Local Distinguishability of Multipartite Orthogonal Quantum States

Jonathan Walgate,* Anthony J. Short, Lucien Hardy, and Vlatko Vedral
Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom
(Received 27 July 2000)

We consider one copy of a quantum system prepared in one of two orthogonal pure states, entangled or otherwise, and distributed between any number of parties. We demonstrate that it is possible to identify which of these two states the system is in by means of local operations and classical communication alone. The protocol we outline is both completely reliable and completely general; it will correctly distinguish any two orthogonal states 100% of the time.

PACS numbers: 03.67.–a, 03.65.–w, 89.70.+c

Pure quantum states may only be perfectly distinguished from one another when they are orthogonal. That is, a state $|\psi\rangle$ may be reliably distinguished from another $|\phi\rangle$, only if $\langle\psi\,|\,\phi\rangle = 0$. We will show that if $\langle\psi\,|\,\phi\rangle = 0$ for given $|\psi\rangle$ and $|\phi\rangle$, then $|\psi\rangle$ may always be distinguished from $|\phi\rangle$ by means of local operations and classical communication (LOCC). This may be surprising, since quantum systems can encode information that may only be extracted by analyzing the system *as a whole.* This well-known phenomenon—entanglement—forms the basis of many recently proposed quantum schemes, such as cryptography [1–3], computation [4], and enhanced communication [5]. A tempting interpretation is that "entangled information" can only be uncovered using global measurements upon the system as a whole. But this is not the case; in our very general situation local measurements, sequentially dependent upon classically communicated prior measurement results, suffice to identify orthogonal entangled quantum states.

Schemes for distinguishing between a set of quantum states, both pure and mixed, have been considered by various authors [6–11]. Closely related to the present paper is the work of Bennett *et al.* [9] who showed that there exist sets of orthogonal product states that cannot be distinguished by LOCC.

Alice and Bob each hold part of a quantum system, which occupies one of two possible orthogonal quantum states $|\psi\rangle$ and $|\phi\rangle$. Alice and Bob know the precise form of $|\psi\rangle$ and $|\phi\rangle$, but have no idea which of these possible states they actually possess: They will have to perform some measurements to find out. A global measurement would suffice, but alas Alice and Bob cannot afford to meet up. Fortunately for them, they are on speaking terms, as one phone call is all they require. This situation, LOCC, is of primary relevance to most applications of entanglement.

The strategy Alice and Bob adopt is simple. They can always find a basis in which the two orthogonal states can be represented:

$$\begin{aligned} |\psi\rangle &= |1\rangle_{A'}|\eta_1\rangle_B + \cdots + |l\rangle_{A'}|\eta_l\rangle_B\,, \\ |\phi\rangle &= |1\rangle_{A'}|\eta_1^\perp\rangle_B + \cdots + |l\rangle_{A'}|\eta_l^\perp\rangle_B\,, \end{aligned} \tag{1}$$

where $\{|i\rangle_{A'}$ for $i = 1$ to $l\}$ form some orthogonal basis set for Alice, $\{|\eta_1\rangle_B, \ldots, |\eta_l\rangle_B\}$ are not normalized, and $|\eta_i^\perp\rangle_B$ is orthogonal to $|\eta_i\rangle_B$. Alice simply measures her part of the system in such a basis, and communicates the result, i, to Bob. Bob then has an easy task: he may distinguish locally between $|\eta_i\rangle_B$ and $|\eta_i^\perp\rangle_B$ and thereby know which state he and Alice shared to begin with.

