Largest separable balls around the maximally mixed bipartite quantum state

Leonid Gurvits and Howard Barnum

CCS-3, Mail Stop B256, Los Alamos National Laboratory, Los Alamos, New Mexico 87545
(Received 30 April 2002; published 12 December 2002)

For finite-dimensional bipartite quantum systems, we find the exact size of the largest balls, in spectral l_p norms for $1 \leq p \leq \infty$, of separable (unentangled) matrices around the identity matrix. This implies a simple and intuitively meaningful geometrical sufficient condition for separability of bipartite density matrices: that their purity $\mathrm{tr}\,\rho^2$ not be too large. Theoretical and experimental applications of these results include algorithmic problems such as computing whether or not a state is entangled, and practical ones such as obtaining information about the existence or nature of entanglement in states reached by nuclear magnetic resonance quantum computation implementations or other experimental situations.

I. INTRODUCTION AND SUMMARY OF RESULTS

Entanglement is an important element of many quantum information processing procedures, from cryptography to computation to quantum teleportation. Indeed, a quantum algorithm operating on pure quantum states must entangle a number of qubits increasing unboundedly with the input size, if it is not to be simulable in polynomial time on a classical computer [1]. It is not known whether this is so when the computer state may be mixed. Determining whether a given state, even of two quantum systems, is entangled or separable (not entangled) is, in general, difficult, and considerable effort has been expended on finding necesssary and/or sufficient conditions. The normalized separable states form a convex set. A key aspect of the geometry of a convex set is the size of the largest ball (especially in l_2 norm) that fits entirely inside it, and the smallest ball that covers it. We here find the inner ball for the set of separable quantum states. The result has both practical and theoretical relevance. For example, it provides a simple sufficient criterion for separability. A bipartite state of a composite system with overall dimension d is separable if its purity $\mathrm{tr}\,\rho^2$ is less than $1/(d-1)$ (as conjectured in Ref. [2]). Because of its simple geometric nature and ease of computation, this criterion is likely to be very useful both in theoretical applications and in analyzing whether entanglement was present in experiments. Just as importantly, knowing the size of such balls helps one to understand the computational complexity of problems involving a convex set. For example, using bounds on the size of the inner ball (rather than the exact result we present here) one of us has shown the NP (nondeterministic polynomial) hardness of the "weak membership" problem for separability when the dimensions of the two systems are not too different [8]. It is likely that the exact result reported herein may be used in extending this hardness result or in obtaining other complexity results about separability and entanglement.

Our main results begin with Theorem 1, that the matrix $I + \Delta$ is separable for all Hermitian Δ with $||\Delta||_2 \leq 1$. Corollary 1 gives similar statements for other p norms. Theorem 3 establishes that for $2 \leq p \leq \infty$, these are the largest such balls, by showing that at any larger radius, there are states whose partial transpose fails to be positive semidefinite (so

they are entangled). A similar result is easy for $1 \leq p \leq 2$, as remarked before the statement of Theorem 2; however, this involves subtracting a normalized pure state to reach the edge of the ball where the state becomes singular and thus is at the edge of the positive cone. By contrast, Theorem 3 involves adding a maximally entangled state, so the $p > 2$ balls hit the boundary of the separable states at some places where positive entangled states lie across the boundary. Theorem 4 tells us about the size of the largest negative eigenvalues of the partial transpose of bipartite positive matrices that are rank-m projectors, giving us information about how quickly we can hit the entangled matrices when departing from the identity by adding a positive multiple of such a projector. In particular, by considering a perturbation Δ proportional to such a projector whose partial transpose has maximal modulus of its most negative eigenvalue, it can be shown that for $p = 2$, also, the largest p-norm ball around I touches the edge of the separable cone at places within the positive cone.

As one example of practical relevance, the "pseudopure" states that describe each molecule in nuclear magnetic resonance quantum information processing are mixtures of the uniform density matrix with a pure state; the signal of quantum dynamics derives from the small pure component. Because of this, the density matrices of the different nuclear spins in a given molecule have not, in experiments done so far, exhibited entanglement despite the pure component being an entangled state; they have remained within known lower bounds on the size of the ball of separable states [3]. Our determination of the exact size of this ball for bipartite entanglement increases known lower bounds on the polarization necessary in order for such bulk computation on pseudopure states to be able to achieve bipartite entanglement, although due to the bipartite nature of our analysis, it does not rule out the production of entangled states that are separable with respect to every bipartition, at lower polarization. This raises the interesting question whether the exponential gap between our bound for bipartite separability and known bounds for separability in this context can be closed. Other quantum information processing procedures may also involve such mixtures; also, mixture with the identity matrix is a frequently studied model of quantum noise, the "depolarizing channel," to which our results are relevant. When this occurs in bipartite contexts, our results are much stronger than previously known. We emphasize, though, that the

sufficient conditions for entanglement and separability provided by our results apply in arbitrary contexts, not only for mixtures of a pure state with the normalized identity.

