Difficulty of distinguishing product states locally

Sarah Croke[*] and Stephen M. Barnett

School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, United Kingdom

Nonlocality without entanglement is a rather counterintuitive phenomenon in which information may be encoded entirely in product (unentangled) states of composite quantum systems in such a way that local measurement of the subsystems is not enough for optimal decoding. For simple examples of pure product states, the gap in performance is known to be rather small when arbitrary local strategies are allowed. Here we restrict to local strategies readily achievable with current technology: those requiring neither a quantum memory nor joint operations. We show that even for measurements on pure product states, there can be a large gap between such strategies and theoretically optimal performance. Thus, even in the absence of entanglement, physically realizable local strategies can be far from optimal for extracting quantum information.

A composite quantum system is more than the sum of its parts; it can have properties that cannot be explained as a result of properties of its constituent particles. This may be thought of as a result of the superposition principle and has far-reaching consequences, giving quantum theory a far richer structure than classical probability theory. Indeed, entangled states, characterized by correlations between particles rather than local properties of constituent particles, famously exhibit correlations that cannot be reproduced by any local classical theory [1]. In addition, there exist properties of composite systems that are not accessible through only local measurement of the subsystems: for example, a measurement which distinguishes between the $j = 0$ and $j = 1$ subspaces of a two spin-half system cannot be performed through only local measurements on the spins.

In contrast to classical probability theory, therefore, local measurements together with postprocessing of measurement results is not enough to perform all measurements allowed by quantum theory. In fact, due to the existence of incompatible observables, even classical communication *between* subsystems (allowing the choice of measurement on one system to depend on the outcome of measurement on the other) gives the measuring parties new capabilities. In general, one-way classical communication, two-way classical communication, and quantum communication (the ability to send quantum states) are each more powerful than the last [2–27]. Remarkably, this is true even for measurements on unentangled states, a phenomenon known as "nonlocality without entanglement" [2–5]. In practical terms, however, for measurements on product states, the known bounds on the gaps in performance are really rather small [4,5].

In this paper, we introduce another piece of the puzzle in the local detection of quantum information and show that two-way classical communication can significantly improve the distinguishability of pure, orthonormal product states.

Such sets of states have two important features: they can be prepared in separated laboratories without either classical or quantum communication between labs and they are perfectly distinguishable through a joint measurement. We derive optimal one-way strategies for two examples of such sets, one of which may be perfectly discriminated with only two rounds of classical communication, while the other, the so-called domino states, requires quantum communication for perfect discrimination. We show that any one-way scheme succeeds with probability of at most $\simeq 85\%$ and $\simeq 84\%$, respectively, a significant deficit compared to the globally optimal schemes.

Physically, current experimental capabilities are such that sequential measurement (i.e., one-way) strategies may be readily implemented in a variety of physical systems. Additional rounds of measurement and classical communication are more technologically challenging; they not only introduce additional errors and inefficiencies, but also require some sort of quantum memory in which to store the local systems in a many-round protocol. Our examples demonstrate that even for the simplest cases of discriminating pure, orthonormal, unentangled states, quantum memories or joint control can be necessary for optimal or even close-to-optimal performance.

We begin with a simple example, first considered by Groisman and Vaidman [9], which demonstrates the asymmetry of classical communication as a resource for performing joint measurements and serves to illustrate some features of optimal measurement strategies that we will need later. Consider the product basis of two-qubit states,

$$|\psi_{00}\rangle = |0\rangle_A \otimes |0\rangle_B, \quad |\psi_{10}\rangle = |1\rangle_A \otimes |0+1\rangle_B,$$
$$|\psi_{01}\rangle = |0\rangle_A \otimes |1\rangle_B, \quad |\psi_{11}\rangle = |1\rangle_A \otimes |0-1\rangle_B, \tag{1}$$

where $\{|0\rangle, |1\rangle\}$ form an orthonormal basis, by convention the eigenbasis of the Pauli operator σ_z, and $|0 \pm 1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are the eigenstates of σ_x. Clearly, the states are perfectly distinguishable given one-way communication from Alice to Bob, but not the other way around: if Alice can send a message to Bob, she simply needs to measure in the $\{|0\rangle, |1\rangle\}$ basis and send the result of her measurement to Bob. Given result "0," Bob measures in the $\{|0\rangle, |1\rangle\}$ basis, while given result "1," he measures in the $\{|0 \pm 1\rangle\}$ basis. On the other hand, if Bob can send messages to Alice but not