Alice and Bob do not initially know this ideal measurement basis, but they do start out knowing the precise form of two states that might correspond to their shared quantum system. These two possible states, $|\psi\rangle$ and $|\phi\rangle$, are orthogonal, so that $\langle\psi\,|\,\phi\rangle = 0$. We can represent them in the following, entirely general way:

$$\begin{aligned} |\psi\rangle &= |1\rangle_{A}|\eta_1\rangle_B + \cdots + |n\rangle_{A}|\eta_n\rangle_B\,, \\ |\phi\rangle &= |1\rangle_{A}|\nu_1\rangle_B + \cdots + |n\rangle_{A}|\nu_n\rangle_B\,, \end{aligned} \tag{2}$$

where $\{|1\rangle_A, \ldots, |n\rangle_A\}$ form an orthonormal basis set for Alice, and the vectors $\{|\eta_1\rangle_B, \ldots, |\eta_n\rangle_B\}$ and $\{|\nu_1\rangle_B, \ldots, |\nu_n\rangle_B\}$ are not normalized and also not necessarily orthogonal. Alice and Bob can express the vectors $\{|\eta_1\rangle_B, \ldots, |\eta_n\rangle_B\}$ and $\{|\nu_1\rangle_B, \ldots, |\nu_n\rangle_B\}$ as a superposition of a set of arbitrary basis vectors $\{|1\rangle_B, \ldots, |m\rangle_B\}$ in Bob's space,

$$|\eta_i\rangle_B = \sum_j F_{ij}|\,j\rangle_B, \qquad |\nu_i\rangle_B = \sum_j G_{ij}|\,j\rangle_B\,, \tag{3}$$

where the elements F_{ij} and G_{ij} form two $n \times m$ matrices F and G. These matrices preserve all the information Alice and Bob hold about states $|\psi\rangle$ and $|\phi\rangle$. Because of the way they are constructed, the matrix $FG^\dagger$ takes the following form:

$$FG^\dagger = \begin{pmatrix} \langle\nu_1\,|\,\eta_1\rangle & \cdots & \langle\nu_1\,|\,\eta_n\rangle \\ \vdots & \ddots & \vdots \\ \langle\nu_n\,|\,\eta_1\rangle & \cdots & \langle\nu_n\,|\,\eta_n\rangle \end{pmatrix}. \tag{4}$$

We can see this is the case by inspection, because $\langle\nu_i\,|\,\eta_j\rangle = \sum_{k=1}^n F_{jk}G_{ik}^*$. The matrix $FG^\dagger$ encapsulates a great deal of significant information for Alice and Bob about the relationship between the states $|\psi\rangle$ and $|\phi\rangle$. Since we know by the conditions of the problem that $\langle\phi\,|\,\psi\rangle = 0$, we know that

 0031-9007/00/85(23)/4972(4)$15.00

$$\langle \phi \mid \psi \rangle = \sum_{i=1}^{n} \langle \nu_i \mid \eta_i \rangle = \mathrm{Trace}(FG^\dagger) = 0\,. \qquad (5)$$

But the $FG^\dagger$ matrix holds more information than the simple fact of the states' orthogonality. It also encodes the key to distinguishing between these two possible states. Alice plans to distinguish $|\psi\rangle$ and $|\phi\rangle$ by finding some basis—any basis—in which she can describe her part such that the states $|\psi\rangle$ and $|\phi\rangle$ take the more restricted form of (1). Alice must choose her $\{|1\rangle_A, \ldots, |n\rangle_A\}$ basis carefully such that no matter what result $|i\rangle_A$ she obtains, Bob can surely distinguish between his possible states. This means that, for all i, $|\nu_i\rangle$ must be orthogonal to $|\eta_i\rangle$. Thus we can write down our distinguishability criterion:

$$\forall\, i \quad \langle \nu_i \mid \eta_i \rangle = 0\,. \qquad (6)$$

In other words, in our matrix representation, we require the diagonal elements of $FG^\dagger$ to be zero. Alice can alter the form of $FG^\dagger$ by changing the basis in which she describes and measures her system. She has a great deal of choice in this regard: Any orthogonal basis set spanning her space will provide a description of form (2), and thus some matrix $FG^\dagger$ of form (4). When she changes her orthonormal basis set, this changes the form of the matrices F and G, and thus changes the form of $FG^\dagger$. In fact, unitary transformations of Alice's measurement basis map to the conjugate unitary transformations upon $FG^\dagger$.

Theorem 1.—A unitary transformation U^A upon Alice's measurement basis will transform the matrix $FG^\dagger$ to $U^{A*}(FG^\dagger)U^{A*\dagger}$.