II. MATHEMATICAL BACKGROUND AND NOTATION

We represent unnormalized states of a quantum system composed of two subsystems of dimensions M and N ("$M \otimes N$ system"), as positive semidefinite $M \times M$ block matrices, with $N \times N$ blocks (so that they are $MN \times MN$ complex matrices). (These are the elements of the unnormalized density operator, in some fixed basis of product states $e_i \otimes f_j$.) Rather than Dirac notation, we use roman letters for vectors, but we use † for the adjoint. Such a matrix A is called *separable* if it can be written

$$A = \sum_i x_i x_i^\dagger \otimes y_i y_i^\dagger. \tag{1}$$

Objects such as $x_i x_j^\dagger$ are outer products (in Dirac notation $|x_i\rangle\langle x_j|$; here $|x_i\rangle$ are not assumed normalized.). We use e_i for elements of an orthonormal basis (typically $|i\rangle$ in Dirac notation). Thus our $e_i \otimes e_j$ would typically be written $|e_i\rangle \otimes |e_j\rangle$, or $|e_i\rangle|e_j\rangle$ or simply $|i\rangle|j\rangle$ in Dirac notation. M_n is the set of $n \times n$ complex matrices, M_{mn} the set of $m \times n$ complex matrices. When interpreting tensor products as block matrices the left-hand factor corresponds to "which block," and the right hand to the indices within blocks. $||X||$ (or $||X||_\infty$), with a matrix X as argument, is the usual operator norm induced by Euclidean norm $||x|| = \sqrt{(x,x)}$ on vectors (i.e., $||X|| := \sup_{||x||=1} ||Xx||$). (It is also the l_∞ norm of the vector of singular values of X, i.e., the largest singular value.) $||X||_1$ is $\mathrm{tr}\sqrt{X^\dagger X}$, the sum of the singular values of X. $||X||_2$, the Frobenius norm, is $\sqrt{\mathrm{tr}\, X^\dagger X}$, the Euclidean norm associated with the inner product $\mathrm{tr}\, X^\dagger Y$. The squared Frobenius norm is also the sum of squared singular values of X, and the sum of squared moduli of X's matrix elements. We write $[a_{ij}]$ for the matrix with elements a_{ij}.

Linear maps ϕ. $M_m \rightarrow M_n$ are called *positive* if they preserve positive semidefiniteness. They also preseve Hermiticity (write Hermitian H as a sum of positive and negative semidefinite parts, and use linearity and positivity). A *stochastic* map takes the identity matrix I to itself. We may apply such a map ϕ to one subsystem of a bipartite system, while doing nothing to the other system. Applying it to the N-dimensional subsystem is just applying it to each block of the block matrix X. We call the resulting map on the bipartite system $\tilde{\phi}$,

$$\tilde{\phi}(X) := \begin{pmatrix} \phi(X_{1,1}) & \phi(X_{1,2}) & \cdots & \phi(X_{1,N}) \\ \phi(X_{2,1}) & \phi(X_{2,2}) & \cdots & \phi(X_{2,M}) \\ \cdots & \cdots & \cdots & \cdots \\ \phi(X_{N,1}) & \phi(X_{N,2}) & \cdots & \phi(X_{N,N}) \end{pmatrix}. \tag{2}$$

An important condition equivalent to separability of A is that for any stochastic positive linear map ϕ, $\tilde{\phi}(A)$ be positive semidefinite. We refer to it as the "Woronowicz condition." This appeared in Ref. [5], but was already essentially

proven (along with the sufficiency of the partial transposition map ("Woronowicz-Peres criterion") for two qubits or a $2 \otimes 3$ system, and a $2 \otimes 4$ counterexample) in Ref. [6], though the terminology of separability and entanglement is not used there. The proof there is given for a $2 \otimes N$ system ($N < \infty$), but it works for $M \otimes N$ by expanding the range of an index. We also use the following fact.

Fact. Let Δ be an $M \times M$ block matrix (whose blocks need not be square). Define Δ' as the matrix whose elements are the operator norms of the blocks of Δ. Then $||\Delta|| \leq ||\Delta'|| \leq M ||\Delta||$. The first inequality is well known; the second holds because $||\Delta_{ij}|| \equiv ||P_i \Delta Q_j|| \leq ||\Delta||$. ($P_i(Q_i)$ is the projector onto the ith subspace in the direct sum decomposition of the row (column) space that defines the blocks.] So, by adding to Δ' a matrix with non-negative entries (therefore not decreasing the norm) we can obtain $||\Delta||$ times the $M \times M$ all-ones matrix, whose norm is M.

III. MAIN RESULT: SEPARABILITY OF PERTURBATIONS OF THE IDENTITY

We give two proofs of the main result. Both proceed via Proposition 2, which states that stochastic positive linear maps on $n \times n$ matrices are contractive with respect to the l_∞ ("operator") norm of matrices, for *all* matrices. (The result for Hermitian matrices only is much easier.) Those interested only in the shortest proof, which uses the Naimark extension, may skip to the statement of Proposition 2 below. We think it is of interest to see the connections of the norm contraction result to two different concepts well known to quantum information theorists: in in the second proof, the Naimark extension and in the first proof, separability. The first proof proceeds via Proposition 1, which is a special case of recent results by one of us providing sufficient criteria for separability.