---

[*]sarah.croke@glasgow.ac.uk

vice versa, there is clearly no procedure that allows Alice and Bob to perfectly distinguish the states: Bob's local states are eigenstates of incompatible observables σ_z and σ_x, and any measurement giving information about one must necessarily disturb the other, thus destroying the orthogonality of at least one pair of states.

It is instructive to consider what is the best Alice and Bob can do if they are limited to communication only from Bob to Alice. Note that Alice's system is essentially classical in that regardless of the information obtained from Bob, the only sensible measurement she can make is in the z basis, which allows her to perfectly determine the index i in the labeling $\{|\psi_{ij}\rangle\}$, but gives no information about the index j. The role of Bob's measurement therefore is to provide the information which allows Alice to distinguish between the states within the pair $\{|\psi_{i0}\rangle, |\psi_{i1}\rangle\}$ for each possible outcome i of Alice's measurement. It follows that Bob's measurement must rule out as well as possible one state from each pair, leaving Alice with two remaining allowed states, which are perfectly distinguishable through Alice's measurement. There are four subsets of two states with the property that the states are perfectly distinguishable on Alice's side:

$$\mathcal{S}_{00} = \{|\psi_{00}\rangle, |\psi_{10}\rangle\}, \quad \mathcal{S}_{01} = \{|\psi_{00}\rangle, |\psi_{11}\rangle\},$$
$$\mathcal{S}_{10} = \{|\psi_{01}\rangle, |\psi_{10}\rangle\}, \quad \mathcal{S}_{11} = \{|\psi_{01}\rangle, |\psi_{11}\rangle\}.$$

Thus, Alice and Bob's strategy, if classical communication is allowed from Bob to Alice only, is for Bob's measurement to optimally assign the state to one of these subsets, while Alice's measurement discriminates between the remaining two states within a subset.

If the states are equiprobable, the measurement on Bob's system maximizing the probability of correctly identifying the state is, in fact, quite well known, as these states arise in the BB84 protocol for quantum key distribution [28]. The index i corresponds to the sender's choice of basis, while j denotes the bit value. Naturally enough due to the symmetry of the set, the optimal measurement is in a basis intermediate to the x basis and the z basis: the so-called Breidbart basis [29],

$$|\phi_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle,$$
$$|\phi_1\rangle = \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle. \tag{2}$$

Outcome 0 leads Bob to guess that the state belongs to subset $\mathcal{S}_{00}$, while outcome 1 leads to a guess of $\mathcal{S}_{11}$. In fact, the optimal measurement is degenerate: measurement of either of the spin observables $\frac{1}{\sqrt{2}}(\sigma_z \pm \sigma_x)$ results in an optimal strategy. This succeeds with probability $\cos^2\frac{\pi}{8} = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \simeq 0.85$, a significant deficit compared to the unit probability of success achievable when one-way communication is allowed from Alice to Bob [9].

