Separable States Are More Disordered Globally than Locally

M. A. Nielsen^{1,*} and J. Kempe^{2,†}

¹Centre for Quantum Computer Technology, University of Queensland, Queensland 4072, Australia ²Departments of Mathematics and Chemistry, University of California, Berkeley, California 94270 (Received 29 November 2000)

A remarkable feature of quantum entanglement is that an entangled state of two parties, Alice (A) and Bob (B), may be more disordered locally than globally. That is, S(A) > S(A, B), where $S(\cdot)$ is the von Neumann entropy. It is known that satisfaction of this inequality implies that a state is nonseparable. In this paper we prove the stronger result that for separable states the vector of eigenvalues of the density matrix of system AB is majorized by the vector of eigenvalues of the density matrix of system A alone. This gives a strong sense in which a separable state is more disordered globally than locally and a new necessary condition for separability of bipartite states in arbitrary dimensions.

DOI: 10.1103/PhysRevLett.86.5184

Ouantum mechanics harbors a rich structure whose investigation and explication are the goal of quantum information science [1,2]. At present only a limited understanding of the fundamental static and dynamic properties of quantum information has been obtained, and many major problems remain open. In particular, we want a detailed ontology and quantitative methods of description for the different types of information and dynamical processes afforded by quantum mechanics. An example of the pursuit of these goals has been the partial development of a theory of quantum entanglement; see, e.g., [3–7] and references therein.

The separability or nonseparability of a quantum state is an issue that has received much attention in the development of a theory of entanglement. The notion of separability captures the idea that a quantum state's static properties can be explained entirely by classical statistics and is sometimes claimed to be equivalent to the notion that a state is "not entangled." More precisely, a state ρ_{AB} of Alice and Bob's system is separable [8] if it can be written in the form $\rho_{AB} = \sum_j q_j \rho_j \otimes \sigma_j$, for some probability distribution $\{q_j\}$, and density matrices ρ_j and σ_j of Alice and Bob's systems, respectively. Thus, we can think of Alice and Bob's systems as having a local, pseudoclassical description, as a mixture of the product states $\rho_i \otimes \sigma_i$ with probabilities q_i . Note that separability is equivalent to the condition

$$\rho_{AB} = \sum_{i} p_{j} |\psi_{j}\rangle \langle \psi_{j}| \otimes |\phi_{j}\rangle \langle \phi_{j}|, \qquad (1)$$

where $\{p_i\}$ is a probability distribution and $|\psi_i\rangle$, $|\phi_i\rangle$ are pure states of Alice and Bob's systems, respectively.

One reason for interest in separability is a deep theorem due to M., P., and R. Horodecki connecting separability to positive maps on operators [5]. The Horodeckis used this theorem to prove that the "positive partial transpose" criterion for separability introduced by Peres [9] is a necessary and sufficient condition for separability of a state ρ_{AB} of a system consisting of a qubit in Alice's possession and either a qubit or qutrit in Bob's possession. More precisely, if we define $\rho_{AB}^{T_B}$ to be the operator that results when the transposition map is applied to system B alone, then the Horodeckis showed that ρ_{AB} is separable if and only if $\rho_{AB}^{T_B}$ is a positive operator. Unfortunately, this cri-

PACS numbers: 03.65.Ud, 03.67.-a

terion, while necessary for a state to be separable in higher dimensions [9], is not sufficient. A hallmark of quantum entanglement is the remarkable

fact that individual components of an entangled system may exhibit *more* disorder than the system as a whole. The canonical example of this phenomenon is a pair of qubits A and B prepared in the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$. The von Neumann entropy S(A) of qubit A is equal to one bit, compared with a von Neumann entropy S(A, B) of zero bits for the joint system. Classically, of course, such behavior is impossible, and the Shannon entropy H(X) of a single random variable is never larger than the Shannon entropy of two random variables, $H(X), H(Y) \leq H(X, Y)$. It has been shown [10] (see Chap. 8 of [11] and [12-14] for related results, including generalizations to the α entropy, and the reduction criterion for separability) that an analogous relation holds for separable states,

