Nonlocality, Asymmetry, and Distinguishing Bipartite States

Jonathan Walgate* and Lucien Hardy†

Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom

(Received 19 February 2002; published 16 September 2002)

Entanglement is a useful resource because some global operations cannot be locally implemented using classical communication. We prove a number of results about what is and what is not locally possible. We focus on orthogonal states, which can always be globally distinguished. We establish the necessary and sufficient conditions for a general set of 2×2 quantum states to be locally distinguishable, and for a general set of $2 \times n$ quantum states to be distinguished given an initial measurement of the qubit. These results reveal a fundamental asymmetry to nonlocality, which is the origin of "nonlocality without entanglement," and we present a very simple proof of this phenomenon.

DOI: 10.1103/PhysRevLett.89.147901 PACS numbers: 03.67.Hk, 03.65.Ud

Many global operations cannot be performed using only local operations and classical communication (LOCC). This one fact underpins the use of entanglement as a resource across quantum information theory. Yet there is no clear delineation of what is and what is not locally possible. What evidence there is can appear counterintuitive, given the close link between entanglement and nonlocal behavior. Any two orthogonal entangled states can be distinguished just as well using LOCC as they can globally [1] (see also [2,3]). But there exist larger sets of orthogonal separable states that LOCC cannot reliably distinguish. Bennett *et al.* presented a set of nine pure product states which, they proved, cannot be distinguished exactly with LOCC [4]. (In fact, they proved the stronger result that any approximate method to distinguish these states must introduce a finite error.) Sets of states exhibiting such "nonlocality without entanglement" have been linked with unextendible product bases (UPBs) [5,6], in that the members of a UPB cannot be exactly LOCC distinguished. Yet this cannot be fundamental to the phenomenon, for there are LOCC indistinguishable sets that form complete orthogonal bases [4].

A set of states, shared between Alice and Bob, is exactly locally distinguishable if there is some sequence of local operations and classical communications that will determine with certainty which state they own. The Bell states present a simple example of an orthogonal set that is not locally distinguishable—a global measurement is needed to tell them apart [7].

In all LOCC protocols, one party must "go first" and perform the initial operation. We formalize this notion to obtain a powerful theorem establishing the necessary and sufficient conditions that a set of $2 \times n$ orthogonal quantum states are exactly distinguishable, with the owner of the qubit going first [see Definition 1, Theorem 1 (below)]. This result is of particular use in characterizing the distinguishability of 2×2 states. Recent investigations by Ghosh *et al.*, focusing on distillable entanglement, have revealed groups of orthogonal 2×2 states that are not LOCC distinguishable [8]. Using our result, we can now completely specify the distinguishable and undistinguishable 2×2 sets.

Our theorem also provides insight into nonlocality without entanglement. Groisman and Vaidman [9] recently constructed a proof that Bennett *et al.*'s nine states cannot be exactly distinguished; they employed the idea that one party must go first, by considering results derived from a restriction to one-way communication. Theorem 1 allows us to develop a more transparent and natural proof of this important theorem, and go some way towards illuminating the origin of the phenomenon.

Definition 1: Alice goes first if Alice is the first person to perform a nontrivial measurement upon the system.—Note that this does not restrict two-way classical communication between Alice and Bob, nor does it limit the number of measurements they may perform sequentially. Note also that in all LOCC protocols *someone* goes first.

Alice's first local operation will be described by a superoperator, , which comprises a set $\{M_m\}$ of Krauss operators, one for every possible outcome, m. The probability of a given state yielding a certain outcome is $p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle$, . The objects $M_m^\dagger M_m$ are the positive operator-valued measure (POVM) elements corresponding to each measurement outcome m. They sum to identity. Being positive operators they are diagonalizable, with real, nonnegative eigenvalues. We will say that a measurement is *trivial* if all the POVM elements are proportional to the identity operator since such a measurement yields no information about the state. Any measurement not of this type will be called *nontrivial.*

Theorem 1: *Alice and Bob share a $2 \times n$ dimensional quantum system: Alice has a qubit, and Bob an n-dimensional system that may be entangled with that qubit. If Alice goes first, a set of l orthogonal states $\{|\psi_i\rangle\}$ is exactly locally distinguishable if and only if there is a basis $\{|0\rangle, |1\rangle\}_A$ such that in that basis*

$$|\psi_i\rangle = |0\rangle_A|\eta_0^i\rangle + |1\rangle_A|\eta_1^i\rangle_B, \tag{1}$$

where $\langle\eta_0^i|\eta_0^j\rangle = \langle\eta_1^i|\eta_1^j\rangle = 0$ if $i \neq j$.

