pi/2$, the states $|a_1\rangle$ and $|a_2\rangle$ are entangled. However, entanglement of the other two states demands further restrictions on the parameters. For instance, the states $|a_3\rangle, |a_4\rangle \in \mathcal{A}_{\pi/4}^{[\alpha,\beta]}$ are entangled if and only if $\alpha \neq \beta, \ \pi/2 - \beta$. In the rest of the Letter, we will mainly analyze the case $\gamma = \pi/4$. For generic consideration of γ, see the Supplemental Material [49]. We also consider the cases where all the states in $\mathcal{A}_{\pi/4}^{[\alpha,\beta]}$ are entangled. Next, we report an interesting feature of the set $\mathcal{A}_{\pi/4}^{[\alpha,\beta]}$.

Proposition 1.—$\mathbb{V}[ij] := Span\{|a_i\rangle, |a_j\rangle\}$ with $i \neq j$ and $|a_i\rangle, |a_j\rangle \in \mathcal{A}_{\pi/4}^{[\alpha,\beta]}$; $\alpha \neq \beta, \ \pi/2 - \beta$. For every choice of $i, j \in \{1, 2, 3, 4\}$, the projector onto the two dimensional subspace $\mathbb{V}[ij]$ is entangled.

See the Supplemental Material [49] for the proof. Coming back to local distinguishability of the set $\mathcal{A}_{\pi/4}^{[\alpha,\beta]}$, it is neither in category (i) nor in category (ii) of Theorem 1. Furthermore, Proposition 1 obstructs it from being in category (iii), as well. Altogether, these guide us to the following result.

Theorem 2.—The set $\mathcal{A}_{\pi/4}^{[\alpha,\beta]}$, with $\alpha \neq \beta, \ \pi/2 - \beta$, is perfectly distinguishable under adaptive LOCC protocol if and only if three copies of the state are available.

Under the adaptive local discrimination scheme, therefore, we have a conclusive answer to the Bennett *et al.* question [2] discussed in the introduction—indeed, there exists an ensemble of states that requires more than two copies of the state for perfect discrimination under an adaptive local scheme. Under such schemes, the set $\mathcal{A}_{\pi/4}^{[\alpha,\beta]}$ can be considered as the strongest nonlocal ensemble (of orthogonal pure states) in $(\mathbb{C}^2)^{\otimes 2}$. Naturally, the question arises regarding whether such a nonlocal ensemble requires all of its states to be entangled. Our next theorem (proof provided in the Supplemental Material [49]) answers this question.

Theorem 3.—Any orthonormal basis of $(\mathbb{C}^2)^{\otimes 2}$ containing exactly three entangled states requires three copies of the state for perfect discrimination under adaptive LOCC.

Theorem 3 is quite interesting, in a sense. It tells that any basis containing three entangled states is two-copy indistinguishable under adaptive LOCC, whereas some bases with all entangled states (e.g., Bell basis) are two-copy distinguishable under a local adaptive scheme. This mimics the phenomenon of more nonlocality with less entanglement [9], as a set with fewer numbers of entangled states turns out to be harder to discriminate. Importantly, the ensemble in Ref. [9] exhibiting this feature lives in $(\mathbb{C}^3)^{\otimes 2}$, and with single-copy consideration, such a phenomenon is not possible in $(\mathbb{C}^2)^{\otimes 2}$. Multicopy adaptive discrimination makes this phenomenon possible for two-qubit ensembles

and, in fact, introduces a hierarchical strength in the more nonlocality with less entanglement phenomenon.

Next, we consider multicopy discrimination of nonlocal ensembles under the adaptive SEP. Recall that this set of operations strictly includes the set of LOCC operations [35], even for two-qubit Hilbert space [36]. Our next result, however, establishes that, given two copies of the state, even this larger class of operations fails to erase the nonlocal feature of some ensembles.