Using this simple set as a building block, we can construct our first example for which two-way classical communication provides a significant advantage over one-way classical communication for discriminating unentangled states. Consider the following orthonormal product basis of a $2 \otimes 4$ level system

(also introduced in [17]):

$$|\psi_{00}\rangle = |0\rangle_A|0\rangle_B, \quad |\psi_{02}\rangle = |0+1\rangle_A|2\rangle_B,$$
$$|\psi_{01}\rangle = |0\rangle_A|1\rangle_B, \quad |\psi_{03}\rangle = |0+1\rangle_A|3\rangle_B,$$
$$|\psi_{10}\rangle = |1\rangle_A|0+1\rangle_B, \quad |\psi_{12}\rangle = |0-1\rangle_A|2+3\rangle_B,$$
$$|\psi_{11}\rangle = |1\rangle_A|0-1\rangle_B, \quad |\psi_{13}\rangle = |0-1\rangle_A|2-3\rangle_B. \tag{3}$$

These states are perfectly distinguishable given just two rounds of classical communication, while any one-way scheme succeeds with probability at most $\cos^2\frac{\pi}{8}$, as we now show.

We first note that Bob can learn in which subspace $\{|0\rangle, |1\rangle\}$ or $\{|2\rangle, |3\rangle\}$ his state lies without disturbing any of the states, via a von Neumann measurement with projectors $\{|0\rangle\langle 0| + |1\rangle\langle 1|, |2\rangle\langle 2| + |3\rangle\langle 3|\}$, thus learning to which of the two subsets $\mathcal{S}_0 = \{|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle\}$ or $\mathcal{S}_1 = \{|\psi_{02}\rangle, |\psi_{03}\rangle, |\psi_{12}\rangle, |\psi_{13}\rangle\}$ the shared state belongs. Each subset is equivalent (up to local unitaries) to the simpler set discussed above. This observation simplifies the analysis of optimal schemes.

There are three cases of interest: (i) Two-way classical communication: Bob measures first and tells Alice to which of the subsets $\mathcal{S}_0$ or $\mathcal{S}_1$ the state belongs. Each subset is perfectly distinguishable with one-way communication from Alice to Bob, so just one more round of communication is needed for perfect discrimination. (ii) One-way communication from Alice to Bob: within each subset, the shared states are perfectly distinguishable with one-way measurement from Alice to Bob. However, Alice does not know in which subset the state lies. Clearly, Alice's measurement must simultaneously distinguish, as well as possible, between the states $\{|0\rangle, |1\rangle\}$ and $\{|0+1\rangle, |0-1\rangle\}$. But this is simply the same problem as we have seen previously and an optimal measurement for Alice is again in the Breidbart basis Eq. (2). Alice communicates the result of measurement to Bob; given outcome 0, Bob's measurement discriminates perfectly between the states $\{|0\rangle, |1\rangle\}$ and $\{|2\rangle, |3\rangle\}$, and given outcome 1, he instead measures in the basis $\{|0 \pm 1\rangle, |2 \pm 3\rangle\}$. The combination of Alice's and Bob's measurement results leads to a unique guess as to the state, which is correct with probability $\cos^2\frac{\pi}{8}$. (iii) One-way communication from Bob to Alice: Bob knows in which subset $\mathcal{S}_0$, $\mathcal{S}_1$ the state lies. In each case, as we have noted, the resulting set is equivalent to our simple example discussed above, for which the optimal one-way strategy succeeds with probability $\cos^2\frac{\pi}{8}$. Thus, any one-way scheme, regardless of the direction of communication, succeeds with probability at most $\cos^2\frac{\pi}{8} \simeq 85\%$, while two rounds of classical communication are sufficient to discriminate the states perfectly.

For our second example, we turn to the domino states [3], an orthonormal basis of a $3 \otimes 3$ level system given by

$$|\psi_{00}\rangle = |0\rangle|0-1\rangle,$$
$$|\psi_{10}\rangle = |1+2\rangle|0\rangle,$$
$$|\psi_{01}\rangle = |0\rangle|0+1\rangle,$$
$$|\psi_{11}\rangle = |1\rangle|1\rangle,$$
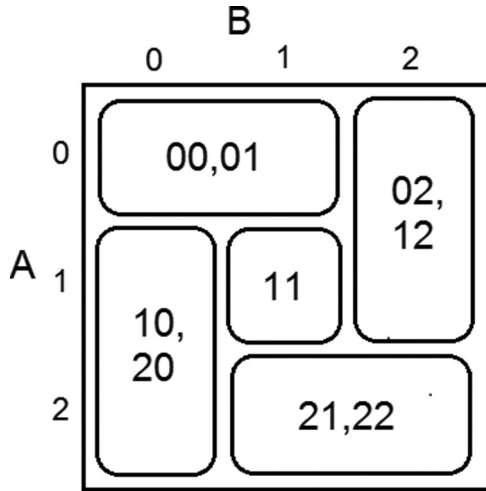$$|\psi_{02}\rangle = |0-1\rangle|2\rangle,$$
$$|\psi_{12}\rangle = |0+1\rangle|2\rangle,$$