Proof: From (2), $|\psi\rangle = \sum_i |i\rangle_A |\eta_i\rangle_B$. Alice's unitary transformation acts thus: $|i\rangle_A = \sum_j U_{ij}^{A\dagger} |j'\rangle_A$. From (3) it follows that, in Alice's new basis $\{|1'\rangle_A, \ldots, |n'\rangle_A\}$,

$$|\psi\rangle = \sum_{ijk} U_{ij}^{A\dagger} |j'\rangle_A F_{ik} |k\rangle_B\,. \qquad (7)$$

For true generality, we consider Bob might assist Alice by unitarily rotating his basis by U^B. We therefore write $|k\rangle_B = \sum_l U_{kl}^{B\dagger} |l'\rangle_B$, giving $|\psi\rangle = \sum_{ijkl} |j'\rangle_A |l'\rangle_B U_{ij}^{A\dagger} F_{ik} U_{kl}^{B\dagger}$. Since $U_{ij}^{A\dagger} = U_{ji}^{A*}$, we can rewrite this as

$$\psi = \sum_{ijkl} |j'\rangle_A |l'\rangle_B U_{ji}^{A*} F_{ik} U_{kl}^{B\dagger}\,. \qquad (8)$$

By analogy with (2) and (3), this means that in the new basis of description we have a new matrix F' where $F'_{ik} = \sum_{jl} U_{ji}^{A*} F_{ik} U_{kl}^{B\dagger}$. Under unitary basis rotations by Alice and Bob, our matrices F and G undergo the curious transformations

$$F' = U^{A*} F U^{B\dagger}, \qquad G' = U^{A*} G U^{B\dagger}. \qquad (9)$$

This means that the object of our interest, the $FG^\dagger$ matrix encoding information about the relationship *between* the states, will transform as

$$\begin{aligned} F'G'^\dagger &= (U^{A*} F U^{B\dagger})(U^{A*} G U^{B\dagger})^\dagger \\ &= U^{A*} F U^{B\dagger} U^B G^\dagger U^{A*\dagger} \\ &= U^{A*} (FG^\dagger) U^{A*\dagger} \qquad \Box\,. \end{aligned} \qquad (10)$$

Bob's unitary rotation U^B drops out, as rotations in his basis will not affect the overlaps $\langle \nu_i \mid \eta_j \rangle$ that make up $FG^\dagger$.

If U^A is unitary, then so is U^{A*}. Alice can find a basis of form (1), and thereby satisfy our distinguishability criterion (6), *if and only if* there exists a unitary matrix $U = U^{A*}$ such that $U(FG^\dagger)U^\dagger$ is a "zero-diagonal" matrix (a matrix whose diagonal elements are all zero). A proof that such a unitary matrix always exists constitutes a proof that two orthogonal quantum states can always be distinguished.

Unitary transformations upon Alice's measurement basis translate into (conjugated) unitary transformations upon her specific $FG^\dagger$ matrix. If she can find a unitary rotation that converts this matrix into zero-diagonal form, she can ensure that Bob will be able to distinguish between states $|\psi\rangle$ and $|\phi\rangle$.

We first prove such a rotation always exists in the two-dimensional case, and then show how Alice may use a finite sequence of such 2×2 transformations to zero diagonalize any traceless $n \times n$ matrix.

Theorem 2.—Let M be the wholly general 2×2 matrix $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$. There exists a 2×2 unitary matrix U such that the diagonal elements of $UMU^\dagger$ are equal.

Proof: Let

$$U = \begin{pmatrix} \cos\theta & \sin\theta e^{i\omega} \\ \sin\theta e^{-i\omega} & -\cos\theta \end{pmatrix}.$$

We need the diagonal elements of $UMU^\dagger$ to be equal. This gives us the condition

$$(x - t)\cos 2\theta + \sin 2\theta (y e^{-i\omega} + z e^{i\omega}) = 0\,. \qquad (11)$$