Proposition 1. If $||X|| \leq 1$, the block matrix

$$\begin{pmatrix} I & X \\ X^\dagger & I \end{pmatrix} \tag{3}$$

is separable. This is the $M = 2$ case of a recent theorem [7] that all positive semidefinite $M \times M$ block Toeplitz or block Hankel matrices whose blocks are $N \times N$ matrices are separable, whose proof we include here. The paper [7] also contains two alternative proofs for the special case $M = 2$. One of those proofs was independently discovered in Ref. [9].

Proof (of separability of positive semidefinite block Toeplitz matrices [7]). The proposition is a corollary to the following Lemma.

Lemma. Consider an $[(M+1) \times N]$ positive semidefinite block Toeplitz matrix T,

$$T = \begin{pmatrix} R_0 & R_1 & R_2 & \cdots & R_M \\ R_1^\dagger & R_0 & R_1 & \cdots & R_{M-1} \\ R_2^\dagger & R_1^\dagger & R_0 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ R_M^\dagger & R_{M-1}^\dagger & R_{M-2}^\dagger & \cdots & R_0 \end{pmatrix}.$$

(This structure is the definition of a Toeplitz matrix.) Suppose that $\mathcal{R}(T) = K$. Then there exist an $N \times K$ matrix X and a $K \times K$ unitary matrix U such the $T(i,j) = XU^{i-j}X^\dagger, 0 \leq i,j \leq M-1$.

Proof. Since our matrix T is positive semidefinite with $\mathcal{R}(T) = K$, $T = YY^\dagger$, where

$$Y = \begin{pmatrix} Y_0 & Y_1 & Y_2 & \cdots & Y_M \end{pmatrix}^T,$$

and each block Y_i is an $N \times K$ matrix. Define the upper submatrix Y_U as

$$Y_U = \begin{pmatrix} Y_0 & Y_1 & Y_2 & \cdots & Y_{M-1} \end{pmatrix}^T,$$

and, correspondingly, the lower submatrix Y_L as

$$Y_L = \begin{pmatrix} Y_1 & Y_2 & Y_3 & \cdots & Y_M \end{pmatrix}^T.$$

It follows straight from the Toeplitz structure that $Y_U Y_U^\dagger = Y_L Y_L^\dagger$. Thus there exists an unitary $K \times K$ matrix U such that $Y_L = Y_U U$ or in other words,

$$Y = \begin{pmatrix} Y_0 & Y_0 U & Y_0 U^2 & \cdots & Y_0 U^{M-1} \end{pmatrix}^T.$$

Recalling that $T = YY^\dagger$, we finally get the identities

$$T(i,j) = XU^{i-j}X^\dagger, 0 \leq i,j \leq M-1; X = Y_0.$$

Corollary. Using the notation of the proof above, put $U = V \text{Diag}(z_1, \ldots, z_K) V^\dagger$ where V is unitary and the complex numbers z_i have norm one, i.e., $\overline{z_i} = z_i^{-1}, 1 \leq i \leq K$. Denote the ith column of XV as L_i and $Z_i = (1, z_i, \ldots, z_i^{M-1})^T$, $1 \leq i \leq K$. Then the following "separability" representation holds:

$$T = \sum_{1 \leq i \leq K} Z_i Z_i^\dagger \otimes L_i L_i^\dagger.$$

We can use Proposition 1 to show a contraction inequality (Proposition 2 below). We got the idea of using separability to obtain operator inequalities involving stochastic positive maps from Ref. [6], where the Kadison inequality $\phi(X^2) \geq [\phi(X)]^2$ for stochastic ϕ and Hermitian X is implicitly connected with the separability of

$$\rho = \begin{pmatrix} I & X \\ X & X^2 \end{pmatrix}.$$

In a sense, for $M = 2$ separability of ρ is equivalent to Proposition 1, as in this case there is a local unitary transformation $\rho \mapsto (A \otimes I)\rho(A^\dagger \otimes I)$ which maps block Toeplitz matrices to block Hankel ones (see Ref. [7]),

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

One can probably prove the next proposition using the Kadison inequality and this transformation.

Proposition 2. Let $\phi : M_n \to M_n$ be a stochastic positive linear map. Then for any $X \in M_n$, $||\phi(X)|| \leq ||X||$.