FIG. 1. Graphical representation of the domino states.

$$|\psi_{20}\rangle = |1-2\rangle|0\rangle,$$
$$|\psi_{21}\rangle = |2\rangle|1-2\rangle,$$
$$|\psi_{22}\rangle = |2\rangle|1+2\rangle. \tag{4}$$

A useful graphical representation of these states is given in Fig. 1. This example is of a different flavor from the previous one, as the states are globally perfectly distinguishable, but two-way classical communication, even in the limit of infinite rounds of measurement and communication, is not enough to perfectly distinguish the states [3]. The known upper bound on the probability of error of any scheme with two-way communication, however, is so small as to be negligible for all practical purposes: 1.9×10^{-8} [4]. We find, by contrast, that the best one-way strategy has an error of more than 16%.

We begin by simply stating the optimal sequential measurement, which is somewhat intuitive, and give some of the technical details later. We assume the states are equiprobable, and we suppose that A is measured first, which due to the symmetry of the states we can do without any loss of generality. There are eight subsets of the set of domino states which are perfectly distinguishable on system B alone; these are

$$\mathcal{S}_0 = \{|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{02}\rangle\}, \quad \mathcal{S}_4 = \{|\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{02}\rangle\},$$
$$\mathcal{S}_1 = \{|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{12}\rangle\}, \quad \mathcal{S}_5 = \{|\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{12}\rangle\},$$
$$\mathcal{S}_2 = \{|\psi_{10}\rangle, |\psi_{21}\rangle, |\psi_{22}\rangle\}, \quad \mathcal{S}_6 = \{|\psi_{20}\rangle, |\psi_{11}\rangle, |\psi_{02}\rangle\},$$
$$\mathcal{S}_3 = \{|\psi_{20}\rangle, |\psi_{21}\rangle, |\psi_{22}\rangle\}, \quad \mathcal{S}_7 = \{|\psi_{20}\rangle, |\psi_{11}\rangle, |\psi_{12}\rangle\}. \tag{5}$$

The optimal sequential strategy assigns the state to one of these subsets in the first step, and perfectly discriminates the states within the subset in the second step. This succeeds with probability $\simeq 83.6\%$, as we show later.

Proving that this is indeed optimal is less straightforward than the previous cases. Our strategy is to place an upper bound on the probability of success of any sequential strategy, by considering a simpler, related discrimination problem, and then show that this bound is achievable. Thus, to bound the probability of success in identifying the state, rather than trying to discriminate between all nine states, let us

suppose instead that we simply try to determine to which of the three subsets $\{|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{02}\rangle\}$, $\{|\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{12}\rangle\}$, or $\{|\psi_{20}\rangle, |\psi_{21}\rangle, |\psi_{22}\rangle\}$ the state belongs; that is, with our choice of labeling $|\psi_{jk}\rangle$, we try to determine the index j, without worrying about k. This is equivalent to discriminating between the equiprobable mixed states,

$$\rho_j = \frac{1}{3} \sum_k |\psi_{jk}\rangle\langle\psi_{jk}|. \tag{6}$$

This problem of subset discrimination is strictly easier than our original problem: any measurement to discriminate between all nine domino states may also be used for subset discrimination, and performs at least as well for this task. Thus the success probability of the optimal sequential measurement discriminating the states $\{\rho_i\}$ is at least as high as the probability of success of any sequential measurement discriminating all nine domino states:

$$P_{\text{corr}}^{\text{seq}}(\{\psi_i\}) \leqslant P_{\text{corr}}^{\text{seq}}(\{\rho_i\}).$$

