Separable balls around the maximally mixed multipartite quantum states

Leonid Gurvits and Howard Barnum
CCS-3, Mail Stop B256, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA
(Received 19 February 2003; published 14 October 2003)

We show that for an m-partite quantum system, there is a ball of radius $2^{-(m/2-1)}$ in Frobenius norm, centered at the identity matrix, of separable (unentangled) positive semidefinite matrices. This can be used to derive an ϵ below which mixtures of ϵ of any density matrix with $1-\epsilon$ of the maximally mixed state will be separable. The ϵ thus obtained is exponentially better (in the number of systems) than existing results. This gives a number of qubits below which nuclear magnetic resonance with standard pseudopure-state preparation techniques can access only unentangled states; with parameters realistic for current experiments, this is 23 qubits (compared to 13 qubits via earlier results). A ball of radius 1 is obtained for multipartite states separable over the reals.

DOI: 10.1103/PhysRevA.68.042312 PACS number(s): 03.67.Mn, 03.67.Lx

I. INTRODUCTION

Entanglement is an important quantum resource, useful in quantum computation, cryptography, and communication protocols. Entangled quantum states are those that cannot be expressed as a mixture of product states. That is, if a (not necessarily normalized, but positive semidefinite) state ρ is an entangled state of m systems (an ''m-partite state''), there is no way to choose positive p_i and states $\rho_i^1,\ldots,\rho_i^m$ for systems 1 through m, such that

$$\rho=\sum_i p_i\rho_i^1\otimes\cdots\otimes\rho_i^m. \tag{1}$$

(If state ρ is normalized, tr $\rho=1$, we get an equivalent definition even if p_i are required to be probabilities, $\Sigma_i p_i=1$.) In this paper, we provide a simple geometric condition sufficient to guarantee separability (nonentanglement) of an m-partite unnormalized state: that the state is proportional to the identity matrix plus a Hermitian perturbation Δ whose Frobenius norm (2-norm) is no greater than $2^{-(m/2-1)}$. This is exponentially better than the best previous bounds we are aware of [1,2]. We use it to obtain balls of normalized separable states. Because the set of separable (unentangled) density matrices is convex, and the size of the largest ball that fits inside it (as well as the smallest ball that covers it) is important to complexity-theoretic questions involving convex sets, we expect the result to have applications in complexity questions about entanglement, such as the complexity of deciding whether or not a multipartite state is entangled. Equally importantly, it can help determine whether or not entanglement is present in interesting theoretical and experimental situations. For example, though the utility of the criterion is emphatically not restricted to such states, it gives us a bound on the ''polarization'' ϵ below which ''pseudopure'' states of the form $(1-\epsilon)I/d+\epsilon\pi$, with π pure, I the identity operator on a multipartite state space of overall dimension d, are separable. Applied to liquid-state nuclear magnetic resonance (NMR) with preparation of an initial pseudopure state, at a temperature of 300 K in an 11 T external field, our criterion implies that unless we have 23 or more nuclear-spin qubits only separable states can be produced (compared to 13 qubits using the bound in Ref. [1]).

The methods of Refs. [1], [2] are very different from ours: they expand the density matrix in an overcomplete basis of pure states and find conditions guaranteeing positivity of all coefficients of the expansion, thus giving an explicit decomposition of form (1). In contrast, the methods we use have a nonconstructive flavor: although they establish that any m-partite (unnormalized) density matrix within a distance $1/2^{(m/2-1)}$ is separable, they do not provide an explicit ''separable representation'' (1) of it. Our methods use general concepts of matrix theory and convex analysis in terms of which the problem is naturally formulated, and involve only short and elementary calculations. This paper is a natural sequel to Ref. [3] in the sense that almost the same mathematics is used. The main (though quite simple) difference here is a generalization of *separability*, so-called $(C_1\otimes C_2\otimes\cdots\otimes C_m)$ separability, where C_i are matrix cones (see Definition 2 below). This generalization arises naturally in extending the bipartite result of Ref. [3] to m-partite systems with $m\geqslant 3$. A reader comfortable with the technique used in Ref. [3] should have no extra problems in understanding this paper.

We also study cones of ''real-separable'' Hermitian matrices, lying in a particular linear subspace of the Hermitian matrices, and find a larger separable ball, the unit Frobenius-norm ball, of matrices in this space. Real separability of a matrix is shown equivalent to separability and being in the aforementioned linear subspace, which turns out to be the tensor product of the local spaces of real symmetric matrices. This may be viewed as a situation in which the density matrix obeys particular symmetries, and it may be useful to have a bound for this situation (which is in any case of mathematical interest). Also, real Hilbert spaces and real separability have been studied in relating quantum information theory to foundational questions and ''generalized information theory'' [4,5], so our results are relevant to such matters. The results on real separability are not required in order to understand the results on ordinary separability, and may be omitted by readers only interested in the latter.

II. NOTATION AND MATHEMATICAL PRELIMINARIES

The mathematical notion of a "regular" positive cone (which we will just call cone) is basic in quantum-information science, especially in the study of entanglement. This is so because the unnormalized quantum states, the unnormalized separable states of a multipartite quantum system, the completely positive maps, the positive maps, and many other sets of interest form such cones. (Appropriate normalizationlike conditions, such as unit trace for states or trace preservation or trace nonincrease for maps, are usually just additional linear equalities or inequalities.) In this section, we review regular positive cones and related notions; background and preliminaries specific to the separable cones (of unentangled states) appear at the beginning of the following section.

Definition 1. A positive cone is a subset K of a real vector space V closed under multiplication by positive scalars. It is called regular if it is (a) convex (equivalently, closed under addition: $K+K=K$), (b) generating ($K-K=V$, equivalently K linearly generates V), (c) pointed ($K\cap -K=\varnothing$, so that it contains no nonnull subspace of V), and (d) topologically closed (in the Euclidean metric topology, for finite dimension).

Such a positive cone induces a partial order $\geqslant_K$ on V, defined by $x\geqslant_K y := x-y\in K$. This partial order is "linear compatible": inequalities can be added and multiplied by positive scalars. A set S is said to *generate* a cone K if K is the set of *positive* linear combinations of elements of S. The topological closure condition guarantees that such a cone is generated (via addition) by its *extreme rays*. These are sets $R_x := \{\lambda x : \lambda \geqslant 0\}$ such that no $y\in R_x$ can be written as a convex combination of elements of C that are not in R_x. We will not make much use of closure and extremality, but at some points we use the fact that positive semidefinite (PSD) matrices can be written as convex combinations of rank-1 PSD matrices (these being the members of the extreme rays of the cone of PSD matrices).

