Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication

M. Hayashi,[1] D. Markham,[2,*] M. Murao,[2,3] M. Owari,[2,†] and S. Virmani[4,‡]

[1]*Imai Quantum Computation and Information Project, ERATO, JST, Tokyo 113-0033, Japan, and Superrobust Computation Project (21st Century COE by MEXT), University of Tokyo, Japan*

[2]*Department of Physics, Graduate School of Science, University of Tokyo, Tokyo 113-0033, Japan*

[3]*PRESTO, JST, Kawaguchi, Saitama 332-0012, Japan*

[4]*Optics Section, Blackett Laboratory and Institute for Mathematical Sciences, Imperial College, London SW7 2AZ, United Kingdom*

(Received 22 June 2005; published 2 February 2006)

We show that entanglement guarantees difficulty in the discrimination of orthogonal multipartite states locally. The number of pure states that can be discriminated by local operations and classical communication is bounded by the total dimension over the average entanglement. A similar, general condition is also shown for pure and mixed states. These results offer a rare operational interpretation for three abstractly defined distancelike measures of multipartite entanglement.

DOI: 10.1103/PhysRevLett.96.040501 PACS numbers: 03.67.Mn, 03.65.Ud, 03.67.Hk

The problem of defining and understanding multiparty entanglement is a major open question in the field of quantum information. As entanglement theory becomes more useful in other areas of many body physics, multiparty entanglement becomes increasingly relevant to general physics, too. Hence, understanding the meaning of entanglement has become an interesting and important question.

In the bipartite case, entanglement is fairly well understood [1]. There are many entanglement measures defined both operationally (in terms of the usefulness of states for quantum information tasks) and abstractly (such that they obey certain axioms and may be called entanglement monotones). One of the most celebrated results in bipartite entanglement theory is that for pure states essentially all measures coincide and have clear operational relevance. For more than two parties, however, the operational approach quickly becomes very difficult. There are no clear ''units of usefulness,'' and we have the possibility of inequivalent types of entanglement [2]. Some abstract measures do persist by their simplicity. In particular, those measures that define ''proximity'' to the set of separable states [3–5] have natural multiparty analogues. However, due to their abstract definition, their operational meaning is not clear and remains an open question.

In this Letter, we consider the connection between distancelike entanglement measures and the task of local operations and classical communication (LOCC) state discrimination with this question in mind. This task illustrates the restriction of only having local access to a system, fundamental to the use of entanglement in quantum information (and notions of locality). Indeed, LOCC measurement of quantum states is important for cryptographic protocols [6], channel capacities [7], and distributed quantum information processing [8].

Intuitively, we expect that entangled states are more difficult to discriminate locally, since inherently they possess properties that are nonlocal. Indeed, it is known that entanglement can make LOCC discrimination more difficult [9]. But the exact relation is thus far unclear, and there are no general quantitative results. The results that are known can be confusing. One of the earliest results on the subject reveals a set of nonentangled, product states that cannot be discriminated perfectly by LOCC [10]. Later, it was shown that any two pure states can be discriminated optimally by LOCC, no matter how entangled they are [11]. There have been several results since then on various LOCC settings [12], and connections have been made to bipartite entanglement distillation and formation [13]. However, many results are specific to the bipartite case or only valid for specific scenarios.

We show a clear connection between distancelike measures of entanglement and LOCC state discrimination in the general multipartite case. We first show how the conditions imposed on the measurement by perfect state discrimination can be rewritten in terms of a quantity which looks like a ''distance'' to the closest separable state. As we weaken these conditions, we then show that this relates directly to three entanglement measures. Finally, combining these results gives a general (pure and mixed state) bound and, for pure states, allows the following interpretation: Entanglement gives an upper bound to the number of pure states that can be discriminated perfectly by LOCC.

By using known entanglement results, we will give examples of existing and new LOCC discrimination bounds in a unified manner.

Theorem 1: A necessary condition for deterministic LOCC discrimination of set $\{\rho_i | i = 1 \dots N\}$ is that the following inequality holds:

$$\sum_i d(\rho_i) \leq D, \tag{1}$$

where D is the total dimension of the system, and

$$d(\rho_i) := \min \frac{1}{\mathrm{tr}\{\rho_i \omega_i\}}$$
such that
$$\text{(i) } \mathbb{1} \geq \frac{\omega_i}{\mathrm{tr}\{\rho_i \omega_i\}} \geq 0, \qquad \text{(ii) } \omega_i \in \mathrm{SEP}, \tag{2}$$

where SEP denotes the set of separable operators.