Proof 1. We show that $\phi(X) \leq 1$ if $||X|| \leq 1$; the proposition follows by ϕ's linearity. Apply $\tilde{\phi}$ to the separable state of Proposition 1, obtaining

$$\begin{pmatrix} I & \phi(X) \\ \phi(X^\dagger) & I \end{pmatrix}. \tag{4}$$

Write $X = X_1 + iX_2$ with X_1, X_2 Hermitian. Then $\phi(X^\dagger) = \phi(X_1^\dagger - iX_2^\dagger) =$ (by Hermiticity preservation of ϕ, which follows from its positivity) $\phi(X_1)^\dagger - i\phi(X_2)^\dagger = \phi(X_1 + iX_2)^\dagger = \phi(X)^\dagger$. Hence Eq. (4) is equal to

$$\begin{pmatrix} I & \phi(X) \\ \phi(X)^\dagger & I \end{pmatrix}. \tag{5}$$

Since this resulted from applying $\tilde{\phi}$ to a separable state, it is a positive semidefinite matrix. Positivity of this matrix is equivalent (cf. e.g., Ref. [10], p. 472) to $\phi(X)^\dagger \phi(X) \leq I$; i.e., $x^\dagger \phi(X)^\dagger \phi(X) x \leq 1$ for all normalized x, i.e., $||X|| \leq 1$.

This proof was independently discovered in Ref. [9]. Let us present a very different proof which does not use separability but another concept well known in the quantum information community.

Proof 2 (lifting). It is well known that the extreme points of the matrix ball $\{X : ||X|| \leq 1\}$ are unitary matrices. Thus we can assume that X is unitary, i.e., $X = \sum_{1 \leq i \leq N} z_i e_i e_i^\dagger$, where $|z_i| = 1, 1 \leq i \leq N$ and $\{e_i, 1 \leq i \leq N\}$ is an orthonormal basis in C^N. Thus $\phi(X) = \sum_{1 \leq i \leq N} z_i Q_i, Q_i = \phi(e_i e_i^\dagger)$. Since ϕ is a positive stochastic map,

$$Q_i \geq 0 (1 \leq i \leq N) \text{ and } I = \sum_{1 \leq i \leq N} Q_i.$$

By Naimark's theorem [11,12] (cf. Ref. [13] for a simple exposition in finite dimension) there exist commuting orthogonal projectors $P_i : C^K \to C^K, N \leq K \leq N^2$, and a unitary injection $U : C^N \to C^K$ such that

$$Q_i = U^\dagger P_i U (1 \leq i \leq N) \text{ and } I = \sum_{1 \leq i \leq N} P_i.$$

It is easy to see that $||\sum_{1 \leq i \leq N} z_i P_i|| \leq 1$. Thus

$$\left\| \sum_{1 \leq i \leq N} z_i Q_i \right\| \leq \|U^\dagger\| \left\| \sum_{1 \leq i \leq N} z_i P_i \right\| \|U\| \leq 1. \tag{6}$$

This second proof suggests that there might be a deeper connection between Naimark's theorem and separability.

We proceed to the main theorems.

Theorem 1. The matrix $I + \Delta$ is separable for all Hermitian Δ with $||\Delta||_2 \leq 1$.

Proof.

$$||\tilde{\phi}(\Delta)||^2 \leq ||A||^2 \leq ||A||_2^2, \tag{7}$$

where $A := [a_{ij}]$, $a_{ij} := ||\phi(\Delta_{ij})||$.

$$||A||_2^2 = \sum_{ij} a_{ij}^2 = \sum_{ij} ||\phi(\Delta_{ij})||^2. \tag{8}$$

(The first inequality is because the operator norm of a block matrix is bounded above by that of the matrix whose elements are the norms of the blocks, and the second is because the Frobenius norm is an upper bound to the operator norm.) But $||\phi(\Delta_{ij})||^2 \leq ||\Delta_{ij}||$ by Proposition 2, and this in turn is less than $||\Delta_{ij}||_2$. So

$$||\tilde{\phi}(\Delta)||^2 \leq \sum_{ij} ||\phi(\Delta_{ij})||^2 \leq \sum_{ij} ||\Delta_{ij}||_2^2 \equiv ||\Delta||_2^2 \leq 1, \quad (9)$$

the last inequality being the premise of the theorem. Having shown that $||\tilde{\phi}(\Delta)|| \leq I$, and also using $\tilde{\phi}(I) = I$, we get $\tilde{\phi}(I + \Delta) \geq 0$, so that by Woronowicz' criterion $I + \Delta$ is separable.

IV. COROLLARIES AND ADDITIONAL RESULTS: MAXIMALITY OF BALLS, SCALING, AND SPECIFIC PERTURBATIONS

Let us now present some corollaries of Theorem 1. Define $||\Delta||_p := (\Sigma_i |\lambda_i|^p)^{1/p}$ (λ_i being the eigenvalues of the square Hermitian matrix Δ.)

Corollary 1 (l_p balls). Consider an $N \times N$ system. Then the matrix $I + \Delta$ is separable for all Hermitian Δ with $||\Delta||_p \leq 1 (1 \leq p \leq 2)$ and $||\Delta||_p \leq B(N,p) =: N^{2/p-1}(2 \leq p \leq \infty)$.