Duality is often a useful tool when dealing with cones. An inner product, written $\langle \cdots,\cdots\rangle$, on a finite-dimensional V selects a particular way of identifying V with with its dual [the space of linear functions ("functionals") from V to $\mathbf{R}$]. The cone C^* dual to C (the set of linear functionals which are non-negative on C) is identified with $\{y\in V : \langle y,x\rangle \geqslant 0, \forall\, x\in C\}$. We define the adjoint of ϕ: $V_1\to V_2$ as $\phi^\dagger : V_2\to V_1$ via

$$\langle B,\phi(A)\rangle = \langle \phi^\dagger(B),A\rangle \tag{2}$$

for all $A\in V_1$, $B\in V_2$.

We say a linear map ϕ: $V_1\to V_2$ is C_1-to-C_2 positive, for cones $C_1\subset V_1$, $C_2\subset V_2$, if $\phi(C_1)\subseteq C_2$. The following proposition is easily (but instructively) verified.

Proposition 1. If $\phi(C_1)\subseteq C_2$, then $\phi^\dagger(C_2^*)\subseteq C_1^*$.

For complex matrices M, we use $M^\dagger$ to denote the transpose of the entrywise complex conjugate of the matrix. (The transpose itself we denote M^T.) The *positive semidefinite cone* $\mathcal{P}(d)$ in the real linear space of Hermitian $d\times d$ matrices is the set of matrices M such that $x^\dagger M x\geqslant 0$ for all $x\in \mathbf{C}^d$. If we use the trace inner product $\langle X,Y\rangle := \mathrm{tr}\, XY$ to identify V^* with V, it is equal to its dual. We will denote by "$\geqslant$" the partial order induced by this cone, and often write $M\geqslant 0$ for the equivalent $M\in\mathcal{P}(d)$.

We will have several occasions to use the following proposition, which follows from the fact that for normal (including Hermitian) matrices Δ, $\|\Delta\|_\infty$ is the largest modulus of an eigenvalue of Δ.

Proposition 2. Let Δ be Hermitian. Then $I+\Delta\geqslant 0$ is equivalent to $\|\Delta\|_\infty\leqslant 1$.

We define more notation.

Definition 2. The linear space of $N\times N$ complex matrices is denoted as $M(N)$, the linear space over the reals of $N\times N$ real matrices is denoted as $M_{\mathbf{R}}(N)$, the linear space of real symmetric $N\times N$ matrices is denoted as $\Sigma_{\mathbf{R}}(N)$, and the linear space over reals of $N\times N$ complex Hermitian matrices is denoted as $\mathcal{H}(N)$. The space of complex block matrices, K blocks by K blocks, with blocks in $M(N)$, is denoted as $\mathcal{B}(K,N)$.

III. SEPARABLE CONES

Let us consider an m-partite unnormalized density matrix (i.e., just positive semidefinite)

$$\rho : H_1\otimes H_2\otimes\cdots\otimes H_m \to H_1\otimes H_2\otimes\cdots\otimes H_m$$

Let $\dim(H_i)=d_i$, $1\leqslant i\leqslant m$. Then any such

$$\rho = \{\rho(i_1,i_2,\ldots,i_m;j_1,j_2,\ldots,j_m),$$

$$1\leqslant i_k,j_k\leqslant d_k; 1\leqslant k\leqslant m\}.$$

Let us block partition ρ with respect to the first index:

$$\rho := \begin{pmatrix} \rho^{1,1} & \rho^{1,2} & \cdots & \rho^{1,d_1} \\ \rho^{2,1} & \rho^{1,2} & \cdots & \rho^{2,d_1} \\ \cdots & \cdots & \cdots & \cdots \\ \rho^{d_1,1} & \rho^{d_1,2} & \cdots & \rho^{d_1,d_1} \end{pmatrix}, \tag{3}$$

where the blocks are

$$\rho^{i,j} : H_2\otimes\cdots\otimes H_m \to H_2\otimes\cdots\otimes H_m$$

and

$$\rho^{i,j} = \{\rho(i,i_2,\ldots,i_m;j,j_2,\ldots,j_m\},\ 1\leqslant i_k,\ j_k\leqslant d_k;\ 2\leqslant k\leqslant m.$$

We will make use of a well-known isomorphism between the spaces of linear maps from $M(K)$ to $M(N)$ and $\mathcal{B}(K,N)$. For any $M\in\mathcal{B}(K,N)$ let χ_M be the map χ defined via $\chi(e_i e_j^\dagger)=M^{i,j}$. Here e_i is the $1\times K$ matrix with 1 in the ith place, zero elsewhere, so $e_i e_j^\dagger$ is the "matrix unit," with 1 in the i,j place and 0 elsewhere. $e_i e_j^\dagger$ are a basis for $M(K)$, so this determines χ_M. We could use the same equation to determine a block matrix M_χ from a map χ, so this is an isomorphism of vector spaces, in fact $\chi_{M_\chi}=\chi$. In the quantum-information literature this is sometimes called the "Jamiolkowski isomorphism" (or equivalence); we have

also called M_χ the "Choi matrix" of χ. It has the important and easily verified property given as follows.

Proposition 3. $\mathrm{tr}\,[\chi(A)B]=\mathrm{tr}\,[M_\chi(A^T\otimes B)]$.

Definition 3. Consider cones $C_i\subset M(d_i)$, $1\leqslant i\leqslant m$. A matrix

$$\rho:H_1\otimes H_2\otimes\cdots\otimes H_m\rightarrow H_1\otimes H_2\otimes\cdots\otimes H_m$$

[i.e., $\rho\in M(d_1d_2\cdots d_m)$] is called $(C_1\otimes C_2\otimes\cdots\otimes C_m)$ separable if it belongs to the cone generated by the set $\{A_1\otimes A_2\otimes\cdots\otimes A_m:A_i\in C_i,1\leqslant i\leqslant m\}$. We call this the separable cone $S(C_1,C_2,\ldots,C_m)$.