To prove theorem 1, we begin by listing some conditions that the POVMs (positive operator value measures) must satisfy. The task of state discrimination is to perform a measurement (in our case, by LOCC) on a system to find out which one of a set of states the system is in. If it is possible to perfectly discriminate among a set of density matrices $\mathcal{S} := \{\rho_i | i = 1 \ldots N\}$ by LOCC, then it is necessary that there exists a POVM $\{M_i\}$ satisfying the following conditions:

$$\sum_i M_i = \mathbb{1}, \tag{3}$$

$$\mathbb{1} \geq M_i \geq 0, \tag{4}$$

$$\forall\ i\ \mathrm{tr}\{M_i \rho_i\} = 1, \tag{5}$$

$$\forall\ i\ M_i \in \mathrm{SEP}. \tag{6}$$

Conditions (3) and (4) are simply the conditions that mean $\{M_i\}$ is a POVM. Condition (5) says that, given a state ρ_i, the result corresponding to outcome M_i occurs with probability 1; i.e., the discrimination is deterministic. Condition (6) is known to be a necessary condition if the POVM $\{M_i\}$ is to be implementable by LOCC [9].

To make the connection to distances between states, we first notice that any POVM element M_i can be expressed as a positive number $s_i = \mathrm{tr}\{M_i\}$ times a density matrix ω_i, $M_i = s_i \omega_i$. We can then use this to immediately rewrite (3)–(6). Condition (5) is rewritten $s_i = 1/\mathrm{tr}\{\rho_i \omega_i\}$. Condition (6) means ω_i is separable. For pure states, s_i now looks like a distancelike quantity between state ρ_i and some separable state ω_i, such that the remaining conditions are satisfied (that is, $\sum_i s_i \omega_i = \mathbb{1}$, $\mathbb{1} \geq s_i \omega_i \geq 0$).

If we then minimize s_i such that conditions (4)–(6) are satisfied for each i independently, we get exactly the definition of $d(\rho_i)$ in theorem 1 (2). Condition (3) implies this minimization must satisfy

$$\sum_i d(\rho_i) \leq D, \tag{7}$$

completing the proof. □

At this point, $d(\rho)$ cannot be considered a "distance to the closest separable state" entanglement measure. It turns out that condition (i) in (2) complicates things a lot, and, indeed, even without this condition, it is not an entanglement monotone for mixed states [see the comment below the definition of the geometric measure (15)]. Hence, the connection to entanglement is not immediate. However, we can use this quantity to relate the problem of state discrimination to other distancelike entanglement monotones, as in the following theorem.

Theorem 2: The following bounds hold for all states ρ:

$$d(\rho) \geq r(\rho) \geq 2^{E_R(\rho)+S(\rho)} \geq 2^{G(\rho)}, \tag{8}$$

where $G(\rho)$ is the geometric measure; $E_R(\rho)$ is the relative entropy of entanglement; $S(\rho)$ is the von Neumann entropy; and $r(\rho) := |P|(1 + R_G(P/|P|)$, where P is the support of state ρ [14], $|P| := \mathrm{tr}\{P\}$, and $R_G(\rho)$ is the robustness of entanglement of state ρ.

In the pure state case, $S(\rho) = 0$ and $P = \rho$, and so these quantities become exactly (up to log) the geometric measure of entanglement, the relative entropy of entanglement, and the robustness of entanglement (from right to left). In the mixed state case, they include some quantification of how mixed the state is. This makes sense in the problem of state discrimination, since the more mixed the states are, the fewer orthogonal states there can be for a given Hilbert space dimension D. We will later show that the quantities in Eq. (8) are equivalent for GHZ states (these are multipartite states defined originally in Ref. [15]).

To prove the relationship to the robustness of entanglement, we must first write $d(\rho)$ in a more convenient form. We can rewrite condition (i) in (2), as $\langle\psi|\omega|\psi\rangle \leq \mathrm{tr}\{\rho\omega\}\forall|\psi\rangle$. By considering the spectral decomposition of ω, it follows that ω can always be rewritten in the form $\omega = \lambda|P|\frac{P}{|P|} + (1 - \lambda|P|)\Delta$ with the additional conditions $\mathrm{tr}\{P\Delta\} = 0$ and $\lambda \geq \langle\psi|\omega|\psi\rangle\forall|\psi\rangle$. Hence,

$$\begin{aligned} &d(\rho) = \min(1/\lambda) \\ &\text{such that} \quad \exists \text{ a state } \Delta, \quad \text{satisfying} \\ &\omega = \lambda|P|\frac{P}{|P|} + (1 - \lambda|P|)\Delta \in \mathrm{SEP}, \\ &\mathrm{tr}\{P\Delta\} = 0, \qquad \lambda \geq \langle\psi|\omega|\psi\rangle \quad \forall\ |\psi\rangle. \end{aligned} \tag{9}$$