Proof. The statements follow from basic p-norm inequalities: the first from the $q = 2$ cases of $||\Delta||_p \geq ||\Delta||_q$ (for $1 \leq p \leq q$), the second from the $q = 2$ cases of $||\Delta||_q \leq n^{1/q - 1/p}||\Delta||_p$ (for $p \geq q$). Note that the dimension n is N^2 in our case. [These inequalities are equivalent to similar ones for the vector p norms $||x||_p := (\Sigma_i x_i^p)^{1/p}$; the first set can be proved by changing variables to $y_i = x_i^p$ and using the triangle inequality for norms, the second by letting $y_i = x_i^q$ and using the convexity of $f: z \mapsto z^\alpha$ for $\alpha \geq 1$ ($\alpha = p/q$ in our case).]

The l_∞ result was also obtained very recently in Ref. [9] using quite different methods. The p balls in Corollary 1 are clearly the largest possible for $1 \leq p \leq 2$: by subtracting any normalized pure state, for which all these p norms are 1, we can leave the positive, and hence the separable, cone. What about $2 < p \leq \infty$? Theorem 3 will show that these are the largest balls for these norms, too.

The next theorem gives information about how fast we can reach the entangled states by perturbing the identity in a specific direction: adding a positive multiple of a pure state. The main point is that, perhaps surprisingly, the entangled states are reached fastest by perturbing with a $2 \otimes 2$ Bell state, rather than, say, a maximally entangled state.

Theorem 2 (Perturbation by positive multiples of pure states). (1) Consider a pure ρ corresponding to a state $|\psi\rangle = \Sigma_{ij} \psi_{ij} e_i \otimes e_j$, $1 \leq i,j \leq N$. The the spectrum of ρ^T is $[d_1^2, \ldots, d_N^2; d_i d_j, -d_i d_j (1 \leq i \neq j \leq N)]$, where $d_1, \ldots, d_N$ are the singular values of the $N \times N$ matrix $\psi := [\psi_{ij}: 1 \leq i,j \leq N]$ (thus $d_1^2 + \cdots + d_N^2 = 1$). (2) Define

$$W(N) = \min_{\rho \in \mathcal{D}(N,N)} -\lambda_{min}(\rho^T),$$

where $\mathcal{D}(N,N)$ is the set of density matrices of $N \times N$ systems. Then $W(N) = \frac{1}{2}$. (3) If $I + a\rho$ is separable for all ρ and $a > 0$ then $a \leq W(N)^{-1} = 2$.

Proof. Diagonalize ψ by local unitaries using the singular value ("Schmidt") decomposition obtaining Diag($d_1, \ldots, d_N$). The corresponding density matrix has blocks $\rho_{ij} = d_i d_j e_i e_j^\dagger$, and the spectrum of ρ^T (which is not changed by applying local unitaries prior to partial transposition) is as given in part (1) of Theorem 2. The bound in part (2) follows from $2ab \leq a^2 + b^2$ and is achieved by $(1/\sqrt{2}, 1/\sqrt{2}, 0, \ldots, 0)$. The Woronowicz-Peres (WP) condition gives part (3).

Contrary to the "folklore," in the result above, the fully entangled state is not the worst one; rather, the worst is a maximally entangled state of two local two-dimensional subspaces.

Theorem 3 establishes the maximum size of the p balls for $p > 2$. The proof involves considering perturbations by a positive multiple of the maximally entangled state and establishes when this procedure hits the entangled states. Before formulating the theorem we introduce some notation. $\mathcal{C}_{WP}(N,N)$ is the closed convex cone of $N^2 \times N^2$ positive matrices satisfying the WP condition, i.e., $\rho \in \mathcal{C}_{WP}(N,N)$ iff $\rho \geq 0$ and $\rho^T \geq 0$. $\mathcal{C}_{Sep}(N,N)$ is the closed convex cone of *separable* positive matrices. Obviously $\mathcal{C}_{WP}(N,N) \subset \mathcal{C}_{Sep}(N,N)$. Both $\mathcal{C}_{WP}(N,N)$ and $\mathcal{C}_{Sep}(N,N)$ are subsets of the real N^4-dimensional linear space $H(N^2)$ of Hermitian $N^2 \times N^2$ matrices. The cone dual to a convex set X (which need not be a cone) is $X^* := \{y: \langle y,x \rangle \geq 0, \forall x \in X\}$.

Theorem 3. Suppose $p > 2$. If the p ball $\mathcal{B}(N,p,a) = \{A \in H(N^2): A = I + \Delta, ||\Delta||_p \leq a\}$ belongs to $\mathcal{C}_{WP}(N,N)$ then $a \leq B(N,p) =: N^{-1+2/p}(2 \leq p \leq \infty)$.

As $\mathcal{C}_{WP}(N,N) \subset \mathcal{C}_{Sep}(N,N)$ this theorem proves that the l_p balls $\mathcal{B}[N,p,B(N,p)]$ in Corollary 1 are largest possible. Moreover, the form of the states $I + a\rho_E$ in the proof shows that for $p > 2$, parts of the boundary are in the interior of the positive cone, so that there are entangled states just beyond. For $p = 2$, $N^{2/p-1} = 1$, so the points $I + a\rho_E$ are at the edge of the positive cone; however, in Sec. V we will prove Theorem 4, which allows us to exhibit interior points of the positive cone that are on the boundary of the largest ball for $p = 2$ as well.