Proof: The proof of sufficiency is simple. If there is a basis such that the l states can be written as above, the states may be locally distinguished as follows. Alice measures in the $\{|0\rangle, |1\rangle\}_A$ basis and communicates the result to Bob. Bob then measures in the corresponding orthogonal basis $\{|\eta_0^i\rangle\}$ or $\{|\eta_1^i\rangle\}$, successfully distinguishing the states.

The proof of necessity is more complicated. Suppose that Alice goes first. The l states must be reliably distinguished. Therefore, after each and every possible result of Alice's measurement, all those states that have not been eliminated as possibilities must remain orthogonal, and are thus potentially distinguishable. Therefore for all pairs of states $|\psi_i\rangle$, $|\psi_j\rangle$, and for all measurement results m, either that pair remains orthogonal postmeasurement or else one of that pair of states has been eliminated. Either $\langle\psi_i|M_m^\dagger M_m|\psi_j\rangle = 0$, or $\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = 0$, or $\langle\psi_j|M_m^\dagger M_m|\psi_j\rangle = 0$.

Consider one POVM element that is not proportional to identity (such an element must exist since Alice's measurement is nontrivial), and take as our $\{|0\rangle, |1\rangle\}_A$ basis the basis in which it is diagonal as follows:

$$M_m^\dagger M_m = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \qquad \alpha > \beta \geq 0.$$

The states $|\psi_i\rangle$, expanded in the $\{|0\rangle, |1\rangle\}_A$ basis at Alice's end can always be written in the form of Eq. (1). We must now prove the stated orthogonality conditions on the $|\eta\rangle$.

For the moment, consider only two states: $|\psi_i\rangle$ and $|\psi_j\rangle$. If Alice eliminates neither pair from the running, those states must remain orthogonal, so $\langle\psi_i|M_m^\dagger M_m|\psi_j\rangle = 0$. Since the original possible states are orthogonal as well, we require that $\langle\eta_0^i|\eta_0^j\rangle + \langle\eta_1^i|\eta_1^j\rangle = 0$, $\alpha\langle\eta_0^i|\eta_0^j\rangle + \beta\langle\eta_1^i|\eta_1^j\rangle = 0$. These simultaneous equations combine thus: $(\alpha - \beta)\langle\eta_1^i|\eta_1^j\rangle = 0$, $(\beta - \alpha)\langle\eta_0^i|\eta_0^j\rangle = 0$. Since $\alpha \neq \beta$,

$$\langle\eta_0^i|\eta_0^j\rangle = \langle\eta_1^i|\eta_1^j\rangle = 0. \tag{2}$$

Hence, in the case that neither state is eliminated, this pair of states must be in the form given in the theorem.

Now consider the special case where Alice achieves a negative identification herself, and thus $\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = 0$ or $\langle\psi_j|M_m^\dagger M_m|\psi_j\rangle = 0$. This tells us a great deal about that state. Imagine she has eliminated $|\psi_i\rangle$. From (1) and (3), we know that $\langle\eta_0^i|\eta_0^i\rangle + \langle\eta_1^i|\eta_1^i\rangle = 1$, $\alpha\langle\eta_0^i|\eta_0^i\rangle + \beta\langle\eta_1^i|\eta_1^i\rangle = 0$. These simultaneous equations reveal that:

$$\alpha(\langle\eta_1^i|\eta_1^i\rangle - 1) = \beta\langle\eta_1^i|\eta_1^i\rangle. \tag{3}$$

But $\alpha > \beta \geq 0$ and $0 \leq \langle\eta_1^i|\eta_1^i\rangle \leq 1$. This means that there is only one possible solution to Eq. (3): $\beta = 0$, $\langle\eta_1^i|\eta_1^i\rangle = 1$. This implies that $|\psi_i\rangle$ is the product state $|1\rangle|\eta_1^i\rangle$. In this case, the other state must take the form:

$$|\psi_j\rangle = |0\rangle_A|\eta_0^j\rangle_B + |1\rangle_A|\eta_1^{i\perp}\rangle_B \tag{4}$$

Again, we see that this particular pair of states have the form given in the theorem.