We can now compare this to the global robustness of entanglement $R_g(\rho)$ [3]

$$\begin{aligned} &R_g(\rho) := \min t \\ &\text{such that} \quad \exists \text{ a state } \Delta, \quad \text{satisfying} \\ &\frac{1}{1+t}(\rho + t\Delta) \in \mathrm{SEP}. \end{aligned} \tag{10}$$

We can understand this as the minimum (arbitrary) noise Δ that we need to add to make the state separable.

We can see that the global robustness of entanglement of the support of state ρ, $R_G(P/|P|)$, is very similar in definition to $d(\rho)$ above, (9), the crucial difference being the removal of the two conditions in the last line of (9). Since relaxing conditions can lead only to a lower minimum, we can see that

$$d(\rho) \geq r(\rho) := |P|[1 + R_g(P/|P|)], \tag{11}$$

proving the left inequality of theorem 2.

For the center and right inequalities of theorem 2, we consider the two quantities separately.

The relative entropy of entanglement is defined as [4]

$$E_R(\rho) := \min_{\omega\in \mathrm{SEP}} S(\rho \parallel \omega), \tag{12}$$

where $S(\rho \parallel \omega) = -S(\rho) - \mathrm{tr}\{\rho \log_2 \omega\}$ is the relative entropy and $S(\rho)$ is the von Neumann entropy. From the definition of $R_g(\rho)$, we know that, for some state Δ, the state given by $\omega_i := [P_i/|P_i| + R_g(P_i/|P_i|)\Delta]/[1 + R_g(P_i/|P_i|)]$ is a separable state. Hence, the following inequalities must hold:

$$\begin{aligned} E_R(\rho_i) + S(\rho_i) &\le -\mathrm{tr}\left\{\rho_i \log_2\left(\frac{P_i/|P_i| + R_g(P_i/|P_i|)\Delta}{1 + R_g(P_i/|P_i|)}\right)\right\} \\ &\le -\mathrm{tr}\left\{\rho_i \log_2\left(\frac{P_i/|P_i|}{1 + R_g(P_i/|P_i|)}\right)\right\} \\ &= \log_2[|P_i|(1 + R_g(P_i/|P_i|))], \end{aligned} \tag{13}$$

where the second line follows from the monotonicity of the logarithm, which states that $\log(A + B) \ge \log(A)$ whenever $B \ge 0$, for two operators A, B [16]. The last line is true even if ρ_i is any state in the span of P_i. Hence,

$$2^{E_R(\rho_i)+S(\rho_i)} \le r(\rho_i). \tag{14}$$

We call the geometric measure $G(\rho)$

$$G(\rho) := -\log_2\{\max_{\omega\in \mathrm{SEP}} \mathrm{tr}\{\rho\omega\}\}. \tag{15}$$

In the case of pure states, this reduces to the geometric measure of entanglement [5]. However, for mixed states, this is not an entanglement monotone (for example, it is maximized by the maximally mixed state). We immediately see that this would be equivalent (up to log) to $d(\rho)$ in (2) if we were to drop condition (i). Hence, we have $d(\rho) \ge 2^{G(\rho)}$. However, it is possible to show a stronger bound. In Ref. [17] it was shown that in the pure state case $G(\rho)$ is bounded from above by the relative entropy of entanglement. We use the same simple concavity arguments now for the mixed state case. By definition, $E_R(\rho_i) + S(\rho_i) = -\max_{\omega\in \mathrm{SEP}} \mathrm{tr}\{\rho \log_2 \omega\}$. By concavity of the logarithm, we have for all ρ, ω, $\mathrm{tr}\{\rho\log_2\omega\} \le \mathrm{tr}\{\rho\omega\}$. Thus,

$$E_R(\rho) + S(\rho) \ge G(\rho). \tag{16}$$

Combining (11), (14), and (16), we get theorem 2. □

We will now look at how we can use our necessary conditions to bound the maximum number of states that can be discriminated locally. Combining theorems 1 and 2, and dividing by N, we obtain the following corollary.

Corollary: The number of states N that can be discriminated perfectly by LOCC is bounded by

$$N \le D/\overline{d(\rho_i)} \le D/\overline{r(\rho_i)} \le D/\overline{2^{E_R(\rho_i)+S(\rho_i)}} \le D/\overline{2^{G(\rho_i)}}, \tag{17}$$

where $\bar{x}_i := 1/N \sum_{i=1}^{N} x_i$ denotes the "average."