This is trivially equivalent to the recursive definition: $S(C_1,C_2,\ldots,C_m)$ is the cone generated by the pairs $A_1\otimes B$ with $A_i\in C_1$, $B\in S(C_2,\ldots,C_m)$.

Examples: Two examples are given as follows. (1) Let for all $1\leqslant i\leqslant m$ the cone C_i be the cone of positive semidefinite matrices, denoted by $\mathcal{P}(d_i)$. In this case the definition of $(C_1\otimes C_2\otimes\cdots\otimes C_m)$ separability is equivalent to the standard notion of separability of multiparty unnormalized density matrices. We will denote the corresponding cone of separable multiparty unnormalized density matrices as $\mathcal{S}(d_1,d_2,\ldots,d_m)$.

(2) Let for all $1\leqslant i\leqslant m$ the cone C_i be the cone of positive semidefinite matrices with real entries. We call the corresponding cone the cone of real-separable multiparty density matrices and denote it by $\mathcal{S}_{\mathbf{R}}(d_1,d_2,\ldots,d_m)$.

We now recursively define a subspace $\mathcal{L}(d_1,\ldots,d_m)$, which we show is the minimal linear subspace (over the reals) of the symmetric matrices $\Sigma_{\mathbf{R}}(d_1,\ldots,d_m)$ that contains the real-separable cone $\mathcal{S}_{\mathbf{R}}(d_1,\ldots,d_m)$.

Definition 4. $\rho\in\mathcal{L}(d_1,d_2,\ldots,d_m)$ iff in the block partition (3), $\rho^{i,j}\in\mathcal{L}(d_2,\ldots,d_m)$ and $\rho^{i,j}=\rho^{j,i}(1\leqslant i,j\leqslant d_1)$; $\mathcal{L}(d)=\Sigma_{\mathbf{R}}(d)$.

It is easily calculated from this definition that the dimension of $\mathcal{L}$ is

$$\dim[\mathcal{L}(d_1,\ldots,d_m)]=\prod_{i=1}^{m}[d_i(d_i-1)/2], \tag{4}$$

the dimension of the tensor product of the spaces of real-symmetric matrices on each H_i, which in fact will turn out to be $\mathcal{L}$; for $m>1$, this is strictly smaller than the dimension $(\Pi_{i=1}^m d_m)(\Pi_{i=1}^m d_m-1)/2$ of $\Sigma_{\mathbf{R}}(d_1\cdots d_m)$. (This accounts for many differences in the "information-theoretic" behavior of quantum mechanics on real vs complex Hilbert spaces (cf. Ref. [5] for example): it is the mathematical way of saying that the expectation values of local observables (tensor products of real-symmetric matrices) in this theory do not suffice to determine a state on the tensor product of real Hilbert spaces [do not determine the expectation values of *all* observables on this space, i.e., all elements of $\Sigma_{\mathbf{R}}(d_1\cdots d_m)$]. It also implies that the separable (i.e., real-separable) states have zero measure in the space of all states on the tensor product of real Hilbert spaces.)

It is easy to prove that $\rho:H_1\otimes H_2\otimes\cdots\otimes H_m\rightarrow H_1\otimes H_2\otimes\cdots\otimes H_m$ is real separable iff ρ is separable and $\rho\in\mathcal{L}(d_1,d_2,\ldots,d_m)$. In fact, we will show

Proposition 4. $\mathcal{L}(d_1,d_2,\ldots,d_m)$ is the minimal linear subspace (over the reals) of $\Sigma_{\mathbf{R}}(d_1d_2\cdots d_m)$ *which contains* $\mathcal{S}_{\mathbf{R}}(d_1,d_2,\ldots,d_m)$.

Proof. It is clear that $\mathcal{L}(d_1,\ldots,d_m)$ is a subspace of ("$\leqslant$") $\Sigma_{\mathbf{R}}(d_1\cdots d_m)$. To be explicit, symmetry means $\rho(i_1,\ldots,i_m,j_1,\ldots,j_m)=\rho(j_1,\ldots,j_m,i_1,\ldots,i_m)$; this follows from the definition of $\mathcal{L}$ and $\mathcal{L}(d_2,\ldots,d_m)$ being a subspace of $\Sigma_{\mathbf{R}}(d_2,\ldots,d_m)$. This establishes our induction step; the base case $\mathcal{L}(d_m)=\Sigma_{\mathbf{R}}(d_m)$ is part of Definition 4.

Suppose $X\in\mathcal{S}_{\mathbf{R}}(d_1,\ldots,d_m)$. That is, $X=\Sigma_k A_k\otimes B_k$, $A_k\in\mathcal{S}_{\mathbf{R}}(d_1,\ldots,d_{m-1})$, and $B_k\in\Sigma_{\mathbf{R}}(d_m)$. By the induction hypothesis, $A_k\in\mathcal{L}(d_1,\ldots,d_{m-1})$. Block partitioning with respect to the mth system,

$$X^{ij}=\sum_k B_k(i,j)A_k=\sum_k B_k(j,i)A_k=X^{ji}. \tag{5}$$

These blocks are in $\mathcal{L}(d_1\cdots d_{m-1})$ because A_k are consequently $X\in\mathcal{L}(d_1,\ldots,d_m)$. The base case is trivial: $\mathcal{S}_{\mathbf{R}}(d_1)\subseteq[\mathcal{S}_{\mathbf{R}}(d_1)\cap\mathcal{L}(d_1)]$ holds with equality because $\mathcal{S}_{\mathbf{R}}(d_1)\equiv\mathcal{P}(d_1)$ and $\mathcal{L}(d_1)=\Sigma_{\mathbf{R}}(d_1)$.