Hence, in all cases, any pair of states must be in the form given in the theorem. But the basis $\{|0\rangle, |1\rangle\}_A$ for which this is true depends only on the POVM element we have been considering, and that element is independent of the states themselves. Therefore $\{|0\rangle, |1\rangle\}_A$ is a basis in which all the states are represented thus: $|\psi_i\rangle = |0\rangle_A|\eta_0^i\rangle_B + |1\rangle_A|\eta_1^i\rangle_B$, where $\langle\eta_0^i|\eta_0^j\rangle = \langle\eta_1^i|\eta_1^j\rangle = 0$ if $i \neq j$. This completes the proof. □

Theorem 1 depends upon the first measurement being made by the owner of the qubit. If we are dealing with 2×2 states, then the proof is applicable to both Alice and Bob going first. Thus, any set of 2×2 states that can be locally distinguished must be expressible in form (1). This allows us to derive the conditions for LOCC distinguishing all possible sets of orthogonal 2×2 states. Analysis has already shown that pairs of orthogonal states can always be LOCC distinguished:

Theorem 2 (Walgate *et al.*): *Two orthogonal* 2×2 *states can always be exactly locally distinguished.*

Proof: It was proven by Walgate *et al.* [1] that Alice can always find a basis of form (1) in which two states (of any dimension) can be distinguished. □

Theorem 3: *Three orthogonal* 2×2 *states can be exactly locally distinguished if and only if at least two of those states are product states.*

Proof: From Theorem 2 it follows that any three states can be written thus:

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A|\eta_0\rangle_B + |1\rangle_A|\eta_1\rangle_B, \\ |\psi_2\rangle &= |0\rangle_A|\eta_0^\perp\rangle_B + |1\rangle_A|\eta_1^\perp\rangle_B, \\ |\psi_3\rangle &= |0\rangle_A|\nu_0\rangle_B + |1\rangle_A|\nu_1\rangle_B. \end{aligned}$$

If this set is to be locally distinguishable with Alice going first, there must be some choice of $\{|0\rangle, |1\rangle\}_A$ such that $\langle\eta_0|\nu_0\rangle = \langle\eta_0^\perp|\nu_0\rangle = 0$, and $\langle\eta_1|\nu_1\rangle = \langle\eta_1^\perp|\nu_1\rangle = 0$. But there is no room in Bob's two-dimensional Hilbert space for three mutually orthogonal states. Therefore in each of these cases, one of the two (unnormalized) states forming the inner product must have zero magnitude. Since the states $|\psi_i\rangle$ must themselves be normalized, this means that two of them must be product states. This leaves us with the triplet:

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A|\eta_0\rangle_B + |1\rangle_A|\eta_1\rangle_B, \\ |\psi_2\rangle &= |0\rangle_A|\eta_0^\perp\rangle_B, \\ |\psi_3\rangle &= |1\rangle_A|\eta_1^\perp\rangle_B. \end{aligned} \tag{5}$$

Three orthogonal 2×2 states can be locally distinguished with Alice going first if and only if they take the form (5). We can reconstruct this argument for Bob going first, with Bob's qubit providing the orthonormal basis. The form of states we obtain is a mirror image of (5), with only the $|\,\rangle_A$ and $|\,\rangle_B$ indexes reversed. States of this form can still be locally distinguished, but now with Bob going first. It is easy to verify that these two arrangements encompass all sets of three orthogonal 2×2 states

containing two product states. Therefore, three orthogonal 2×2 states can be locally distinguished if and only if at least two of those states are product states. □

Theorem 4: *Four orthogonal* 2×2 *states can be exactly locally distinguished if and only if all of them are product states.*

Proof: Given Theorem 3, any three of a set of four distinguishable states must contain at least two product states. Thus, two of $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$, two of $|\psi_1\rangle, |\psi_2\rangle, |\psi_4\rangle$, and two out of $|\psi_1\rangle, |\psi_3\rangle, |\psi_4\rangle$ must be product states. It follows that at least three of the four states are product states—in general, for Alice going first, three such states can be written:

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A|\phi\rangle_B, \\ |\psi_2\rangle &= |1\rangle_A|\theta\rangle_B, \\ |\psi_3\rangle &= |0\rangle_A|\phi^\perp\rangle_B \end{aligned} \tag{6}$$

There is only one state that is orthogonal to the above three, and that is also a product state:

$$|\psi_4\rangle = |1\rangle_A|\theta^\perp\rangle_B. \tag{7}$$

Four orthogonal 2×2 states can be locally distinguished with Alice going first if and only if all of them are product states of form (6) and (7). Again, a complementary argument with Bob going first provides another set of distinguishable product states, which together with set (6) and (7) covers all possibilities. Therefore four orthogonal 2×2 states can be locally distinguished if and only if all of them are product states. □

A 2×2 system has a four-dimensional Hilbert space, and so cannot contain a set of more than four mutually orthogonal states. Thus, this completes our analysis.