Proof of Theorem 3. It is easy to see that the cone dual to $\mathcal{B}(N,p,a)$, i.e., $\mathcal{B}(N,p,a)^*$, is $\{A \in H(N^2): \text{tr}(A) \geq a||A||_q, q = p/(p-1)\}$. It is known [6] that $\mathcal{C}_{WP}(N,N)^* = \{\rho_1 + \rho_2^T: \rho_i \geq 0, i = 1,2\}$. If $\mathcal{B}(N,p,a) \subset \mathcal{C}_{WP}(N,N)$ then $\mathcal{C}_{WP}(N,N)^* \subset \mathcal{B}(N,p,a)^*$ and at least $\text{tr}(\rho) = \text{tr}(\rho^T) \geq ||\rho^T||_q$ for all $\rho \geq 0$. Consider the fully entangled pure $N \times N$ state ρ_E. Then $\text{tr}(\rho_E) = 1$. It follows from part (1) of Theorem 2 that ρ_E^T has $N + N(N-1)/2$ eigenvalues equal to $1/N$ and $N(N-1)/2$ eigenvalues equal to $-1/N$. Thus we get that $1 \geq a||\rho_E||_q = aN^{(2-q)/q}$ and, finally, $a \leq N^{(q-2)/q} = N^{2/p-1}$.

The following corollary of Theorem 1 gives (as is evident from the proof) the strongest sufficient condition for separa-

bility of $A \geq 0$ that can be derived by scaling [considering all ways of writing $A = \zeta(I+\Delta)$ with $\zeta > 0$] and using the Frobenius norm case of Theorem 1 (applied to Δ).

Corollary 2 (scaling). Let A be an (unnormalized) density matrix of a bipartite system with total dimension $d = NM$ and $\lambda = (\lambda_1, \ldots, \lambda_d)$ be the vector of eigenvalues of A. If

$$S(\lambda) =: d - \frac{||\lambda||_1^2}{||\lambda||_2^2} \leq 1 \tag{10}$$

then A is separable.

Proof. It is easy to see that $S(\lambda) = \min_{a>0} ||a\lambda - e||_2^2$, where e is a vector of all ones. Therefore if $S(\lambda) \leq 1$ then $A = b(I + \Delta)$, where $b > 0$ and $||\Delta||_2^2 \leq 1$. It follows from Theorem 1 that $A = b(I + \Delta)$ is separable.

Corollary 3 (largest Frobenius ball for density matrices). Suppose that A is a normalized density matrix of a bipartite system with total dimension $d = NM$, i.e., $\Sigma_{1 \leq i \leq d} \lambda_i = 1$ and $\lambda_i \geq 0, 1 \leq i \leq d$. If $||A - (1/d)I||_2^2 = ||\lambda - (1/d)e||_2^2 \leq 1/d(d-1) =: r^2$ then A is separable. r is the largest such constant.

Proof. Define $t = \lambda - (1/d)e$. Then $||\lambda||_1^2 = 1$ and $||\lambda||_2^2 = 1/d + ||t||_2^2$. Thus $S(\lambda) = d - 1/(||t||_2^2 + 1/d)$ and $S(\lambda) \leq 1$ if and only if $||t||_2^2 \leq 1/d(d-1)$. From Corollary 2 it follows that A is separable. On the other hand, $r = 1/\sqrt{d(d-1)}$ is the radius of the largest ball inside the d-dimensional simplex.

Remark. In terms of the "purity" $\mathrm{tr}\, \rho^2$ of the density matrix (which takes the value 1 for pure states and $1/d$ for the maximally mixed state), Corollary 3 says that ρ is separable if its purity is less than or equal to $1/(d-1)$.

One might conjecture that for $N \times N$ bipartite systems (so $d = N^2$), any λ not satisfying Eq. (10) is the spectrum of some nonseparable positive matrix. This is not so: a sufficient condition for separability of two-qubit density matrices in terms of the spectrum is [14] $\lambda_1 - \lambda_3 - \sqrt{\lambda_2 \lambda_4} \leq 0$, where λ_i are decreasingly ordered. This can hold when the purity is greater than 1/3, as also noted in Ref. [15].

Corollary 4. The matrix $I + a\rho$, where ρ is an $N \times N$ state, is separable if $-1 \leq a \leq N^2/(N^2-2)$.

Proof. Clearly it is enough to prove this for pure states. In this case the vector of eigenvalues of $I + a\rho$ is

$$\lambda_a =: (1, 1, \ldots, 1, 1+a).$$

Direct computation gives that $S(\lambda_a) = N^2 - (N^2+a)^2/(N^2 + 2a + a^2)$. It follows that $S(\lambda_a) \leq 1$ if and only if $-1 \leq a \leq N^2/(N^2-2)$.