For the opposite direction, let $X\in\mathcal{L}(d_1,\ldots d_m)\cap\mathcal{S}(d_1,\ldots,d_m)$. By separability,

$$X=\sum_k A_k\otimes B_k\otimes\cdots\otimes Z_k, \tag{6}$$

where $A_k\in\mathcal{P}(d_1)$, $B_k\in\mathcal{P}(d_2),\ldots,Z_k\in\mathcal{P}(d_m)$ (and no restriction to $m=26$ is intended). Let $A_k=A_k^1+iA_k^2$ with A_k^1 real symmetric, A_k^2 real skew symmetric, and similarly for B, C, etc. Substituting these in Eq. (6) and keeping only terms with an even number of imaginary factors (since $X\in\mathcal{L}$), and block partitioning the matrix according to the first subsystem, each block has the form

$$\sum_k A_k^1(i,j)R_k+\sum_k A_k^2(i,j)S_k. \tag{7}$$

Thus $X=X_1+X_2$, where the first term is block symmetric and the second term is block skew symmetric. This second term must therefore be zero. By the recursive definition of $\mathcal{L}$ (and $\mathcal{S}$) we have that, for each fixed value of i,j, X^{ij} must be block symmetric when partitioned according to the second ("B") system. This block is

$$\sum_k A_k^1(i,j)B_k^1(m,n)C^k\otimes\cdots Z^k$$

$$+\sum_k A_k^1(i,j)B_k^2(m,n)C^k\otimes\cdots Z^k \tag{8}$$

and again only the first component is nonzero. Proceeding thus through all the subsystems, all terms with a skew-symmetric factor must be zero and we have

$$X=\sum_k A_k^1\otimes B_k^1\otimes\cdots Z_k^1, \tag{9}$$

with each of $A_k, B_k, \ldots, Z_k$ real symmetric and positive semidefinite, i.e., $X \in \mathcal{S}_{\mathbf{R}}$. That $\mathcal{L}$ is the *minimal* linear subspace of $\Sigma_{\mathbf{R}}$ containing $\mathcal{S}_{\mathbf{R}}$ is clear from the fact that $\mathcal{S}_{\mathbf{R}}$ contains all m-fold tensor products of positive semidefinite real-symmetric matrices, and these span the space of tensor products of real-symmetric matrices, whose dimension, as remarked just after the definition of $\mathcal{L}$, is equal to that of $\mathcal{L}(d_1, \ldots, d_m)$.

An advantage of defining $\mathcal{L}$ as we did above, rather than by the equivalent characterization as the tensor product of the spaces $\Sigma_{\mathbf{R}}(d_i)$ obtained at the end of the preceding proof, is that Definition 4 gives a criterion for membership in $\mathcal{L}$ easily checked on any matrix, while the tensor product characterization just gives us bases for $\mathcal{L}$.

The next lemma gives a simple but very useful criterion for $\mathcal{P}(d_1) \otimes C(d_2)$ separability for any cone $C(d_2)$ of Hermitian matrices. It is a slight generalization of the necessary and sufficient criterion (cf. Refs. [6], [7]) for ordinary $[C(d_2) = \mathcal{P}(d_2)]$ bipartite separability [that every positive linear map, applied to one subsystem of the bipartite system (i.e., to every block of its block density matrix) gives a positive semidefinite matrix].

Definition 5. A linear operator $\phi: M(d_2) \to M(N)$ is called $C(d_2)$ positive if $\phi(C(d_2)) \subset \mathcal{P}(N)$. If X is a block matrix as in Eq. (3), $X^{i,j} \in M(d_2)$, and $\phi: M(d_2) \to M(N)$ is a linear operator, then we define

$$\tilde{\phi}(X) := \begin{pmatrix} \phi(X^{1,1}) & \phi(X^{1,2}) & \ldots & \phi(X^{1,d_1}) \\ \phi(X^{2,1}) & \phi(X^{2,2}) & \ldots & \phi(X^{2,d_1}) \\ \ldots & \ldots & \ldots & \ldots \\ \phi(X^{d_1,1}) & \phi(X^{d_1,2}) & \ldots & \phi(X^{d_1,d_1}) \end{pmatrix}. \tag{10}$$

Lemma 1. Suppose that the cone $C(d_2) \subset \mathcal{H}(d_2) \subset M(d_2)$. Then X is $\mathcal{P}(d_1) \otimes C(d_2)$ separable iff $\tilde{\phi}(X) \geq 0$ (i.e., is positive semidefinite) for all $C(d_2)$-positive linear operators $\phi: M(d_2) \to M(d_1)$.

The proof uses the following proposition, which generalizes the duality between positive linear maps and separable states.

Proposition 5. For Hermitian matrices $M \in \mathcal{B}(d_1, d_2)$, the following are equivalent: (1) $\mathrm{tr}\, MZ \geq 0$ for all $\mathcal{P}(d_1) \otimes C(d_2)$-separable matrices Z and (2) $M^{ij} = \chi(e_i e_j^\dagger)$ for some χ such that $\chi(\mathcal{P}(d_1)) \subseteq C(d_2)^*$.

The proposition is a special case of the following lemma.

Lemma 2. For Hermitian $M \in \mathcal{B}(d_1, d_2)$ the following are equivalent: (1) $\mathrm{tr}\,(MZ) \geq 0$ for all $C(d_1) \otimes C(d_2)$-separable matrices Z and (2) $M^{ij} = \chi(e_i e_j^\dagger)$ for some χ such that $\chi(C(d_1)^T) \subseteq C(d_2)^*$.

By C^T, C a set of matrices, we mean the set of transposes of matrices in C; if C is a cone, so is C^T.

Proof of Lemma 2. Item 1 is equivalent to

$$\mathrm{tr}\,[M(A \otimes B)] \geq 0 \quad \text{for all } A \in C(d_1), \quad B \in C(d_2). \tag{11}$$

By Proposition 3 this is equivalent to

$$\mathrm{tr}\,[\chi(A^T)B] \geq 0 \tag{12}$$

for all $A \in C(d_1)$, $B \in C(d_2)$, i.e., $\chi(C(d_1)^T) \subseteq C(d_2)^*$.

Proof of Lemma 1. "Only if" is trivial: $\mathcal{P}(d_1) \otimes C(d_2)$ separability of X means $X = \Sigma_i A_i \otimes B_i$, with $A_i \in \mathcal{P}(d_1)$, $B_i \in C(d_2)$, hence $\tilde{\phi}(X) = \Sigma_i A_i \otimes \phi(B_i)$; since we assumed $\phi(C(d_2)) \subseteq \mathcal{P}(d_1)$, we have $\phi(B_i) \in \mathcal{P}(d_1)$, so $\tilde{\phi}(X) \in \mathcal{S}(d_1, d_1)$.