Furthermore, this set has the rather nice property that Bob's system is essentially classical; his state is always diagonal in the $\{|0\rangle, |1\rangle, |2\rangle\}$ basis, and thus regardless of the measurement on A, the only sensible measurement on B is in this basis. The role of Alice's measurement then, as in our first example, is simply to inform Bob how to interpret his measurement result. By inspection of the states ρ_j [Eq. (6)], we see that if Bob obtains outcome 0, then Alice's measurement must discriminate between the orthonormal states $\{|0\rangle, |1+2\rangle, |1-2\rangle\}$ to provide Bob with the information required to identify one of the states $\{\rho_0, \rho_1, \rho_2\}$, respectively. Similar observations for Bob's outcomes 1 and 2 reveal that the role of Alice's measurement is to simultaneously distinguish as well as possible the states within the three bases $\{|0\rangle, |1\pm2\rangle\}$, $\{|0\rangle, |1\rangle, |2\rangle\}$, and $\{|0\pm1\rangle, |2\rangle\}$. There are 27 subsets containing exactly one state from each basis: Alice's job is to optimally discriminate between these subsets. This sounds like a rather daunting task; however, it turns out, as we discuss below, that the optimal strategy is one that only ever identifies those subsets $\{\mathcal{S}_0, \ldots, \mathcal{S}_7\}$ given in Eq. (5).

Thus Alice's measurement giving the optimal one-way strategy for this simpler problem is precisely that conjectured to be optimal for discriminating all nine domino states. This succeeds with probability 83.6%, which as argued above is therefore an upper bound on the success probability for discriminating the domino states with only one-way classical communication. Further, this bound is achievable via the conjectured sequential scheme given above, which we therefore conclude is an optimal one-way strategy. In the remainder of the paper, we discuss some of the technical details of the derivation of Alice's optimal measurement. We give more details and an alternative proof elsewhere [30].

Alice wishes to optimally assign the state to one of the subsets $\{\mathcal{S}_i\}$. She performs a measurement on her system and, upon obtaining outcome j, takes this to indicate that the state belongs to the subset $\mathcal{S}_j$. The most general measurement she can perform on her system is described by a probability operator measure (POM) [31], also known as a positive operator-valued measure (POVM) [32], that is a set of positive

operators $\{\pi_j\}$ that form a resolution of the identity

$$\pi_j \geqslant 0, \quad \sum_j \pi_j = I. \tag{7}$$

The probability of obtaining outcome j in a measurement on a system prepared in state ρ is given by the Born rule: $P(j|\rho) = \text{Tr}(\rho\pi_j)$. Thus, the probability that Alice chooses a subset containing the prepared state is given by

$$\begin{aligned}
\text{P}_{\text{corr}} &= \sum_{ij} \frac{1}{9} \sum_{k||\psi_{ij}\rangle \in \mathcal{S}_k} \text{Tr}_{AB}(|\psi_{ij}\rangle\langle\psi_{ij}|\pi_k) \\
&= \frac{8}{3} \sum_k \frac{1}{8} \text{Tr}_A(\sigma_k \pi_k),
\end{aligned}$$

where in the last line we have defined $\sigma_k = \text{Tr}_B(\frac{1}{3}\sum_{ij||\psi_{ij}\rangle \in \mathcal{S}_k}|\psi_{ij}\rangle\langle\psi_{ij}|)$. σ_k is thus the density operator obtained by taking an equal mixture of the states in the subset $\mathcal{S}_k$, traced over Bob's system. It follows from the above that $\{\pi_k\}$ is the optimal measurement to discriminate the equiprobable states $\{\sigma_k\}$. Explicitly, the states σ_k are given by