$$S(A), S(B) \le S(A, B). \tag{2}$$

This result is a consequence of the concavity of S(A, B) — S(A) [1,15], since when $\rho_{AB} = \sum_{j} q_{j} \rho_{j} \otimes \sigma_{j}$ we have $S(A, B) - S(A) \ge \sum_{j} q_{j} [S(\rho_{j} \otimes \sigma_{j}) - S(\rho_{j})] \ge 0$. Unfortunately, the inequalities (2) are insufficient to characterize separability. To see this, consider the Werner state of two qubits $\rho_p = p|\Psi\rangle\langle\Psi| + (1-p)I/4$ (0 \le \displaysis) $p \le 1$) and $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. The positive partial transpose criterion implies that the state is separable if and only if $p \le 1/3$. The marginal density matrices being fully mixed for all p, however, one obtains $S(A) = S(B) = 1 \le S(A, B) = H(\frac{1+3p}{4}, \frac{1-p}{4}, \frac{1-p}{4}, \frac{1-p}{4})$ for $0 \le p \le 0.747...$, so the condition (2) is fulfilled for a range of inseparable states.

The notion of von Neumann entropy is a valuable notion of disorder in a quantum state; however, more sophisticated tools for quantifying disorder exist. One such tool is the theory of majorization, whose basic elements we now review (see Chap. 2 and 3 of [16], [17], or [18] for more extensive background). Suppose $x=(x_1,\ldots,x_d)$ and $y=(y_1,\ldots,y_d)$ are two d-dimensional real vectors; we usually suppose in addition that x and y are probability distributions; that is, the components are non-negative and sum to one. The relation $x \prec y$, read "x is majorized by y," is intended to capture the notion that x is more "mixed" (i.e., disordered) than y. Introduce the notation \downarrow to denote the components of a vector rearranged into decreasing order, so $x^{\downarrow} = (x_1^{\downarrow}, \ldots, x_d^{\downarrow})$, where $x_1^{\downarrow} \geq x_2^{\downarrow} \geq \cdots \geq x_d^{\downarrow}$. Then we define $x \prec y$, if

$$\sum_{i=1}^{k} x_j^{\downarrow} \le \sum_{i=1}^{k} y_j^{\downarrow},\tag{3}$$

for $k=1,\ldots,d-1$, and with the inequality holding with equality when k=d. To understand how this definition connects with disorder consider the following result (see Chap. 2 of [16] for a proof): $x \prec y$ if and only x=Dy, where D is a doubly stochastic matrix. Thus, when $x \prec y$ we can imagine that y is the input probability distribution to a noisy channel described by the doubly stochastic matrix D, inducing a more disordered output probability distribution, x. Majorization can also be shown [16] to be a more stringent notion of disorder than entropy in the sense that if $x \prec y$ then it follows that $H(x) \ge H(y)$.

Given the known connections between measures of disorder such as the von Neumann entropy and separability, it is natural to conjecture that there might be some relationship between separability and the vectors $\lambda(\rho_{AB})$, $\lambda(\rho_A)$, $\lambda(\rho_B)$ of eigenvalues for ρ_{AB} and the corresponding reduced density matrices. Majorization suggests the following theorem as a natural way of strengthening the necessary conditions for separability, Eq. (2).

Theorem 1 (disorder criterion for separability).—If ρ_{AB} is separable, then

$$\lambda(\rho_{AB}) \prec \lambda(\rho_A)$$
 and $\lambda(\rho_{AB}) \prec \lambda(\rho_B)$. (4)

[By convention we append zeros to the vectors $\lambda(\rho_A)$ and $\lambda(\rho_B)$ so they have the same dimension as $\lambda(\rho_{AB})$.]

The disorder criterion for separability, Theorem 1, is the main result of this paper. Note that it provides a more stringent criterion for separability than (2), since for any two states ρ and σ , $\lambda(\rho) \prec \lambda(\sigma)$ implies that $S(\rho) \geq S(\sigma)$, but not necessarily conversely.