The real and imaginary parts of this equation can be solved for the angles ω and θ:

$$\tan\omega = \frac{\mathrm{Im}(x - t)\mathrm{Re}(z + y) - \mathrm{Re}(x - t)\mathrm{Im}(z + y)}{\mathrm{Re}(x - t)\mathrm{Re}(z - y) + \mathrm{Im}(x - t)\mathrm{Im}(z - y)}, \qquad (12)$$

$$\tan 2\theta = \frac{\mathrm{Re}(x - t)}{\mathrm{Re}(z + y)\cos\omega - \mathrm{Im}(z - y)\sin\omega}\,. \qquad (13)$$

The right-hand side of (12) is always real, and thus there will always be an angle ω that satisfies the equation. Given a definite ω, we can always solve (13) for a definite θ for the same reason. Thus for any 2×2 matrix M, there exists a 2×2 unitary matrix that "equidiagonalizes" it (equalizes all its diagonal elements). This completes the proof $\Box$.

This mathematical result can be applied to the 2×2 dimensional case. Since the $|\psi\rangle$ and $|\phi\rangle$ states are orthogonal, the corresponding $FG^\dagger$ matrix is traceless, in which case equidiagonalization constitutes zero diagonalization. Equations (12) and (13) therefore always pick out a specific unitary transformation that will zero diagonalize $FG^\dagger$. By measuring in that basis, Alice and Bob can always distinguish between the two possible orthogonal states of their system.

We want to consider all situations of greater dimensionality than 2, but we first concentrate on situations where Alice's Hilbert space has 2^k dimensions (where k is some positive integer). The $AB^\dagger$ matrix has the same dimensionality and will have $2^k \times 2^k$ elements. Note that while this particular class of $FG^\dagger$ matrices—those of dimension 2^k—may seem limited, it includes all quantum states comprising sets of qubits. In such cases, Alice can adopt a simple strategy to equidiagonalize this potentially huge matrix in a relatively small number of steps. We know from Theorem 2 above that Alice may unitarily rotate any two diagonal elements in her $FG^\dagger$ matrix so that they become equal. By grouping the diagonal elements into 2^{k-1} pairs, and equidiagonalizing each pair, she can create 2^{k-1} equal pairs.

Both elements of an equal pair can then be individually made equal to the elements of another equal pair, using only two 2×2 unitary transformations. Thereby, Alice can create 2^{k-2} "quartets" of equal diagonal elements with just 2^{k-1} further 2×2 unitary transformations. By repeating this process k times, Alice will set all the diagonal elements exactly equal. If her $FG^\dagger$ matrix has 2^k diagonal elements, then $k2^{k-1}$ elementary operations will serve to equidiagonalize it. This satisfies Alice's requirements: Since she knows that her physical $FG^\dagger$ matrix is traceless, she knows that all the diagonal elements $\langle \nu_i \mid \eta_i \rangle$ will be thereby set to zero. Therefore Alice and Bob can distinguish the two orthogonal states. Of course, Alice need not physically enact each and every separate 2×2 unitary transformation. A single $2^k \times 2^k$ unitary transformation will represent the product of all these rotations, and finding this one transformation that equidiagonalizes $FG^\dagger$ in one shot is a perfectly tractable problem for Alice to solve.

The matrix $FG^\dagger$ will not, in general, be of size $2^k \times 2^k$. Alice may nevertheless devise an approach that is guaranteed to yield state equations of form (1). She needs to be inventive. Her favored tactic so far, a sequence of pairwise equalizations, will converge upon the desired unitary matrix only in the infinite limit. She can find a more elegant method, however. The 2^k dimensional case is unproblematic, so if Alice can *enlarge* $FG^\dagger$ such that it achieves a dimensionality of a power of 2, she can solve her problem.