Corollary 5. If we consider the normalized mixtures $\sigma = (1-\epsilon)I/d + \epsilon\rho$, for pure ρ, and scale them as

$$\sigma = \frac{1-\epsilon}{d}\left(I + \frac{d\epsilon}{1-\epsilon}\rho\right), \tag{11}$$

by Corollary 4 these are separable if $\epsilon \leq 1/(d-1) \equiv 1/(N^2-1)$.

A very slightly better, but messier, bound can be obtained by solving a quadratic equation derived from Corollary 2,

reminding us that the most obvious or tractable scaling is not generally the best. Corollary 5 is of course also true for mixed ρ.

V. PERTURBATION OF THE IDENTITY BY POSITIVE MULTIPLES OF PROJECTORS

A final result again illustrates the power of scaling (Corollary 2). It gives us the most negative eigenvalue of a partial transpose of a projector on a bipartite system. This is interesting because it tells us when we will hit the entangled matrices if we add a positive multiple of that projector to the identity. Define

$$W_m(N) := \min_{\rho \in \mathcal{P}(m,N)} -\lambda_{min}(\rho^T),$$

where $\mathcal{P}(m,N)$ stands for the compact set of all rank m orthogonal projectors in $C^N \otimes C^N$. Notice that part (2) of Theorem 2 states that $W_1(N) = W(N) = \frac{1}{2}$; clearly $W_N(N) = 0$, it follows from Theorem 1 that also $W_{N-1}(N) = 0$; it is easy to prove that if K/L is an integer then $W_K(N)/K \leq W_L(N)/L$.

Theorem 4.

$$W_{N(N-1)/2}(N) = \frac{N-1}{2}.$$

Proof. Let us define the following operator intervals:

$$\mathcal{I}(a,N) =: \{\rho : C^N \otimes C^N \to C^N \otimes C^N : (1+a)I \geq \rho \geq I\}.$$

It follows by a straightforward rescaling from the l_∞ part of Corollary 1 and Theorem 3 that we have the following properties.

Property 1. If $0 \leq a \leq 2/(N-1)$ then all matrices in $\mathcal{I}(a,N)$ are separable (and thus satisfy the Woronowicz-Peres condition).

Property 2. If $a > 2/(N-1)$ then there exists a matrix in $\mathcal{I}(a,N)$ which does not satisfy the Woronowicz-Peres condition.

It is easy to see that the extreme points of the compact convex set $\mathcal{I}(a,N)$ are of the form $I + aP$, where P is an arbitrary orthogonal projector; correspondingly d dimensional vectors composed of eigenvalues of extreme points have (up to permutations) the following form:

$$\lambda_{m,a} = e + aV_m, 0 \leq m \leq d = N^2,$$

where e is the all-ones vector and vector V_m has its first m coordinates equal to 1 and the rest equal to 0. Simple algebra gives that $S(\lambda_{N(N-1)/2,2/(N-1)}) = 1$ and $S(\lambda_{k,2/(N-1)}) < 1$ for all $k \neq N(N-1)/2$. Therefore if $\epsilon > 0$ is small enough then $S(\lambda_{k,2/(N-1)+\epsilon}) < 1$ for all $k \neq N(N-1)/2$. Corollary 2 implies that for all small enough $\epsilon > 0$ matrices $I + [2/(N-1) + \epsilon]P$ are are separable (and thus satisfy the Woronowicz-Peres condition) provided that P is an orthogonal projector of rank $k \neq N(N-1)/2$. It follows from Property 2 above that for all $a > 2/(N-1)$ there exists an orthogonal projector P_a such that $I + aP_a$ does not satisfy the Woronowicz-Peres condition, in other words that

$$|\lambda_{min}(P_a^T)| > a^{-1}.$$

It follows that if $a = 2/(N-1) + \epsilon$ and $\epsilon > 0$ is small enough then necessarily the rank $\mathcal{R}$ satisfies

$$\mathcal{R}(P_a) = \frac{N(N-1)}{2}.$$

Thus $W_{N(N-1)/2}(N) \geq (N-1)/2$, but Property 1 above implies that $W_{N(N-1)/2}(N) \leq (N-1)/2$. Therefore,

$$W_{N(N-1)/2}(N) = \frac{N-1}{2}.$$

One implication of this result is that the boundary of the largest $p=2$ ball also contains points in the interior of the postive cone. One sees this by noting that $a = 2/(N-1)$ is the largest a for which $I + aP$ is separable, where P is the rank $N(N-1)/2$ projector achieving the value $W_{N(N-1)/2} = (N-1)/2$ of Theorem 4. For all greater a, the matrix is entangled; so is the scaled operator $(N-1)/N$ times this matrix. But for $a = 2/(N-1)$ this scaled matrix satisfies $[(N-1)/N](I + aP) = I + \Delta$, where Δ is Hermitian with $N(N+1)/2$ eigenvalues $-1/N$ and $N(N-1)/2$ eigenvalues $+1/N$. This is well within the interior of the positive cone, and $||\Delta||_2 = 1$.