Proof.— If ρ_{AB} is separable, it may be written in the form of (1). Let $\rho_{AB} = \sum_k r_k |e_k\rangle\langle e_k|$ be a spectral decomposition for ρ_{AB} . By the classification theorem for ensembles (Theorem 2.6 in [1]) it follows that there is a unitary matrix u_{ki} such that

$$\sqrt{r_k} |e_k\rangle = \sum_j u_{kj} \sqrt{p_j} |\psi_j\rangle |\phi_j\rangle. \tag{5}$$

Next we trace out system B in (1) to give $\rho_A = \sum_i p_j |\psi_j\rangle\langle\psi_j|$. Letting $\rho_A = \sum_l a_l |f_l\rangle\langle f_l|$ be a spectral

decomposition and applying the classification theorem for ensembles we see that there is a unitary matrix v_{jl} such that $\sqrt{p_j} |\psi_j\rangle = \sum_l v_{jl} \sqrt{a_l} |f_l\rangle$. Substituting into (5) gives $\sqrt{r_k} |e_k\rangle = \sum_{jl} \sqrt{a_l} u_{kj} v_{jl} |f_l\rangle |\phi_j\rangle$. Multiplying this equation by its adjoint and using the orthonormality of the vectors $|f_l\rangle$ we obtain

$$r_k = \sum_{l} D_{kl} a_l \,, \tag{6}$$

where

$$D_{kl} \equiv \sum_{j_1,j_2} u_{kj_1}^* u_{kj_2} v_{j_1l}^* v_{j_2l} \langle \phi_{j_1} | \phi_{j_2} \rangle.$$
 (7)

To complete the proof all we need to do is show that D_{kl} is doubly stochastic. The fact that $D_{kl} \ge 0$ follows by defining $|\gamma_{kl}\rangle \equiv \sum_j u_{kj} v_{jl} |\phi_j\rangle$ and noting that $D_{kl} = \langle \gamma_{kl} | \gamma_{kl} \rangle \ge 0$. From (7) and by the unitarity of u we have

$$\sum_{k} D_{kl} = \sum_{j_1 j_2} \delta_{j_1 j_2} v_{j_1 l}^* v_{j_2 l} \langle \phi_{j_1} | \phi_{j_2} \rangle = \sum_{j} v_{j l}^* v_{j l} = 1.$$

Similarly, $\sum_{l} D_{kl} = 1$, and thus D is a doubly stochastic matrix. \square

The disorder criterion for separability Eq. (4) is strictly stronger than the entropic criterion (2). Indeed, for Belldiagonal states of two qubits, it follows from the positive partial transpose criterion and a straightforward calculation that condition (4) is equivalent to separability, whereas as remarked earlier the condition S(A), $S(B) \leq S(A,B)$ is not sufficient to characterize separability even for the more restricted case of Werner states. More generally, the disorder criterion (4) completely characterizes the separability properties of Werner states in arbitrary (d) dimensions. More precisely, states of the form $\rho_p = p|\Psi\rangle\langle\Psi| + (1-p)/d^2I$, where $|\Psi\rangle =$ $(|00\rangle + |11\rangle + \cdots + |(d-1)(d-1)\rangle)/\sqrt{d}$ are known to be separable if and only if $p \le 1/(d+1)$ [19]. The marginal density matrices of these states are completely mixed and Eq. (4) thus becomes

$$\frac{1}{d^2} [1 + (d^2 - 1)p, 1 - p, \dots, 1 - p] \prec \frac{1}{d} (1, \dots, 1),$$
(8)

which is easily seen to be equivalent to $p \le 1/(d+1)$.

Another interesting application of the disorder criterion Eq. (4) is to the problem of finding nonseparable states near the completely mixed state $I^{\otimes n}/d^n$ of n qudits (d-dimensional quantum systems). Consider the state $\rho \equiv (1-\epsilon)I^{\otimes n}/d^n + \epsilon|\psi\rangle\langle\psi|$, where $|\psi\rangle$ is the cat state of n qudits. Partitioning the n qudits so that the first n-1 belong to Alice and the final qudit to Bob, a straightforward calculation shows that the disorder criterion is violated whenever $\epsilon > 1/(1+d^{n-1})$, and thus ρ must be inseparable when ϵ satisfies this condition. Note that this result has previously been obtained by other techniques [20,21] (see also [22–25]); however, the utility of the disorder criterion is demonstrated in this application by the

ease with which it is applied and its generality, as compared to the more complex and state-specific arguments used previously to study the separability of ρ .