Such an enlargement represents an expansion of Alice's quantum system into a Hilbert space of greater dimension. A general unitary operation that achieves this is the SWAP operation, which exchanges the states of two quantum systems between their respective Hilbert spaces. Alice must perform a SWAP operation to transfer the state of her original quantum system $\mathcal{H}_n^A$ described by (2) to an n-dimensional subspace of a larger space, $\mathcal{H}_l^{A'}$, where $l \geq n$ and $l = 2^k$ for some integer k:

$$\begin{aligned} &|i\rangle_A |j\rangle_{A'} \Rightarrow |j\rangle_A |i\rangle_{A'} \quad \text{when } i, j = 1 \text{ to } n, \\ &|i\rangle_A |j\rangle_{A'} \Rightarrow |i\rangle_A |j\rangle_{A'} \quad \text{otherwise.} \end{aligned} \tag{14}$$

Since the size of $FG^\dagger$ is simply equal to the number of orthonormal vectors in Alice's measurement basis, this operation expands it to size $l \times l$. In her new basis, $\{|1\rangle_{A'}, \ldots, |l\rangle_{A'}\}_A$, Alice describes the two possible states (2) thus:

$$\begin{aligned} |\psi\rangle &= |1\rangle_{A'} |\eta_1'\rangle_B + \cdots + |l\rangle_{A'} |\eta_l'\rangle_B, \\ |\phi\rangle &= |1\rangle_{A'} |\nu_1'\rangle_B + \cdots + |l\rangle_{A'} |\nu_l'\rangle_B. \end{aligned} \tag{15}$$

Here, $|\eta_i'\rangle_B$ and $|\nu_i'\rangle_B$ are new unnormalized vectors, but remain describable in Bob's original basis $\{|1\rangle_B, \ldots, |m\rangle_B\}$. Now her system has a convenient number of dimensions; Alice proceeds as before. She will obtain and perform a measurement guaranteeing Bob possesses one of two orthogonal states.

SWAP operations like these are physically unproblematic, and do not in any way derogate the entangled information Alice shares with Bob. One physical realization of this procedure requires just one ancillary qubit. Alice introduces this qubit "Z," known to be in state $|0\rangle_Z$ to her system, giving her state equations of form

$$\begin{aligned} |\psi\rangle = &|10\rangle_{AZ} |\eta_1\rangle_B + \cdots + |n0\rangle_{AZ} |\eta_n\rangle_B \\ &+ |11\rangle_{AZ} |\eta_{n+1}\rangle_B + \cdots + |n1\rangle_{AZ} |\eta_{2n}\rangle_B. \end{aligned} \tag{16}$$

Since qubit Z is in state $|0\rangle_Z$, we know all the unnormalized vectors $|\eta_{n+i}\rangle_B$ have zero amplitude. This gives rise to the rather lopsided $FG^\dagger$ matrix, wherein $\{FG^\dagger\}_{ij} = 0$ everywhere that either $i > n$ or $j > n$. With this $FG^\dagger$ matrix, Alice's problems are over. Between the numbers n and $2n$ there lies a power of 2. Thus there is a submatrix of $FG^\dagger$ that includes all n nonzero terms, and just enough zero-valued terms to round things out to the most convenient dimensionality. Alice can find unitary manipulations on this submatrix that transform it (and thereby simultaneously transform the $FG^\dagger$ matrix as a whole) into zero-diagonal form. She simply follows the procedure outlined previously, obtaining a finite sequence of unitary transformations that, taken together, represent a single rotation of her measurement basis.

This unlikely procedure is surprisingly efficient for distinguishing $|\psi\rangle$ and $|\phi\rangle$. No matter what the dimensionality of the problem, there is a solution after a finite number of steps: a number of steps equal to $\frac{1}{2} l \log_2 l$, where l is the expanded dimensionality. Through the use of this

SWAP operation Alice can always accomplish perfect distinguishability with minimal effort.

We have considered only the bipartite case thus far, but the strategy used by Alice and Bob can also be deployed by any number of people. States of tripartite form, for instance,

$$\begin{aligned} |\psi\rangle &= |\alpha_1\rangle_A|\beta_1\rangle_B|\gamma_1\rangle_C + \cdots + |\alpha_n\rangle_A|\beta_n\rangle_B|\gamma_n\rangle_C\,, \\ |\phi\rangle &= |\alpha_1'\rangle_A|\beta_1'\rangle_B|\gamma_1'\rangle_C + \cdots + |\alpha_n'\rangle_A|\beta_n'\rangle_B|\gamma_n'\rangle_C\,, \end{aligned} \tag{17}$$

can, when Alice swaps into a larger Hilbert space, easily be represented thus:

$$\begin{aligned} |\psi\rangle &= |1\rangle_{A'}|\Gamma_1\rangle_{BC} + \cdots + |l\rangle_{A'}|\Gamma_l\rangle_{BC}\,, \\ |\phi\rangle &= |1\rangle_{A'}|\Gamma_1^\perp\rangle_{BC} + \cdots + |l\rangle_{A'}|\Gamma_l^\perp\rangle_{BC}\,. \end{aligned} \tag{18}$$