Theorem 4.—There exist suitable choices of the parameters α, β, and γ such that, under adaptive SEP protocol, perfect discrimination of the set $\mathcal{A}_{\gamma}^{[\alpha,\beta]}$ requires three copies of the state.

For instance, $\alpha, \beta \neq 0, \pi/2$, and $\gamma = \pi/6$ constitute such choices. Generic analysis is referred to in the Supplemental Material [49]. Similar to Theorem 1, any protocol on the first copy that just updates the prior probability distribution without eliminating state(s) does not work well in this case, either. Theorem 4 is also important from another perspective. Mathematical characterization of local operations is extremely hard, in general. While implementation of such an operation may be done by some finite round of LOCC protocol, its implementation may also demand an infinite round of protocol. One can also define topological closure of such different sets. However, all these different classes of local operations are strictly included within the set of SEP protocol [35]. Therefore, the ensembles in Theorem 4 remain two-copy indistinguishable under adaptive protocol even under an infinite round of LOCC. Arguably, these are the strongest two-qubit nonlocal ensembles under any adaptive discrimination scheme—LOCC and/or SEP. Considering general $\mathcal{A}_{\gamma}^{[\alpha,\beta]}$, we, indeed, find ensembles that are perfectly two-copy distinguishable under adaptive SEP, whereas adaptive LOCC requires three copies for perfect discrimination (ensembles in Theorem 2 are such examples).

Therefore, we are left with the only possibility whether the aforesaid ensembles are two-copy distinguishable under a nonadaptive local protocol. In such a protocol, Alice (Bob) addresses both the systems at her (his) end simultaneously to perform some global measurement and communicates the outcomes with the other party. Such measurement includes SEP as well as entangled basis measurements. It is important to note that existence of an ensemble that is distinguishable under a multicopy local nonadaptive scheme but indistinguishable under an adaptive local scheme will establish an intriguing superadditivity behavior for the locally accessible information of multisite quantum ensembles [52]. Therefore, our constructions are quite interesting—either they will establish two-copy indistinguishability (under generic protocol), or it will demonstrate superadditivity of locally accessible information. In this regard, superadditivity phenomena of classical capacity of a noisy quantum channel is worth mentioning [53–56]. There, also, entangled decoding on multiple copies of noisy channels turns out to be more efficient than its multiple single-copy use.

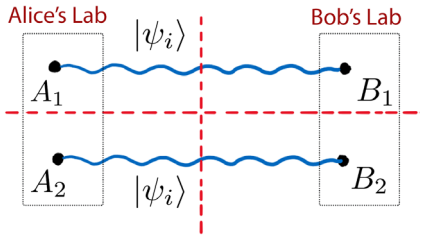

FIG. 1. Alice and Bob share multiple copies of an unknown state $|\psi_i\rangle$ belonging to a known ensemble $\mathcal{E}_N$. Availability of additional entanglement resources across the vertical (party-cut) and/or horizontal (copy-cut) dotted lines give rise to different sets of allowed operations performed by Alice and Bob. (a) No additional entanglement across the vertical and horizontal lines gives adaptive LOCC, (b) adaptive SEP (more generally entangling operation) requires additional entanglement across vertical line but no entanglement across horizontal line, (c) additional entanglement across horizontal line but no entanglement across vertical line gives nonadaptive LOCC, (d) nonadaptive SEP requires entanglement across both vertical and horizontal lines.

An ensemble indistinguishable under a local nonadaptive scheme will also be indistinguishable under adaptive LOCC. However, such an ensemble may be perfectly distinguished with adaptive SEP. Note that physical realization of both the local nonadaptive scheme as well as adaptive SEP scheme require entanglement. While, in the first case, entanglement is across the cut between different copies, in the later case entanglement is consumed across the cut between parties (see Fig. 1). However, at present, we have no intuition for construction of such ensembles and leave this question open for further research. In the following, rather, we focus on possible application of the present constructions.