It is natural to conjecture the converse to Theorem 1, that if both the conditions in Eq. (4) hold, then ρ_{AB} is separable. Unfortunately, this is not the case, as the following two qubit examples show.

Example 1.—Let $\rho_{AB}^p \equiv p|00\rangle\langle00| + (1-p)|\Phi\rangle \times \langle\Phi|$ with the Bell state $|\Phi\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. Then the partial transpose criterion implies that this state is non-separable whenever $p \neq 1$. However, $\lambda(\rho_{AB}^p) = (p, 1-p) \prec \lambda(\rho_{AB}^p) = [(1+p)/2, (1-p)/2]$ for $1/3 \leq p$; that is, criterion (4) is fulfilled for this non-separable state.

More generally, we now show that attempts to characterize separability based only upon the eigenvalue spectra $\lambda(\rho_{AB})$, $\lambda(\rho_A)$, and $\lambda(\rho_B)$ can never work. We demonstrate this by exhibiting a pair of two qubit states ρ_{AB} and σ_{AB} such that all these vectors of eigenvalues are the same (i.e., the states are globally and locally *isospectral*), yet ρ_{AB} is not separable, while σ_{AB} is.

Isospectral example.

The isospectrality of the these states may be checked by direct calculation, and the fact that ρ_{AB} is nonseparable while σ_{AB} is follows from the partial transpose criterion. (Other examples of this phenomenon have been found by other researchers, including Davis [26] and Wootters [27].) It is worth emphasizing how remarkable such examples are: these density matrices have the same spectra, both globally and locally, yet one is separable, while the other is not. This runs counter to the often-encountered wisdom that a complete understanding of a quantum system can be obtained by studying the local and global properties of the spectra of that system. This is the point of view apparently adopted, for instance, in the theory of quantum phase transitions [28], perhaps leading to the disregard of important physical effects in that theory.

Given the isospectral example it is natural to ask under what conditions a separable state exists, given specified global and local spectra. We can report the following result in this direction.

Theorem 2.—If ρ_{AB} is a density matrix such that $\lambda(\rho_{AB}) \prec \lambda(\rho_A)$, then there exists a separable density matrix σ_{AB} such that $\lambda(\sigma_{AB}) = \lambda(\rho_{AB})$ and $\lambda(\sigma_A) = \lambda(\rho_A)$.

Proof.—Suppose $(r_j) = \lambda(\rho_{AB})$ and $(s_k) = \lambda(\rho_A)$. By Horn's lemma [29,30], there is a unitary matrix u_{jk} such that $s_j = \sum_k |u_{jk}|^2 r_k$. Introduce orthonormal bases $|j\rangle$

for system B and $|k\rangle$ for system A, and for each nonzero r_i define

$$|\psi_j\rangle \equiv \frac{\sum_k u_{jk} \sqrt{s_k} |k\rangle}{\sqrt{r_i}}.$$
 (10)

Then define $\sigma \equiv \sum_j r_j |\psi_j\rangle\langle\psi_j| \otimes |j\rangle\langle j|$. Note that σ is manifestly separable with spectrum $\lambda(\rho_{AB})$, while a simple calculation shows that $\operatorname{tr}_B(\sigma) = \sum_k s_k |k\rangle\langle k|$, and thus $\lambda(\sigma_A) = \lambda(\rho_A)$, completing the proof. \square

A stronger conjecture is that whenever both $\lambda(\rho_{AB}) \prec \lambda(\rho_A)$ and $\lambda(\rho_B)$, then there exists a separable state σ_{AB} which is isospectral to ρ_{AB} . Unfortunately, the following theorem shows that this is not true.