For "if," note that $\tilde{\phi}(X) \geq 0$ says that for any positive semidefinite $B \in \mathcal{B}(N, K)$,

$$\sum_{ij} \mathrm{tr}\,[B^{ij} \phi(X^{ij})] \geq 0. \tag{13}$$

By the definition of dual cone [and the self-duality of $\mathcal{P}(d_1)$] it is easily seen that $\phi^\dagger(\mathcal{P}(d_1)) \subseteq C(d_2)^*$. Now, Eq. (13) is equivalent to

$$\sum_{ij} \mathrm{tr}[\,\phi^\dagger(B^{ij}) X^{ij}] = \mathrm{tr}[\,\tilde{\phi}^\dagger(B) X] \geq 0. \tag{14}$$

Letting $B^{ij} = e_i e_j^\dagger$, so B is the block matrix of a positive semidefinite rank-1 state (specifically, the unnormalized maximally entangled state $xx^\dagger$ with $x = \Sigma_i e_i \otimes e_i$), we have that the matrix $\tilde{\phi}^\dagger(B)$ satisfies condition 2 of the Proposition; as ϕ ranges over all $\mathcal{P}(d_1)$-to-$C(d_2)^*$-positive maps, $\tilde{\phi}^\dagger(B)$ ranges over all such matrices so by Proposition 5 X is $\mathcal{P}(d_1) \otimes C(d_2)$ separable.

The next proposition will allow us to extend the (exact) bipartite result from Ref. [3] to multiparty systems. The bipartite result was that everything in the ball $B(N,1) := \{I + \Delta: \|\Delta\|_2 \leq 1\}$ of size 1 in Frobenius norm around the identity operator is separable; therefore, so is everything in the cone, which we call $G(d_1 d_2, 1)$, generated by that ball, for a bipartite system with subsystems of dimensions d_1, d_2. We define a slight generalization of this cone.

Definition 6. Let $G(N,a) \subset \mathcal{H}(N) \subset M(N)$ be the cone generated by Hermitian $N \times N$ matrices of the form $\{I + \Delta: \|\Delta\|_2 := (\mathrm{tr}(\Delta\Delta^\dagger)^{1/2} \leq a\}$.

A sufficient condition for tripartite separability of X is clearly that it belongs to the cone generated by $A_i \otimes Z_i$, where $A_i \in \mathcal{P}(d_1)$ and $Z_i \in G(d_2 d_3, 1)$; this can be used to derive a tripartite sufficient condition for separability in terms of Frobenius norm. Letting this tripartite 2-norm ball generate a cone of separable tripartite states, similar reasoning gives a ball of 4-partite states, and so on. The key to the induction step is the following proposition.

Proposition 6. If $\phi: M(N) \to M(K)$ is a $G(N,a)$-positive linear operator [i.e., $\phi(X) \geq 0$ for all $X \in G(N,a)$] and $\phi(I) = I \in M(K)$, then (1) $\|\phi(X)\|_\infty \leq a^{-1} \|X\|_2$ for all $X \in \mathcal{H}(N)$ and (2) $\|\phi(Y)\|_\infty \leq a^{-1} \sqrt{2} \|Y\|_2$ for all $Y \in M(N)$.

Proof. All $G(N,a)$ positive ϕ satisfy $\phi(I + \Delta) \geq 0$ for all Δ such that $\|\Delta\|_2 \leq a$, which when $\phi(I) = I$ gives $I + \phi(\Delta) \geq 0$; by Proposition 2 this is equivalent to $\|\phi(\Delta)\|_\infty \leq 1$, establishing item 1. Item 2 uses item 1 and the following lemma.

Lemma 3. If a linear operator $\phi: M(N) \to M(K)$ satisfies $\phi(\mathcal{H}(N)) \subseteq \mathcal{H}(K)$ and $\|\phi(Z)\|_\infty \leq \|Z\|_2$ for all Hermitian Z

$\in M(N)$, then $\|\phi(Y)\|_\infty \leq \sqrt{2}\|Y\|_2$ for all $Y \in M(N)$. To show this, let $Y=A+iB$ with A, B Hermitian. Now, $\phi(Y) = \phi(A)+i\phi(B)$, so $\|\phi(Y)\|_\infty \leq \|\phi(A)\|_\infty + \|\phi(B)\|_\infty$. This is less than or equal to $\|A\|_2+\|B\|_2$ by assumption (A, B being Hermitian). The conclusion follows from the square root of the elementary inequality $(x+y)^2 \leq 2(x^2+y^2)$ [obtained from $2xy \leq x^2+y^2$, which comes from $(x-y)^2 \geq 0$].

The following example shows that the extra $\sqrt{2}$ factor (for general vs Hermitian matrices) is the best possible in Lemma 3.

Consider ϕ: $M(2) \to M(2)$, $\phi(X) = X(1,1)A_1 + X(2,2)A_2$; where A_1, A_2 are real-symmetric anticommuting unitary matrices:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Notice that for real a, b we have that $aA_1+bA_2 = (a^2+b^2)^{1/2}U$ for some real-symmetric unitary U. Thus $\phi(\mathcal{H}(2)) \subset \mathcal{H}(2)$ and $\|\phi(Z)\|_\infty \leq \|Z\|_2$ for all Hermitian $Z \in M(2)$. Consider the following (non-Hermitian) matrix:

$$Y = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Then $\|Y\|_2^2 = 2$ and $\|\phi(Y)\|_\infty^2 = \|\phi(Y)\|_2^2 = 4$, since $\mathrm{Det}[\phi(Y)] = 0$.

Remark. If we add to the premises of Lemma 3 the additional assumption that we used to obtain Proposition 6 from Lemma 3, namely, that $\phi(I)=I$, we can obtain a contraction bound (when $k \geq 2$) of $\sqrt{2-1/n}$ instead of $\sqrt{2}$, as well as an example showing that $\sqrt{2-2/n}$ can be achieved. Proposition 2 of Ref. [3] is a similar contraction bound with constant 1 rather than $\sqrt{2}$ on all matrices, not just Hermitian ones, for the usual positive maps; the proofs used there do not work for the different notion of positivity used here.

Now everything is ready for our attack on multipartite separability.

Theorem 1. Let H_1, H_2 have dimensions n_1, n_2. If an unnormalized density matrix ρ: $H_1 \otimes H_2 \to H_1 \otimes H_2$ satisfies the inequality $\|\rho - I\|_2 \leq a/\sqrt{2}$, then it is $\mathcal{P}(n_1) \otimes G(n_2,a)$ separable.