Multiparty secret sharing.—Secret sharing is an important cryptographic primitive [57]. In the (k, m) secret sharing scheme, an administrator wishes to distribute a k-bit classical message among m spatially separated parties in such a way that perfect revelation of the message requires (classical) collaboration among all m parties. In a quantum scenario, the administrator encodes the k-bit massage in some m-partite state, i.e., $i \mapsto \rho_i \in \mathcal{D}(\mathcal{H}^{\otimes m})$ such that $\{\rho_i\}_{i=1}^{2^k}$ is a mutually orthogonal set of states [28]. Our construction turns out to be efficient for a (2,6) pure quantum protocol (encoded states are pure). The administrator encodes her 2-bit message into an ensemble $\mathcal{E}_4 \equiv \{|\psi_i\rangle\}_{i=1}^{4}$ which is indistinguishable under two-copy adaptive LOCC, prepares three copies of the state, and distributes those among the six separated parties. In short, $i \mapsto |\psi_i\rangle \mapsto |\psi_i\rangle_{A_1B_1} \otimes |\psi_i\rangle_{A_2B_2} \otimes |\psi_i\rangle_{A_3B_3}$. No four parties can exactly decode the message through classical collaboration among them [58].

In a stronger variant of the aforesaid task, even the classical collaborations among the parties are insufficient

for a perfect revelation of the message—the parties need to come together to decode the information. It is also possible to come up with such a (1,2) protocol from our construction. Recall that the result of Walgate *et al.* [4] prohibits any such $(1, m)$ pure quantum protocol. So, the administrator chooses some pair of index i, j as in Proposition 1 and then encodes her message into the density operators $\sigma(\lambda) \coloneqq \lambda|a_i\rangle\langle a_i| + (1-\lambda)|a_j\rangle\langle a_j|$ supported on the subspace $\mathbb{V}[ij]$ and its orthogonal pair $\sigma^{\perp}(\mu)$ supported on the complementary subspace. Whenever $\lambda, \mu \in (0, 1)$, the perfect revelation of the message demands that both the parties come together to apply a global discrimination measurement. At this point it may be interesting to find the values of λ and μ that will ensure the least amount of information accessible by LOCC.

Discussion.—We have discussed the problem of local state discrimination when multiple copies of the unknown state are available. Our study is a major advancement in this direction as it establishes that there exist ensembles of pure composite orthogonal states that are not two-copy distinguishable under adaptive LOCC protocol. Under a multicopy adaptive scheme, we have completely characterized the nonlocal behavior of the orthogonal ensembles of two-qubit Hilbert space. Such two-copy indistinguishable sets find useful applications in multiparty secret sharing tasks.

Our study also raises a number of interesting questions. A conclusive answer to the possible superadditivity behavior for locally accessible information is worth discussing. A nonadaptive protocol is still missing for the example of ensembles where adaptive SEP protocol extracts more classical information than local. A study of multicopy state discrimination for higher dimensional and multipartite Hilbert spaces might reveal several other interesting features. One can consider more exotic adaptive protocols that allow us to interact back and forth with the different copies by means of nonprojective measurements. We believe that, even under this more exotic protocol, our two-copy local indistinguishable ensembles will remain indistinguishable. Formal proof of this assertion demands further research.

M. B. acknowledges a research grant of the INSPIRE-Faculty Fellowship from the Department of Science and Technology, Government of India. M. A. acknowledges support from the CSIR Project No. 09/093(0170)/2016-EMR-I. S. S. B. is supported by the National Natural Science Foundation of China through Grant No. 11675136, the Foundational Questions Institute through Grant No. FQXiRFP3-1325, the Hong Kong Research Grant Council through Grant No. 17300918, and the ID No. 61466 Grant from the John Templeton Foundation, as part of the "Quantum Information Structure of Spacetime (QISS)" Project (qiss.fr). The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the John Templeton Foundation.