Alice simply behaves as before, and leaves Bob and Claire to distinguish between the resulting bipartite orthogonal states. The problem collapses to its original formulation, which we have already solved. If n people share the quantum system, performing a series of $n - 2$ such measurements will cascade their problem down to the bipartite case. We can conclude that two orthogonal states of any quantum system, shared in any proportion between any number of separated parties, can be perfectly distinguished.

Our procedure distinguishes perfectly between two orthogonal states, $|\psi\rangle$ and $|\phi\rangle$. What if Alice and Bob must distinguish between more than two orthogonal states? In general, this will not be possible so long as Alice and Bob share only one copy of their state. In whichever bases they perform sequential measurements, their binary outcome may not perfectly distinguish between more than two possibilities.

It is natural to quantify Alice and Bob's situation by asking *how many* copies of their state they require to perfectly distinguish between it and the other possibilities. A detailed analysis of this problem is beyond the scope of this paper. Nevertheless, our basic procedure places an upper bound on the number of copies required. n possible orthogonal states can be distinguished perfectly with $n - 1$ copies.

Let us denote the possible states $|\psi_i\rangle$. Alice and Bob simply act on their first copy as if they were distinguishing $|\psi_0\rangle$ and $|\psi_1\rangle$. If the state they share happens to be either $|\psi_0\rangle$ or $|\psi_1\rangle$, then their measurement result will be a definite verdict in favor of one or the other possibility. If they share instead some other $|\psi_i\rangle$, since $\langle\psi_i \mid \psi_j\rangle = \delta_{ij}$, Alice and Bob's measurement will randomly decide upon $|\psi_0\rangle$ some of the time, and will seem to measure $|\psi_1\rangle$ otherwise. A positive measurement for $|\psi_0\rangle$ is no guarantee of Alice and Bob sharing that state, for all the other states (barring $|\psi_1\rangle$) sometimes produce that result. What a verdict for $|\psi_0\rangle$ does show is that Alice and Bob definitely do not share $|\psi_1\rangle$, which they would have detected with certainty.

Proceeding in this way, Alice and Bob can always use a single copy of their state to exclude one possibility. After $n - 1$ such operations, they can have excluded $n - 1$ states, and can thus distinguish between n possibilities. This represents an upper bound upon the number of copies required for state distinction. Note that there are certainly sets of orthogonal states that can be distinguished using less than $n - 1$ copies. An example are the four Bell states, where only two copies will suffice.

We have proved that any two orthogonal quantum states shared between any number of parties may be perfectly distinguished by local operations and classical communication. Since orthogonal states are the only perfectly distinguishable states, this means that all pairs of distinguishable states are distinguishable with LOCC—global measurements are never required. Whether nonorthogonal states may also be optimally distinguished in this way remains an open question.

We would like to acknowledge the support of Hewlett-Packard. J.W. and A.J.S. thank the U.K. EPSRC (Engineering and Physical Sciences Research Council), and L.H. thanks the Royal Society for funding this research.

*Electronic address: jon.walgate@qubit.org

[1] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] M. Mosca, R. Jozsa, A. Steane, and A. Ekert, Philos. Trans. R. Soc. London A **358**, 261 (2000).
[5] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[6] C.H. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[7] A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[8] C.A. Fuchs, Ph.D. thesis, The University of New Mexico [LANL Report No. quant-ph/9601020, 1996 (unpublished)].
[9] C.H. Bennett *et al.,* Phys. Rev. A **59**, 1070 (1999).
[10] R. Cleve, D. Gottesman, and H. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[11] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).