The sets of three and four LOCC distinguishable 2×2 states (5) and (6) + (7) display a remarkable asymmetry: The states can be distinguished if one person goes first, but not the other way round.

Definition 2: A set of bipartite states is asymmetrically *distinguishable if there is a specific party such that those states can only be exactly LOCC distinguished when that party goes first.*

Consider the triplet (5). With Alice going first, it is clear how to distinguish these states, but if Bob goes first this cannot be achieved because, as can be easily shown, there is no basis $\{|0\rangle, |1\rangle\}_B$ in which the states take the form of Theorem 1. This three-state asymmetry manifests if and only if one of the states is entangled. The corresponding four-state asymmetry, however, involves only separable states.

The four states (6) + (7) may be locally distinguished if Alice goes first, but not if Bob goes first so long as $|\langle\phi|\theta\rangle| \neq 1$. Bob can do nothing reliable until he receives some information from Alice. Conversely, Alice can only reliably discover which state she possesses by allowing Bob to discover, and hoping that he shares his knowledge. An example of this phenomenon was discussed by Groisman and Vaidman [9]. They imposed stronger constraints, limiting Alice and Bob to one-way communication in the direction $B \rightarrow A$, and showed that the states given by $|\phi\rangle_B = |0\rangle_B$, $|\theta\rangle_B = |0 + 1\rangle_B$ cannot be distinguished in that circumstance. This is a four-state example of the asymmetry we have outlined, which arises not from a one-way communication restriction, nor indeed any practical limits on Alice and Bob's LOCC protocol. Rather, this asymmetry appears in the set of states itself: Alice and Bob will know without consultation who must make the first move.

This asymmetry emerges from the most basic level. The two states $|0\rangle_A|\phi\rangle_B$ and $|1\rangle_A|\theta\rangle_B$ are, of course, orthogonal, but while Alice's intervention is both necessary and sufficient to distinguish them, Bob's is not. The point is the orthogonality of any pair of product states must be *locally* manifested. One might naively expect that the addition of the second pair of orthogonal states, "completing" the 2×2 Hilbert space, would provide a balance, and reintroduce symmetry. This is not the case.

There is one and only one "symmetric" set of four orthogonal 2×2 states, in the sense that only one set can be reliably discriminated no matter who measures first: $|00\rangle$, $|10\rangle$, $|01\rangle$, $|11\rangle$. An interesting property of these states is that they can encode a single bit such that neither Alice nor Bob can access it without help from the other. If we let $|00\rangle$ and $|11\rangle$ encode "0" and $|10\rangle$ and $|01\rangle$ encode "1," both Alice and Bob have the power to reveal the bit to their partner, but neither can gain any access to it directly.

Nonlocality without entanglement occurs when a set of product states cannot be distinguished with either Alice or Bob going first. Bennett *et al.*'s paper considered a set of nine such states, which were symmetric under the exchange of Alice and Bob's systems. But this symmetry is not fundamental to the nonlocality. In its simplest form, we can think of nonlocality without entanglement manifesting asymmetrically for only one party. Groisman and Vaidman used this insight when they created a proof of Bennett's result built from their observations on one-way indistinguishability [9]. What is really at issue is not the kind of LOCC protocols employed by Alice and Bob, nor the content of their communications, but the asymmetric properties of subsets of the states themselves. Framed this way, the "full-blown" phenomenon has a very simple proof.

Theorem 5 (Bennett *et al.*): *The nine* 3×3 *states depicted in Fig.* 1 *and specified below cannot be exactly distinguished using only local operations and classical communication.*

$$\begin{aligned} |\psi_1\rangle &= |1\rangle_A|1\rangle_B, \\ |\psi_{2,3}\rangle &= |0\rangle_A|0 \pm 1\rangle_B, \\ |\psi_{4,5}\rangle &= |2\rangle_A|1 \pm 2\rangle_B, \\ |\psi_{6,7}\rangle &= |1 \pm 2\rangle_A|0\rangle_B, \\ |\psi_{8,9}\rangle &= |0 \pm 1\rangle_A|2\rangle_B. \end{aligned} \tag{8}$$