Hence, in the pure state case, where the bounds reduce to the geometric measure of entanglement, the relative entropy of entanglement, and the robustness of entanglement (from right to left), we can interpret these three distance-like measures as bounds on the number of pure states that we can discriminate perfectly by LOCC (see Fig. 1).

Given this hierarchy of bounds (17), we can apply known results from entanglement theory to find some bounds on N, one of which we will show is tight. First, the robustness of entanglement is completely solved for pure bipartite states [3]. For a state with Schmidt decomposition $|\psi\rangle = \sum_i \alpha_i |ii\rangle$, the robustness was found to be $R_g(\psi) = (\sum_i \alpha_i)^2 - 1$. We can immediately put this into (17). For instance, if we have a set of pure bipartite states all with the same entanglement (Bi), we have

$$N(\mathrm{Bi}) \le d_1 d_2 \bigg/ \left(\sum_i \alpha_i\right)^2, \tag{18}$$

where d_1, d_2 are the dimensions of the Hilbert spaces and α_i are the Schmidt coefficients for any one of the states in the set. This has the consequence that it is impossible to distinguish more than d maximally entangled states [where d is the dimension of one subspace, then $(\sum \alpha_i)^2 = d$], reproducing a known result [18,19].

In the multiparty case, we know from Wei *et al.* [17] that, for the m-party W state $|W\rangle := |00\ldots01\rangle + |00\ldots10\rangle + \ldots + |01\ldots00\rangle + |10\ldots00\rangle$ and GHZ state $|\mathrm{GHZ}\rangle := |0\rangle^{\otimes m} + |1\rangle^{\otimes m}$, the relative entropy of entanglement and the geometric measure coincide and are given by $E_R(|\mathrm{GHZ}\rangle) = E_G(|\mathrm{GHZ}\rangle) = 1$ and $E_R(|W\rangle) = E_G(|W\rangle) = \log_2(m/(m-1))^{(m-1)}$. Therefore, for any set of states where the state with the average geometric measure (or the lowest) is that of GHZ or W, we have

$$N(\mathrm{GHZ}) \le 2^{m-1} N(W) \le 2^m((m-1)/m)^{(m-1)}. \tag{19}$$

In fact, if we now call $N(\mathcal{S}_{\mathrm{GHZ}})$ the maximum number of states, in a set made of all GHZ type states (i.e., GHZ up to local unitary transformations), that can be discriminated perfectly by LOCC, then we can show $N(\mathcal{S}_{\mathrm{GHZ}}) = 2^{m-1}$ by explicit construction. We form a set of states $\mathcal{S}_{\mathrm{GHZ}} = \{|\mathrm{GHZ}_i\rangle := \mathbb{1} \otimes U_i |\mathrm{GHZ}\rangle\}_{i=1}^{2^{m-1}}$ by local unitaries $\{U_i\}$ over $m-1$ parties. The $\{U_i\}$ are formed from all the

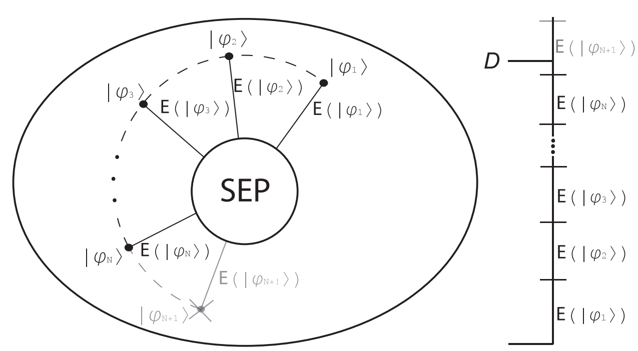

FIG. 1. To discriminate the pure states $\{|\varphi_i\rangle\}_{i=1}^N$ perfectly under LOCC, the sum of the entanglement "distances" $E(|\varphi_i\rangle)$ must be less than the total dimension D (theorems 1 and 2); thus, $N \le D/\overline{E(|\varphi_i\rangle)}$.

possible combinations of products of the identity and σ_x Pauli operations, e.g., $U_1 = \mathbb{1}^{\otimes m-2} \otimes \sigma_x$, giving a set of $\sum_{k=0}^{m-1}\binom{m-1}{k} = 2^{m-1}$ states. It is easy to check that these can be discriminated by making local σ_z measurements. Calling $\mathcal{S}_W$ a set of states equal to the W state up to local unitary transformations with (19) gives

$$N(\mathcal{S}_W) < N(\mathcal{S}_{\rm GHZ}). \tag{20}$$

We also note that, if we can find such a bound by any of the entanglement measures in (17) and show it is tight, those measures below it in the hierarchy are equal. The GHZ case is such an example giving $R_G(|{\rm GHZ}\rangle) = 1$, and is one of the few cases where the global robustness of entanglement is known for multiparty systems. We round off the examples by showing another simple known result. If even one state in a complete basis is entangled, then (17) shows that the basis cannot be discriminated perfectly [20].