Theorem 3.—For the class of states ρ_{AB}^p in Example 1 (which are nonseparable when 1 > p > 1/3) the disorder criterion (4) is fulfilled yet there is no separable σ_{AB} (globally and locally) isospectral to ρ_{AB}^p when $1 > p \ge 1/2$.

Proof.—Suppose $\sigma \equiv \sigma_{AB}$ is a separable state isospectral to ρ_{AB}^p . Then $\sigma = p|s_1\rangle\langle s_1| + (1-p)|s_2\rangle\langle s_2|$ for orthonormal states $|s_1\rangle$ and $|s_2\rangle$. We suppose for now that σ can be given a separable decomposition with only two terms, $\sigma = q|a_1\rangle\langle a_1| \otimes |b_1\rangle\langle b_1| + (1-q)|a_2\rangle\langle a_2| \otimes |b_2\rangle\langle b_2|$. We show later that this is the only case that need be considered. Define angles α , β , and ϕ by $|\langle a_1|b_1\rangle| \equiv \cos(\alpha)$; $|\langle a_2|b_2\rangle| \equiv \cos(\beta)$; $\cos(\phi) \equiv \cos(\alpha)\cos(\beta)$. Then the global and local spectra for σ are easily calculated,

$$\lambda(\sigma_{AB}) = \left(\frac{1 \pm \sqrt{1 - 4q(1 - q)\sin^2(\phi)}}{2}\right), \quad (11)$$

with similar expressions for $\lambda(\sigma_A)$ and $\lambda(\sigma_B)$, with α and β appearing in place of ϕ . Assuming $1/2 \le p$ this gives $\sin^2(\alpha) = \sin^2(\beta) = (1 - p^2)/4q(1 - q)$ and $p(1-p) = q(1-q)\sin^2(\phi)$. Using $\sin^2(\phi) = 1 - [1-\sin^2(\alpha)][1-\sin^2(\beta)]$ to substitute the former expression into the latter, we find $q(1-q) = (1+p)^2/8$. For $p > \sqrt{2} - 1 \approx 0.41$ there is no q in the range 0 to 1 satisfying this equation, so we deduce that no such separable state σ can exist.

To complete the proof we show that any separable decomposition $\sigma = \sum_{i} q_{i} |a_{j}\rangle\langle a_{j}| \otimes |b_{j}\rangle\langle b_{j}|$ can be assumed to have two terms (cf. Lockhart [31]). Without loss of generality we assume that there is no redundancy in the decomposition; that is, there do not exist values $j \neq k$ such that $|a_j\rangle|b_j\rangle = |a_k\rangle|b_k\rangle$ (up to phase). We show that assuming the decomposition has three or more terms leads to a contradiction. Note that the decomposition must contain contributions from at least two linearly independent states, say $|a_1\rangle |b_1\rangle$ and $|a_2\rangle |b_2\rangle$. Furthermore, because $rank(\sigma) = 2$ any other state in the sum must be a linear combination of these two states, $|a_i\rangle|b_i\rangle = \alpha_i|a_1\rangle|b_1\rangle + \beta_i|a_2\rangle|b_2\rangle$. By the noredundancy assumption neither $|\alpha_i| = 1$ nor $|\beta_i| = 1$, so we must have $0 < |\alpha_i|, |\beta_i| < 1$. Consider now three possible cases. In the first case, $|a_1\rangle = |a_2\rangle$ (up to phase), in which case $|a_j\rangle=|a_1\rangle$ (up to phase) for all j, and thus $\lambda(\sigma_A)=(1,0)\neq\lambda(\rho_A^p)$, a contradiction. A similar contradiction arises when $|b_1\rangle=|b_2\rangle$ up to phase. The third and final case is when neither $|a_1\rangle=|a_2\rangle$ nor $|b_1\rangle=|b_2\rangle$ up to phase. In this case $\alpha_j|a_1\rangle|b_1\rangle+\beta_j|a_2\rangle|b_2\rangle$ cannot be a product state, a contradiction. \square