[1] I. Chuang and M. Nielsen, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] 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).
[3] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Distinguishability of Bell States, Phys. Rev. Lett. **87**, 277902 (2001).
[4] J. Walgate and L. Hardy, Nonlocality, Asymmetry, and Distinguishing Bipartite States, Phys. Rev. Lett. **89**, 147901 (2002).
[5] A. Peres and W. K. Wootters, Optimal Detection of Quantum Information, Phys. Rev. Lett. **66**, 1119 (1991).
[6] E. Chitambar and Min-Hsiu Hsieh, Revisiting the optimal detection of quantum information, Phys. Rev. A **88**, 020302 (R) (2013).
[7] 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).
[8] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States, Phys. Rev. Lett. **85**, 4972 (2000).
[9] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local Indistinguishability: More Nonlocality with Less Entanglement, Phys. Rev. Lett. **90**, 047902 (2003).
[10] 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).
[11] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Distinguishability of maximally entangled states, Phys. Rev. A **70**, 022304 (2004).
[12] J. Watrous, Bipartite Subspaces Having No Bases Distinguishable by Local Operations and Classical Communication, Phys. Rev. Lett. **95**, 080505 (2005).
[13] J. Niset and N. J. Cerf, Multipartite nonlocality without entanglement in many dimensions, Phys. Rev. A **74**, 052103 (2006).
[14] R. Duan, Y. Feng, Z. Ji, and M. Ying, Distinguishing Arbitrary Multipartite Basis Unambiguously Using Local Operations and Classical Communication, Phys. Rev. Lett. **98**, 230502 (2007).
[15] J. Calsamiglia, J. I. de Vicente, R. Muñoz-Tapia, and E. Bagan, Local Discrimination of Mixed States, Phys. Rev. Lett. **105**, 080504 (2010).
[16] S. Bandyopadhyay, More Nonlocality with Less Purity, Phys. Rev. Lett. **106**, 210402 (2011).
[17] E. Chitambar, R. 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).
[18] S. Halder, Several nonlocal sets of multipartite pure orthogonal product states, Phys. Rev. A **98**, 022303 (2018).
[19] M. Demianowicz and R. Augusiak, From unextendible product bases to genuinely entangled subspaces, Phys. Rev. A **98**, 012313 (2018).

[20] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Strong Quantum Nonlocality without Entanglement, Phys. Rev. Lett. **122**, 040403 (2019).

[21] S. Agrawal, S. Halder, and M. Banik, Genuinely entangled subspace with all-encompassing distillable entanglement across every bipartition, Phys. Rev. A **99**, 032335 (2019).

[22] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Genuinely nonlocal product bases: Classification and entanglement-assisted discrimination, Phys. Rev. A **100**, 032321 (2019).

[23] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Local state discrimination and ordering of multipartite entangled states, arXiv:1910.14308.

[24] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[25] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding Bits in Bell States, Phys. Rev. Lett. **86**, 5807 (2001).

[26] T. Eggeling and R. F. Werner, Hiding Classical Data in Multipartite Quantum States, Phys. Rev. Lett. **89**, 097905 (2002).

[27] W. Matthews, S. Wehner, and A. Winter, Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding, Commun. Math. Phys. **291**, 813 (2009).

[28] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[29] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).

[30] R. Rahaman and M. G. Parker, Quantum scheme for secret sharing based on local distinguishability, Phys. Rev. A **91**, 022330 (2015).

[31] C. A. Fuchs, Just two nonorthogonal quantum states, in *Quantum Communication, Computing, and Measurement*, edited by P. Kumar, G. M. D'Ariano, and O. Hirota (Springer, Boston, 1998), Vol. 2, https://arxiv.org/abs/quant-ph/9810032.

[32] M. F. Pusey, J. Barrett, and T. Rudolph, On the reality of the quantum state, Nat. Phys. **8**, 475 (2012).

[33] S. Bandyopadhyay, M. Banik, S. S. Bhattacharya, S. Ghosh, G. Kar, A. Mukherjee, and A. Roy, Reciprocal ontological models show indeterminism of the order of quantum theory, Found. Phys. **47**, 265 (2017).