Proof. Let $\rho = I+\Delta$, Δ Hermitian; by Lemma 1, we are looking for a bound on $\|\Delta\|_2$ that ensures, for any $G(n_2,a)$-to-$\mathcal{P}(n_1)$-positive linear operator, $\tilde{\phi}(I+\Delta) \geq 0$. $\phi(I)=I$, so $\tilde{\phi}(I+\Delta) = I + \tilde{\phi}(\Delta)$; $\|\tilde{\phi}(\Delta)\|_\infty \leq 1$ will ensure this (cf. Proposition 2). The argument establishing that $\|\tilde{\phi}(\Delta)\|_\infty \leq 1$ is essentially identical to the proof of the main theorem of Ref. [3], except that because ϕ is not an ordinary positive map we must use the weaker contraction bound of Proposition 6, with its $\sqrt{2}$ factor, in place of the result of Ref. [3] with factor 1:

$$\|\tilde{\phi}(\Delta)\|_\infty^2 \leq \|A\|_\infty^2 \leq \|A\|_2^2 = \sum_{ij} a_{ij}^2 = \sum_{ij} \|\phi(\Delta^{ij})\|_\infty^2, \tag{15}$$

where $A := [a_{ij}]$, $a_{ij} := \|\phi(\Delta^{ij})\|_\infty$. (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, a known result whose proof is sketched in, e.g., Ref. [3], and the second is because the Frobenius norm is an upper bound to the operator norm.) $\|\phi(\Delta^{ij})\|_\infty^2 \leq 2a^{-2}\|\Delta^{ij}\|_\infty^2$ by Proposition 6, and it is an elementary norm inequality that $\|\Delta^{ij}\|_\infty \leq \|\Delta^{ij}\|_2$. So

$$\|\tilde{\phi}(\Delta)\|_\infty^2 \leq \sum_{ij} \|\phi(\Delta^{ij})\|_\infty^2 \leq 2a^{-2} \sum_{ij} \|\Delta^{ij}\|_2^2 \equiv 2a^{-2}\|\Delta\|_2^2. \tag{16}$$

Thus if $\|\Delta\|_2 \leq a/\sqrt{2}$, $\|\tilde{\phi}(\Delta)\|_\infty \leq 1$.

Corollary 1. If an m-partite unnormalized density matrix ρ: $H_1 \otimes \cdots \otimes H_m \to H_1 \otimes \cdots \otimes H_m$ satisifes $\|\rho - I\|_2 \leq 1/(2^{m/2-1})$, then it is separable.

Proof. The main result of Ref. [3] is that $G(d_1 d_2, 1) \subset \mathcal{S}(d_1, d_2)$. This is the base case for an induction on the number of subsystems. For the induction step, fix $m>2$ and suppose as our induction hypothesis the corollary holds for $m-1$, i.e., $G(d_1,\ldots,d_{m-1},2^{-[(m-1)/2-1]}) \subseteq \mathcal{S}(d_1,\ldots,d_{m-1})$. Theorem 1 tells us $G(d_1,\ldots,d_m,2^{-[(m-1)/2-1]}/\sqrt{2} \equiv 2^{-(m/2-1)})$ is $\mathcal{P}(d_m) \otimes G(d_1 \cdots d_{m-1}, 2^{-[(m-1)/2-1]})$ separable, and therefore (by the induction hypothesis and the recursive definition of separability) separable.

If we had an analog to Theorem 1, with $G(n_1,a)$ instead of $\mathcal{P}(n_1)$, and some constant α replacing $1/\sqrt{2}$, then we could get one over a polynomial instead of an exponential in Corollary 1, by recursively dividing systems into subsystems of more or less equal size, since this involves a logarithmic number of partitionings compared to splitting off one system at a time. The first step toward such a theorem would be to apply the characterization of $C(d_1) \otimes C(d_2)$ separability given by Lemma 2 to $G(d_1,a)$, $G(d_2,a)$; the fact that neither of these cones is self-dual has so far proved an obstacle to our getting useful results along these lines.

Note that for tripartite separability, this corollary gives a ball of radius $1/\sqrt{2}$. Even here, it is an interesting open question whether this is tight; in fact, any example showing that the radius of a maximal separable 2-norm ball is smaller than 1 would be very interesting.

Theorem 2. Consider $\rho \in \mathcal{L}(d_1,\ldots,d_m)$. If $\|\rho - I\|_2 \leq 1$, then

$$\rho = \sum a_i \rho^{(i)} \otimes \rho_i, a_i \geq 0, \tag{17}$$

where for all i $\rho_1^{(i)}$ is a real positive semidefinite $d_1 \times d_1$ matrix, $\rho_i \in \mathcal{L}(d_2,\ldots,d_m)$ and $\|I - \rho_i\|_2 \leq 1$.

Proof. The proof goes essentially like that of Theorem 1 except that the blocks Δ^{ij} are Hermitian by Proposition 4.

Consequently we may use item 2 rather than item 1 of Proposition 6, and obtain the larger radius ball.

Corollary 2. If $\rho \in \mathcal{L}(d_1,\ldots,d_m)$ and $\|\rho - I\|_2 \leq 1$, then ρ is real separable. In other words the maximal separable ball in $\mathcal{L}(d_1,\ldots,d_m)$ around the identity I has radius 1.

The next proposition is immediate from results of Ref. [3], derived using ''scaling,'' i.e., considering all ways of writing a matrix ρ as a positive scalar times the sum of the identity and a Hermitian perturbation, and minimizing the 2-norm of the perturbation.

Proposition 7. Define $\mu(\rho)$ as the maximum of $\|\Delta\|_2$ over all Δ such that there exists an $\alpha > 0$ for which $\rho = \alpha(I + \Delta)$. Let ρ be a normalized ($\mathrm{tr}\,\rho = 1$) density matrix. Then the following three statements are equivalent: (1) $\mu(\rho) \leq a$, (2) $\mathrm{tr}\,\rho^2 \leq 1/(d - a^2)$, and (3) $\|\rho - I/d\|_2 \leq a/\sqrt{d(d-a^2)}$.

Using this Proposition, Theorem 1 has (via Corollary 1) the following corollary.