$$\sigma_0 = \tfrac{2}{3}|0\rangle\langle0| + \tfrac{1}{3}|0-1\rangle\langle0-1|,$$

$$\sigma_1 = U\sigma_0 U^\dagger, \quad \sigma_2 = VU\sigma_0 U^\dagger V^\dagger, \quad \sigma_3 = V\sigma_0 V^\dagger,$$

$$\sigma_4 = \tfrac{1}{3}|0-1\rangle\langle0-1| + \tfrac{1}{3}|1\rangle\langle1| + \tfrac{1}{3}|1+2\rangle\langle1+2|,$$

$$\sigma_5 = U\sigma_4 U^\dagger, \quad \sigma_6 = UV\sigma_4 V^\dagger U^\dagger, \quad \sigma_7 = V\sigma_4 V^\dagger,$$

where we have introduced the unitary operators

$$U = -|0\rangle\langle0| + |1\rangle\langle1| + |2\rangle\langle2|,$$

$$V = |0\rangle\langle2| + |1\rangle\langle1| + |2\rangle\langle0|.$$

Any measurement $\{\pi_j\}$ discriminating optimally between the states $\{\rho_j\}$ with priors $\{p_j\}$ satisfies the so-called Helstrom conditions, which are known to be both necessary and sufficient [33–36]:

$$\sum_j p_j \rho_j \pi_j - p_k \rho_k \geqslant 0, \tag{8}$$

$$\pi_i(p_i\rho_i - p_j\rho_j)\pi_j = 0. \tag{9}$$

Denoting $\Gamma = \sum_i p_i\rho_i\pi_i$, an alternative, equivalent condition, which is sometimes easier to use in practice, is obtained by summing over i in Eq. (9), giving

$$(\Gamma - p_j\rho_j)\pi_j = 0. \tag{10}$$

Our strategy to find the optimal probability of success for Alice's measurement is to use the Helstrom conditions constructively to find $\Gamma = \frac{1}{8}\sum_i \sigma_i\pi_i$ such that the operators $\Gamma - \frac{1}{8}\sigma_j$ are rank-two positive semidefinite for all j. Thus, Eq. (8) is satisfied, and choosing π_j to be a weighted projector onto the zero eigenvalue eigenstate of $\Gamma - \frac{1}{8}\sigma_j$ ensures that Eq. (10) is also satisfied. If we can choose the weights such that the resulting operators π_j sum to the identity, we

have succeeded in finding an optimal measurement. This task is facilitated by noting that the states have rather a lot of symmetry. It is clear that the set $\{\sigma_k\}$ is invariant under the action of the two unitary operators U and V. Hence we search for a measurement $\{\pi_i\}$ with the same symmetry properties. It follows that we are searching for an operator $\Gamma = \frac{1}{8}\sum_i \sigma_i\pi_i$ which is invariant under U and V: $\Gamma = U\Gamma U^\dagger = V\Gamma V^\dagger$, which further implies that Γ is of the form

$$\Gamma = p(|0\rangle\langle0| + |2\rangle\langle2|) + q|1\rangle\langle1|.$$

Finally, using the symmetry again, we need only check the condition (8) for σ_0 and σ_4, and the rest follow by construction. Imposing that each of $\Gamma - \frac{1}{8}\sigma_0$ and $\Gamma - \frac{1}{8}\sigma_4$ have one zero eigenvalue allows us to solve for p and q, giving $p \simeq 0.110$, $q \simeq 0.093$, and $P_{\text{corr}} = \frac{8}{3}\text{Tr}(\Gamma) = \frac{8}{3}(2p+q) \simeq 0.836$. We note without proof that we can indeed form a resolution of the identity from the resulting operators $\{\pi_i\}$, which therefore define an optimal measurement. Finally, we recall that the simplified problem of discriminating the three mixed states $\{\rho_0,\rho_1,\rho_2\}$ given above leads to a problem of discriminating between 27 subsets on Alice's side. Performing the same analysis as above, it is readily verified that the measurement just derived, which optimally discriminates the eight subsets $\{\mathcal{S}_0,\ldots,\mathcal{S}_7\}$, remains optimal. It is tedious but straightforward to check that the Helstrom condition (8) is satisfied for the remaining states, which are therefore never identified.