Given that attempts to characterize separability based on the local and global spectra are doomed to failure, it is still interesting to ask whether the conditions $\lambda(\rho_{AB}) \prec \lambda(\rho_A)$ and $\lambda(\rho_{AB}) \prec \lambda(\rho_B)$ are equivalent to some other interesting physical condition. We have tried to find such an equivalence, with little success, but can identify several plausible possibilities which these conditions are not equivalent to. They are not equivalent to the property of violating a Bell inequality, of having a positive partial transpose, or of being distillable. Another interesting idea is to find states which have positive partial transposition but which violate the disorder criterion. Such a state will necessarily be bound entangled [32]. We have not yet identified any such states, despite searching through several of the known classes of bound-entangled states and doing numerical searches.

In summary, we have connected two central notions in the theory of entanglement, using majorization to obtain a simple set of necessary conditions for a state to be separable in arbitrary dimensions. Understanding the physical import of these conditions and their relationship to criteria such as the positive partial transpose condition remains an interesting problem for further research.

We thank Carl Caves and Pranaw Rungta for discussions about separability and quantum information in general. J. K. thanks the Centre for Quantum Computer Technology at the University of Queensland for its hospitality and acknowledges support by the U.S. ARO under Contract/Grant No. DAAG55-98-1-0371.

- [2] J. Preskill, *Physics 229: Advanced Mathematical Methods of Physics—Quantum Computation and Information* (California Institute of Technology, Pasadena, CA, 1998), http://www.theory.caltech.edu/people/preskill/ph229/.
- [3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).
- [4] M. A. Nielsen, Phys. Rev. Lett. 83, 436 (1999).
- [5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A 223, 1 (1996).
- [6] V. Vedral and M. B. Plenio, Phys. Rev. A 57, 1619 (1998).
- [7] G. Vidal, Phys. Rev. Lett. 83, 1046 (1999).
- [8] R. F. Werner, Phys. Rev. A 40, 4277 (1989).
- [9] A. Peres, Phys. Rev. Lett. 77, 1413 (1996).
- [10] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A 210, 377 (1996).
- [11] M. A. Nielsen, Ph.D. thesis, University of New Mexico, 1998, e-print quant-ph/0011036.
- [12] N. J. Cerf and C. Adami, Phys. Rev. A 60, 893 (1999).
- [13] P. Horodecki, R. Horodecki, and M. Horodecki, Acta Phys. Slovaca 48, 141 (1998).
- [14] M. Horodecki and P. Horodecki, Phys. Rev. A 59, 4206 (1999).
- [15] E. H. Lieb and M. B. Ruskai, J. Math. Phys. (N.Y.) **14**, 1938 (1973).
- [16] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).
- [17] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic Press, New York, 1979).
- [18] P.M. Alberti and A. Uhlmann, Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing (Dordrecht, Boston, 1982).
- [19] W. Dür and J. I. Cirac, Phys. Rev. A 61, 042314 (2000).
- [20] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 032313 (2000).
- [21] P. Rungta et al., e-print quant-ph/0001075.
- [22] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. 83, 3562 (1999).
- [23] G. Vidal and R. Tarrach, Phys. Rev. A 59, 141 (1999).
- [24] C. M. Caves and G. J. Milburn, Opt. Commun. 179, 439 (2000).
- [25] S. L. Braunstein et al., Phys. Rev. Lett. 83, 1054 (1999).
- [26] R. Davis (private communication).
- [27] W. Wootters (private communication).
- [28] S. Sachdev, *Quantum Phase Transitions* (Cambridge University Press, Cambridge, England, 1999).
- [29] A. Horn, Am. J. Math. 76, 620 (1954).
- [30] M. A. Nielsen, Phys. Rev. A 62, 052308 (2000).
- [31] R. B. Lockhart, J. Math. Phys. (N.Y.) 41, 6766 (2000).
- [32] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 80, 5239 (1998).

^{*}Email address: nielsen@physics.uq.edu.au

[†]Also at École Nationale Superieure des Télécommunications, Paris, France.

Email address: kempe@math.berkeley.edu

^[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation* and *Quantum Information* (Cambridge University Press, Cambridge, England, 2000).