Corollary 3. If an m partite normalized (i.e., unit trace) density matrix $\rho: H_1 \otimes \cdots \otimes H_m \to H_1 \otimes \cdots \otimes H_m$ satisfies $\|\rho - I/d\|_2 \leq 1/2^{m/2-1} d$, where $d = \dim(H_1 \otimes \cdots \otimes H_m)$, then it is separable.

[The proposition actually gives the (negligibly) tighter statement with $2^{m/2-1}\sqrt{d(d-2^{-(m-2)})}$ in the denominator.]

IV. DISCUSSION

In many interesting experimental or theoretical situations, the system is in a pseudopure state: a mixture of the uniform density matrix with some pure state π:

$$\rho_{\epsilon,\pi} := \epsilon\pi + (1-\epsilon)I/d, \tag{19}$$

where $d = d_1 \times d_2 \times \cdots \times d_m$ is the total dimension of the system. For example, consider NMRQIP, where $d_i = 2$ for $i = 1, \ldots, m$, $d = 2^m$, and m is the number of spins individually addressed in the molecule being used. As discussed in more detail below, the initialization procedures standard in most NMRQIP implementations prepare pseudopure states.

Write

$$\rho_{\epsilon,\pi} = (1/d)I + \epsilon(\pi - I/d). \tag{20}$$

Since $\|\epsilon(\pi - I/d)\|_2 = \epsilon\sqrt{(d-1)/d}$, by Corollary 3, this is separable if

$$\epsilon \leq 2^{-(m/2-1)}/\sqrt{d(d-1)}, \tag{21}$$

For m D-dimensional systems (so $d = D^m$), this implies the (negligibly loosened) bound

$$\epsilon \leq 2^{-(m/2-1)}/D^m. \tag{22}$$

This is an exponential improvement over the result in Ref. [2] (the qubit case is in Ref. [1]) of $\epsilon \leq 1/(1 + D^{2m-1})$. For m qubits, for example, our result goes asymptotically as $2^{-[(3/2)m-1]}$, vs $2^{-(2m-1)}$ in Ref. [1]. Another comparison is with our earlier bound of

$$\epsilon \leq 1/(D^m - 1) \tag{23}$$

guaranteeing separability for m D-dimensional systems with respect to every bipartition [3]. It is interesting that this is exponentially larger than the present bound guaranteeing multipartite separability, although we do not know that a tight multipartite bound would still exhibit this exponential separation.

In liquid-state NMR at high temperature T, the sample is placed in a high dc magnetic field. Each spin is in a highly mixed thermal state. It is not maximally mixed because of the energy splitting between the higher-energy state in which the spin is aligned with the magnetic field and the higher-energy one in which it is antialigned. This gives probabilities for those states that are proportional to the Boltzmann factors $e^{\pm\beta\mu B}$, where $\beta \equiv 1/kT$ with k Boltzmann's constant, μ the magnetic moment of the nuclear spin, and B the external field strength. For realistic high-T liquid NMR values of $T = 300$ K, $B = 11$ T, $\beta\mu B \approx 3.746 \times 10^{-5} \ll 1$. Calling this η, $e^{\pm\eta} \approx 1 \pm \eta$, so the probabilities are $p_\uparrow \approx (1-\eta)/2$, $p_\downarrow \approx (1+\eta)/2$, where $\uparrow/\downarrow$ denote alignment/antialignment of the spin with the field. With independent, distinguishable nuclear spins, Maxwell-Boltzmann statistics give the highest-probability pure state, with all m spins up (field-aligned), probability about $(1+\eta)^m/2^m \approx (1+m\eta)/2^m$. Standard pseudopure-state preparation creates a mixture of this state and the maximally mixed state by applying a randomly chosen unitary from the group of unitaries fixing the all-spin-aligned state. [U could be chosen uniformly (i.e., with Haar measure on this group), but efficient randomization procedures may draw from carefully chosen finite sets of such unitaries [8].] Thus, we get a mixture

$$(1-\epsilon)I/2^m + \epsilon|\uparrow\cdots\uparrow\rangle\langle\uparrow\cdots\uparrow|, \tag{24}$$

with

$$\epsilon = \eta m/2^m. \tag{25}$$

With $\eta \approx 3.746 \times 10^{-5}$, this implies that below about 23 qubits, NMR pseudopure states are all separable compared to the $\approx$13 qubits one gets from the bound in Ref. [1].

A quantum computation in which the computer state remains *pure* and unentangled can be efficiently (polynomially) simulated on a classical computer [9]. Whether quantum computations involving only general, potentially mixed, separable states are efficiently classically simulable, and whether they are capable of the same performance as universal quantum computation, or at least of some speedups over classical computation, are open questions. Our results, of course, do not directly address this question. On the basis of a suspicion that entangled states are required for such speedup, doubt is sometimes cast on the usefulness of NMR-based quantum-information-processing protocols that do not, even asymptotically, achieve entanglement. Even without entanglement considerations, however, it is clear that pseudopure-state NMR quantum computing will not give asymptotic gains over classical computing because of the exponentially decreasing signal-to-noise ratio from Eq. (25). As pointed out in Ref. [10], it does not follow that no application of liquid-state NMR can have better-than-classical

asymptotic performance: NMRQIP is not limited to pseudopure-state initialization. It is not known that NMRQIP with other initialization schemes, such as those that involve preparing a *fixed* number of pseudopure qubits as the total number of spin qubits grows, can be efficiently classically simulated, and even with one pure qubit interesting things can be efficiently done for which no efficient classical algorithm is currently known [10]. Another nonpseudopure initialization scheme is the Schulman-Vazirani algorithmic cooling procedure [11], which essentially uses an efficient (and NMR implementable) compression algorithm to convert the thermal state with S bits of entropy for m nuclear spins, into $\log_2 S$ maximally mixed qubits and $m-\log_2 S$ pure ones. Their work shows that the theoretical model derived from NMR with an initial thermal state is as powerful as standard quantum computation. Though the overhead required is polynomial, the space overhead is large enough to be impractical, given the small number of qubits available in liquid-state NMR. But algorithmic cooling is certainly relevant in principle to the asymptotic power of an implementation, and could be practically relevant to a high-temperature bulk QIP implementation that was expected to be sufficiently scalable that asymptotic considerations are relevant.