[34] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, Nonlocality without entanglement: Quantum theory and beyond, Phys. Rev. Research **2**, 012068(R) (2020).

[35] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328**, 303 (2014).

[36] R. Duan, Y. Feng, Y. Xin, and M. Ying, Distinguishability of quantum states by separable operations, IEEE Trans. Inf. Theory **55**, 1320 (2009).

[37] N. Yu, R. Duan, and M. Ying, Four Locally Indistinguishable Ququad-Ququad Orthogonal Maximally Entangled States, Phys. Rev. Lett. **109**, 020506 (2012).

[38] N. Yu, R. Duan, and M. Ying, Distinguishability of quantum states by positive operator-valued measures with positive partial transpose, IEEE Trans. Inf. Theory **60**, 2069 (2014).

[39] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, Limitations on separable measurements by convex optimization, IEEE Trans. Inf. Theory **61**, 3593 (2015).

[40] 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).

[41] G. Chiribella, G. Mauro D'Ariano, and P. Perinotti, Informational derivation of quantum theory, Phys. Rev. A **84**, 012311 (2011).

[42] H. Barnum and A. Wilce, Local tomography and the Jordan structure of quantum theory, Found. Phys. **44**, 192 (2014).

[43] G. Niestegge, Local tomography and the role of the complex numbers in quantum mechanics, Proc. R. Soc. A. **476**, 20200063 (2020).

[44] M. Hayashi, Discrimination of two channels by adaptive methods and its application to quantum system, IEEE Trans. Inf. Theory **55**, 3807 (2009).

[45] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, Adaptive versus nonadaptive strategies for quantum channel discrimination, Phys. Rev. A **81**, 032339 (2010).

[46] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, Fundamental limits to quantum channel discrimination, npj Quantum Inf. **5**, 50 (2019).

[47] S. Pirandola and C. Lupo, Ultimate Precision of Adaptive Noise Estimation, Phys. Rev. Lett. **118**, 100502 (2017).

[48] T. P. W. Cope and S. Pirandola, Adaptive estimation and discrimination of Holevo Werner channels, Quantum Meas. Quantum Metrol. **4**, 44 (2017).

[49] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.210505 for general analysis of Proposition 1 involving calculation of concurrence [50], and proof of Theorem 3 invoking a well-known result from the Ref. [51].

[50] W. K. Wootters, Entanglement of Formation of an Arbitrary State of Two Qubits, Phys. Rev. Lett. **80**, 2245 (1998).

[51] P. Horodecki, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Rank two bipartite bound entangled states do not exist, Theor. Comput. Sci. **292**, 589 (2003).

[52] P. Badziag, M. Horodecki, A. Sen(De), and U. Sen, Locally Accessible Information: How Much Can the Parties Gain by Cooperating?, Phys. Rev. Lett. **91**, 117901 (2003).

[53] C. A. Fuchs, Nonorthogonal Quantum States Maximize Classical Information Capacity, Phys. Rev. Lett. **79**, 1162 (1997).

[54] C. King and M. B. Ruskai, Capacity of quantum channels using product measurements, J. Math. Phys. (N.Y.) **42**, 87 (2001).

[55] B. Schumacher and M. D. Westmoreland, Optimal signal ensembles, Phys. Rev. A **63**, 022308 (2001).

[56] C. King, M. Nathanson, and M. B. Ruskai, Qubit Channels Can Require More Than Two Inputs to Achieve Capacity, Phys. Rev. Lett. **88**, 057901 (2002).

[57] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).

[58] Collaboration among certain groups of the four parties can reveal, at most, 1-bit data which is only half of the desired message. It is also not hard to argue that collaboration among any five parties cannot reveal a 2-bit message exactly. It should be noted that security of the protocol is assured under the adaptive protocol considered in Definition 1. A more generic protocol might further demand limitation on the LOCC operations among different groups of the parties.