We thus find that for these cases, it is two-way classical communication that significantly boosts the distinguishability of the states and that quantum communication provides only a small additional boost in one case. It is known, of course, that two-way communication is more powerful than one-way communication; however explicit, quantitative gaps for the problem of discriminating orthogonal states have been shown in the literature only for measurements on entangled states (see, e.g., [16,21]). It is surprising that even a single round of two-way classical communication can provide such a significant improvement in measurements on pure product states.

The optimal sequential measurement is a well-motivated indicator of achievable experimental performance in local measurement schemes: many rounds of measurement and classical communication quickly become infeasible and further require quantum memories to store the local quantum systems. Thus, even for rather simple cases and when information is encoded in product states, an appreciable gap can exist between the performance of the best readily achievable local measurement and the theoretically allowed optimum measurement. In practical terms, this is arguably a much stronger manifestation of nonlocality without entanglement than the known theoretical cases—albeit of a different flavor.

[1] J. S. Bell, Physics **1**, 195 (1964).

[2] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).

[3] 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).

[4] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, Comm. Math. Phys. **323**, 1121 (2013).

[5] E. Chitambar and M.-H. Hsieh, Phys. Rev. A **88**, 020302(R) (2013).

[6] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[7] D. Brody and B. Meister, Phys. Rev. Lett. **76**, 1 (1996).

[8] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[9] B. Groisman and L. Vaidman, J. Phys. A: Math. Gen. **34**, 6881 (2001).

[10] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).

[11] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).

[12] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).

[13] P.-X. Chen and C.-Z. Li, Phys. Rev. A **68**, 062107 (2003).

[14] P.-X. Chen and C.-Z. Li, Phys. Rev. A **70**, 022306 (2004).

[15] S. De Rinaldis, Phys. Rev. A **70**, 022309 (2004).

[16] M. Owari and M. Hayashi, New J. Phys. **10**, 013006 (2008).

[17] Y. Feng and Y. Shi, IEEE Trans. Inf. Theory **55**, 2799 (2009).

[18] J. Calsamiglia, J. I. de Vicente, R. Muñoz-Tapia, and E. Bagan, Phys. Rev. Lett. **105**, 080504 (2010).

[19] S. M. Cohen, Phys. Rev. A **84**, 052322 (2011).

[20] B. L. Higgins, A. C. Doherty, S. D. Bartlett, G. J. Pryde, and H. M. Wiseman, Phys. Rev. A **83**, 052314 (2011).

[21] M. Nathanson, Phys. Rev. A **88**, 062316 (2013).

[22] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg, Phys. Rev. Lett. **111**, 183601 (2013).

[23] Z.-C. Zhang, Q.-Y. Wen, F. Gao, G.-J. Tian, and T.-Q. Cao, Quantum Inf. Proc. **13**, 795 (2014).

[24] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, and A. Winter, Commun. Math. Phys. **328**, 303 (2014).

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

[26] Z.-C. Zhang, K.-Q. Feng, F. Gao, and Q.-Y. Wen, Phys. Rev. A **91**, 012329 (2015).

[27] Y.-L. Wang, M.-S. Li, Z.-J. Zheng, and S.-M. Fei, Quantum Inf. Proc. **15**, 1661 (2016).

[28] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[29] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology: Proceedings of Crypto* Vol. 82 (Plenum, New York, 1982), p. 267.

[30] S. Croke, S. M. Barnett, and G. Weir (unpublished).

[31] S. M. Barnett, *Quantum Information* (Oxford University Press, Oxford, 2009).

[32] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1995).

[33] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).

[34] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **IT-21**, 125 (1975).

[35] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[36] S. M. Barnett and S. Croke, J. Phys. A: Math. Theor. **42**, 062001 (2009).