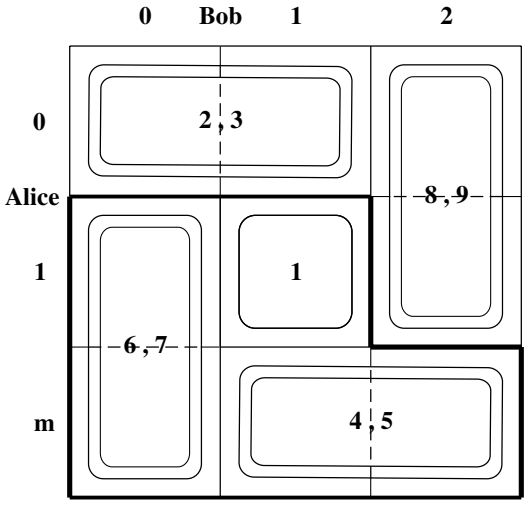

FIG. 1. Bennett *et al.*'s depiction of the states as a set of dominoes.

Proof: We will prove that the states cannot be distinguished if Alice goes first. If so, then by their symmetry the states cannot be distinguished with Bob going first either.

Alice performs a general measurement, represented by a set of 3×3 POVM elements $M_m^\dagger M_m$, which we will write in the $\{|0\rangle, |1\rangle, |2\rangle\}_A$ basis:

$$M_m^\dagger M_m = \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix}.$$

The effect of this positive operator upon states 1, 4, 5, 6, and 7 (highlighted in bold in the diagram) is entirely specified by those elements drawn from the $\{|1\rangle, |2\rangle\}_A$ subspace: m_{11}, m_{12}, m_{21}, and m_{22}. This select set of states is of dimension 2×3, yet there is palpably no basis in which Alice can express them in the form of Theorem 1. These states are thus indistinguishable with Alice going first, and Alice cannot perform a nontrivial measurement upon the $\{|1\rangle, |2\rangle\}_A$ subspace. Thus, the corresponding submatrix must be proportional to the identity, and, hence, $m_{11} = m_{22}$ and $m_{12} = m_{21} = 0$.

Exactly the same argument can be made for the states 1, 2, 3, 8, and 9 and the $\{|0\rangle, |1\rangle\}_A$ subspace. Therefore $m_{00} = m_{11}$ and $m_{01} = m_{10} = 0$. Since $M_m^\dagger M$ is Hermitian, $m_{20} = m_{02}^*$. Alice's POVM element must look like this:

$$M_m^\dagger M_m = \begin{pmatrix} \alpha & 0 & m_{02} \\ 0 & \alpha & 0 \\ m_{02}^* & 0 & \alpha \end{pmatrix}. \tag{9}$$

Now consider the $\{|0\rangle, |2\rangle\}_A$ subspace, and the states 2 and 4. Alice's measurement must either leave them orthogonal or distinguish them outright. In the former case, we demand that $\langle\psi_4|M_m^\dagger M_m|\psi_2\rangle = 0$. Simple algebra shows that, given , $\langle\psi_4|M_m^\dagger M_m|\psi_2\rangle = \frac{1}{2} m_{02}^*$. Thus, $m_{02} = 0$ and $M_m^\dagger M_m$ is proportional to the identity.

If Alice distinguishes the states outright then for one of states 2 and 4, $\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = 0$. But given (9), $\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \alpha$. Thus, $\alpha = 0$ and, since POVM elements must be positive, $M_m^\dagger M_m$ is the null matrix.

The above argument applies to all possible measurement outcomes, and thus all of Alice's POVM elements must be proportional to the identity if she and Bob are to distinguish the states. By definition, Alice cannot go first; by the symmetry of states (8), neither can Bob. Therefore the states (8) cannot be distinguished using only local operations and classical communication. This completes the proof. □

We have shown that sets of orthogonal $2 \times n$ states can be distinguished only if they can be written in a particular form, and we have seen how this result dictates the distinguishability of the 2×2 states. "Nonlocality without entanglement" can be constructed from the asymmetries that arise in sets of such states.

We thank the U.K. EPSRC and the Royal Society for funding this research.

*Electronic address: jon.walgate@qubit.org
†Electronic address: lucien.hardy@qubit.org

[1] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[2] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001).
[3] Y.-X. Chen and D. Yang, Phys. Rev. A **65**, 022320 (2002).
[4] 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).
[5] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[6] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, quant-ph/9908070.
[7] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).
[8] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De), and U. Sen, quant-ph/0111136.
[9] B. Groisman and L. Vaidman, J. Phys. A **34**, 6881 (2001).