The simplicity of the basis for the proofs of the main results here allows it to be used with other necessary conditions on LOCC measurements. The condition of separability (6), for example, may be changed to more tractable conditions such as positivity of partial transpose or biseparability [21]. It can easily be seen that these conditions would lead to analogous bounds to those derived above. In the case of biseparability, the example of bipartite states above shows that, for pure states, it is always possible to give some easily computable bound.

We have given an interpretation of the global robustness of entanglement, the relative entropy of entanglement, and the geometric measure of entanglement as bounds on the number of pure states that can be discriminated perfectly by LOCC. Our general mixed state results imply that the presence of entanglement guarantees a certain minimal level for this difficulty. The difficulty of LOCC state discrimination is an important consideration in various quantum information tasks (e.g., quantum data hiding [9]), which may give more uses of these results. This is the topic of ongoing investigations. In this direction, it is also possible to extend theorem 1 to the case of imperfect discrimination. This leads to bounds on the LOCC accessible information, as in Refs. [19,22], which will be presented in a separate paper.

We thank Keiji Matsumoto and Martin Plenio for useful discussions. This work was sponsored by the Asahi Glass Foundation, the JSPS, Leverhulme Trust, and the Royal Commission for the Exhibition of 1851.

*Corresponding author.
Electronic address: markham@phys.s.u-tokyo.ac.jp
†Corresponding author.
Electronic address: s.virmani@imperial.ac.uk
‡Corresponding author.
Electronic address: owari@eve.phys.s.u-tokyo.ac.jp

[1] M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001).
[2] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000); S. Ishizaka and M. B. Plenio, Phys. Rev. A **72**, 042325 (2005).
[3] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999); A. W. Harrow and M. A. Nielsen, Phys. Rev. A **68**, 012308 (2003); M. Steiner, Phys. Rev. A **67**, 054305 (2003).
[4] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[5] A. Shimony, Ann. N.Y. Acad. Sci. **755**, 675 (1995); H. Barnum and N. Linden, J. Phys. A **34**, 6787 (2001); T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).
[6] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984); A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] P. Hayden and C. King, quant-ph/0409026; J. Watrous, Phys. Rev. Lett. **95**, 080505 (2005).
[8] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).
[9] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
[10] 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).
[11] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000); S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001); Z. Ji, H. Cao, and M. Ying, Phys. Rev. A **71**, 032323 (2005).
[12] M. Hillery and J. Mimih, Phys. Rev. A **67**, 042304 (2003); P. X. Chen and C. Z. Li, Phys. Rev. A **68**, 062107 (2003); S. de Rinaldis, Phys. Rev. A **70**, 022309 (2004); S. Virmani and M. B. Plenio, Phys. Rev. A **67**, 062308 (2003); F. Anselmi, A. Chefles, and M. B. Plenio, New J. Phys. **6**, 164 (2004); A. Chefles, Phys. Rev. A **69**, 050307(R) (2004); H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).
[13] P. Badziąg, M. Horodecki, A. Sen, and U. Sen, Phys. Rev. Lett. **91**, 117901 (2003); M. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, Phys. Rev. Lett. **93**, 170503 (2004); S. Ghosh, P. Joag, G. Kar, S. Kunkri, and A. Roy, Phys. Rev. A **71**, 012321 (2005).
[14] The support of a state ρ, with eigendecomposition $\rho = \sum_i \alpha_i |i\rangle\langle i|$, is given by $P = \sum_i |i\rangle\langle i|$.
[15] D. M. Greenberger, M. Home, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 69.
[16] R. Bhatia, *Matrix Analysis*, Springer Graduate Texts in Mathematics Vol. 169 (Springer, New York, 1991).
[17] T.-C. Wei, M. Ericsson, P. M. Goldbart, and W. J. Munro, Quantum Inf. Comput. **4**, 252 (2004).
[18] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001); S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004).
[19] M. Nathanson, J. Math. Phys. (N.Y.) **46**, 062103 (2005).
[20] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).
[21] E. M. Rains, Phys. Rev. A **60**, 179 (1999); **63**, 019902(E) (2001).
[22] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).