However, there is still the interesting possibility that one may produce an entangled overall density matrix (and not just a mixture of the maximally mixed state with an entangled state) via pseudopure-state NMRQIP. The results herein increase (to 23, with η as above) the number of qubits known to be required before this may be possible. Since we have not shown that our bounds are tight, even at 23 qubits there is no guarantee one can prepare an entangled pseudopure state. By contrast, from Eqs. (23) and (25) one needs $m=1/\eta$ qubits (about 26,700 for our η) to have any hope of obtaining a pseudopure state that is not bipartite separable with respect to partitions of the qubits into two sets. Again, we remind the reader that nonpseudopure protocols could conceivably give such a ''biseparable'' state with far fewer qubits; in the Appendix we discuss some implications of our results for this possibility.

In conclusion, we have derived an upper bound, exponentially better than those already known, on the Frobenius-norm radius of a ball of separable matrices around the identity matrix. The bound has implications for the minimum polarization needed for bulk quantum-information-processing protocols initialized by preparing pseudopure states from a thermal state via averaging, to produce entanglement: known lower bounds on this minimal polarization are exponentially increased by our results. We stress, however, that this is just one application of a general, computationally simple sufficient criterion for multipartite entanglement, applicable to states of any form. Its geometric nature should make it useful in many applications, both theoretical and practical. The question of whether this bound is tight, or whether there is a larger separable Frobenius-norm ball around the identity, remains open.

ACKNOWLEDGMENTS

We thank Manny Knill and Isaac Chuang for discussions and the U.S. DOE and NSA for financial support.

APPENDIX: ENTANGLEMENT AND THERMAL INITIAL STATES IN NMR

Schulman and Vazirani's algorithmic cooling protocol [11] shows that it is, in theory, possible to prepare any entangled state from sufficiently many thermal NMR qubits. The question of just how many qubits are required by means possibly simpler than algorithmic cooling is also of interest. One can gain some information about this using our results, by applying Corollary 3 to the initial thermal density matrix of an NMR system. This matrix, which is approximately

$$\begin{pmatrix} \frac{1+\eta}{2} & 0 \\ 0 & \frac{1-\eta}{2} \end{pmatrix}^{\otimes n} \tag{A1}$$

(with each qubit expressed in the $|\uparrow\rangle$, $|\downarrow\rangle$ basis), has

$$\|\rho - I/d\|_2^2 = \frac{(1+\eta^2)^m - 1}{2^m} \approx m\,\eta^2/2^m. \tag{A2}$$

This should be compared to the separability condition of Corollary 3, which guarantees separability if this squared distance is below $2^{-(3m-2)}$. The comparison gives that for m qubits, the thermal state (and any state reachable from it by unitary transformation) is separable if

$$\eta \leqslant m^{-1/2} 2^{m-1}. \tag{A3}$$

For the same experimental conditions considered above, 14 qubits are required before this bound is exceeded (rather than the 23 for the pseudopure state prepared from this thermal state).

If one wants the possibility of bipartite entanglement with respect to some partition of the qubits into two sets, it is necessary to beat the bound [closely related to Eq. (23)]

$$\|\rho - I/d\|_2^2 \leqslant \frac{1}{d(d-1)}. \tag{A4}$$

For the thermal state, this gives $\eta \leqslant m^{-1/2} 2^{-m/2}$. With $\eta = 3.746 \times 10^{-5}$ as before, the bound is not surpassed until 25 qubits. Although this comes from an essentially tight bound, that does not imply that entanglement can be achieved through computation starting with this initial state. Although the thermal state has the same magnitude perturbation as some entangled state, the latter will have different eigenvalues, so unitary manipulation will not get us there, and it is an interesting question what we can achieve along these lines using NMR-implementable nonunitary manipulations (which may sometimes require extra thermal ancilla bits that should be counted as resources). To understand when *unitary* manipulations might be guaranteed to give us entanglement, a promising approach is to look for conditions on the spectrum of a matrix sufficient for an entangled state with that spectrum to exist. We conjecture that the problem of determining, from a spectrum, whether or not an entangled state with that spectrum exists is NP (nondeterministic polynomial) -hard in

terms of an appropriate measure of problem size; this does not rule out easier-to-evaluate sufficient conditions, perhaps obtained from relaxations of the above problem. Theorem 4 of Ref. [3] gives some information on spectra sufficient to guarantee entanglement.

For the pseudopure fraction ϵ there is an *upper* bound of $2/(2+2^m)$ from Ref. [3] nearly matching the lower bound (23). Comparison to the expression $\epsilon=\eta m/2^m$ for pseudopure polarization suggests that, at some large number of qubits $m \geqslant 2/\eta$, even pseudopure protocols will exceed this bound. With $\eta=3.746\times10^{-5}$ this gives about 53 400 qubits. This is far beyond the range generally viewed as relevant for liquid-state NMR, and improved polarization is unlikely to bring it into this range. Since the state demonstrating entanglement at the upper bound is not in general pseudopure, exceeding this bound is still no guarantee we can get entanglement. Also, this is well in the range where algorithmic cooling could produce much stronger entanglement. Still, one can imagine that in other bulk QIP implementations the balance between the difficulty of implementing complex unitaries (relatively easy in NMR) and the difficulty of preparing large numbers of thermal qubits (apparently relatively hard in NMR) could be different, and entanglement generation by simple manipulations on thermal states, perhaps even by pseudopure-state preparation, might be promising.

[1] S. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
[2] 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. Walls, R. Glauber, M. Scully, and H. Carmichael (Springer, New York, 2001); see also e-print quant-ph/0001075.
[3] L. Gurvits and H. Barnum, Phys. Rev. A **66**, 062311 (2002).
[4] C. M. Caves, C. A. Fuchs, and P. Rungta, Found. Phys. Lett. **14**, 199 (2001).
[5] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. **43**, 4537 (2002).
[6] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[8] E. Knill, I. Chuang, and R. Laflamme, Phys. Rev. A **57**, 3348 (1998).
[9] R. Jozsa and N. Linden, e-print quant-ph/0201143.
[10] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[11] L. J. Schulman and U. Vazirani, in *Proceedings of the 31st Annual ACM Symposium on the Theory of Computing (STOC)* (ACM Press, New York, 1999), pp. 322–329, earlier version is e-print quant-ph/9804060.