VI. DISCUSSION AND CONCLUSION

For a product of RN-dimensional systems in a mixture

$$\rho = (1-\epsilon)I/N^R + \epsilon \rho' \qquad (12)$$

(ρ' a normalized density matrix) [4], extending Ref. [3], found lower and upper bounds on the value $\epsilon_{max}(\rho)$ below (and at) which the state can be guaranteed to be separable: $1/(1+N^{2R-1}) \leq \epsilon_{max}(\rho) < 1/(1+N^{R-1})$. (The $N=2$ case is in Ref. [3].) For bipartite systems ($R=2$), these bounds are $1/(1+N^3)$ and $1/(1+N)$. The lower bound is close to what one can get from the l_∞ (operator norm) result, while the upper bound comes from mixing in the maximally entangled ρ_E. The results of this paper give $1/(N^2-1) \leq \epsilon_{max}(\rho) \leq 2/(2+N^2)$. The lower bound is via Corollary 5 of Theorem 1, and is tighter due to the use of Frobenius rather than operator norm; the upper bound uses Theorem 2 and the same scaling as in Corollary 5, and is tighter because the maximally entangled state is not the optimal state to mix in.

Our knowledge of the exact size of the two-norm ball in the bipartite case gives us a bound exponentially better than known bounds on $\epsilon_{max}(\rho)$. This shows how much more powerful our sufficient condition for separability is than previously known geometric conditions, in the bipartite setting.

It is also illuminating to investigate the implications of our results in the multipartite setting; we will compare with the results of Refs. [4,3] mentioned above. For multipartite states ($R > 2$) we get a slightly better upper bound on $\epsilon_{max}(\rho)$. For example, for even R, $\epsilon_{max}(\rho) \leq 2/(2+N^R)$, by dividing the systems into equal sized sets and viewing the state as bipartite. For qubits, this is actually the same as in Ref. [3], although since we used a slightly less than optimal scaling, we could improve it a bit. Our results also imply that no matter what state ρ is mixed in, if $\epsilon \leq 1/(N^R-1)$, the state is separable with respect to every bipartition. This is dramatically larger than bound of Ref. [3] below which the state is guaranteed separable, but not directly comparable because a state can be separable with respect to every such bipartition yet not be separable [16]. This raises the important question of the size of the largest separable ball in the multipartite case, to which we expect our methods can contribute.

In conclusion, we have found the exact size of the largest p-norm balls of entangled states around the identity, for all $1 \leq p \leq \infty$, and established for $2 \leq p \leq \infty$ that the edge of these balls can be reached within the positive cone. Applied via scaling as we illustrated with several corollaries and examples, this yields sufficient conditions for separability which can be exponentially stronger in many situations than previously known conditions. In particular, we found the strongest such condition statable in terms of the spectrum of a density matrix, and derivable via scaling of the $p=2$ result: for normalized density matrices of $d \otimes d$ systems, it is that the purity tr ρ^2 be less than $1/(d-1)$. In addition, for three special classes of perturbations (positive multiples of pure states, positive multiples of the maximally entangled state, and positive multiples of projectors), we found the smallest perturbation in the class achieving entanglement. The pure state result, that it is a $2 \otimes 2$ Bell state rather than an $N \otimes N$ maximally entangled state, is not only mathematically interesting but transparent in meaning, and possibly surprising. These are natural special classes of perturbations that have been previously considered in quantum information theory, so we expect that these results will find application in many appropriate situations. Because of the natural geometric form of our general sufficient conditions for separability (Theorem 1) and related results, their status as a basic aspect of the geometry of the entangled states, and the important role of these balls in computational questions, we anticipate many applications for them, in theory and in the interpretation and engineering of experiments that aim to produce entanglement.

[1] R. Jozsa and N. Linden, e-print quant-ph/0201143.

[2] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).

[3] S. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

[4] P. Rungta, W. J. Munro, K. Nemoto, P. Deuar, G. J. Milburn,

and C. M. Caves, in *Directions in Quantum Optics: A Collection of Papers Dedicated to the Memory of Dan Walls*, edited by D.F. Walls, R.J. Glauber, M.O. Scully, and H. Carmichael (Springer, New York, 2001).

[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[6] S.L. Woronowicz, Rev. Mod. Phys. **10**, 165 (1976).

[7] L. Gurvits, LANL Unclassified Technical Report No. LAUR-01-2030, 2001 (unpublished).

[8] L. Gurvits, e-print quant-ph/0201022.

[9] T. Ando (unpublished).

[10] R.A. Horn and C.R. Johnson, *Matrix Analysis* (Cambridge

University Press, Cambridge, 1985).

[11] M.A. Neumark, Izv. Akad. Nauk. SSSR, Ser. Mat. 4 **53**, 277 (1940).

[12] M.A. Neumark, C. R. (Dokl.) Acad. Sci. URSS **41**, 359 (1943).

[13] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).

[14] F. Verstraete, K. Audenaert, and B. De Moor, Phys. Rev. A **64**, 012316 (2001).

[15] K. Zyczkowski and M. Kús, Phys. Rev. A **63**, 032307 (2001).

[16] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).