Separability and Fourier representations of density matrices

Arthur O. Pittenger[1,*] and Morton H. Rubin[2]
[1]*Department of Mathematics and Statistics, University of Maryland, Baltimore County, Baltimore, Maryland 21228-5398*
[2]*Department of Physics, University of Maryland, Baltimore County, Baltimore, Maryland 21228-5398*
(Received 7 January 2000; revised manuscript received 16 March 2000; published 18 August 2000)

Using the finite Fourier transform, we introduce a generalization of Pauli-spin matrices for d-dimensional spaces, and the resulting set of unitary matrices $S(d)$ is a basis for $d\times d$ matrices. If $N=d_1\times d_2\times\cdots\times d_b$ and $H^{[N]}=\otimes H^{[d_k]}$, we give a sufficient condition for separability of a density matrix ρ relative to the $H^{[d_k]}$ in terms of the L_1 norm of the spin coefficients of ρ. Since the spin representation depends on the form of the tensor product, the theory applies to both full and partial separability on a given space $H^{[N]}$. It follows from this result that for a prescribed form of separability, there is always a neighborhood of the normalized identity in which every density matrix is separable. We also show that for every prime p and $n>1$, the generalized Werner density matrix $W^{[p^n]}(s)$ is fully separable if and only if $s\leqslant(1+p^{n-1})^{-1}$.

PACS number(s): 03.67.Lx, 03.67.Hk, 03.65.Ca

I. INTRODUCTION

One of the predictions of quantum mechanics is that spatially separated components of a system can be entangled. The consequent prediction of nonclassical correlations among the separated components of a quantum system has led to critiques of the foundations of quantum mechanics, as in the famous Einstein, Podolsky, Rosen paper [1], and to experiments that have confirmed the predicted nonclassical correlations, as in [2]. Interest in entangled systems has been heightened by proposed applications in quantum computation, for example [3], and in quantum communication, as exemplified most dramatically by teleportation [4]. As a result, there have been many publications that have examined various aspects of entanglement, its measurement, and its use in quantum communication, such as Refs. [5–9], to mention only a few recent papers.

In this paper we shall be interested in the separability properties of quantum systems in states defined on finite-dimensional Hilbert spaces $H=H_1\otimes\cdots\otimes H_n$, where the H_k denote the Hilbert spaces of the subsystems. A state specified by a density matrix ρ is said to be fully separable on H if it is a convex combination of tensor products:

$$\rho=\sum_a p(a)\rho^{(1)}(a)\otimes\cdots\otimes\rho^{(n)}(a), \tag{1}$$

where $\rho^{(k)}(a)$ is a density matrix on H_k. Since the same ρ can have different convex representations, it has proven difficult to determine generally applicable operational conditions for separability, and determining such conditions is one of the motivations for this paper. It is also possible to have different types of separability by allowing sets of the subsystems to be entangled, cf. [9,10], and one can describe a lattice of levels of separability. The theory we develop here applies to all of these various definitions of separability.

A necessary condition for separability is that the partial transpose ρ^{T_r} of a state ρ should be a state [11]. If we represent ρ as a matrix, this means that if $\rho=(\rho_{j_1\ldots j_n,k_1\ldots k_n},)$ then (taking $r=1$)

$$\rho^{T_1}=(\rho_{k_1j_2\ldots j_n,j_1k_2\ldots k_n},) \tag{2}$$

is also a density matrix. It is easy to confirm that if a density matrix is separable, its partial transposes are also separable, but it has been shown [12] that the converse is true only in the $2\otimes2$ and $2\otimes3$ cases. In the proof of this last result [12], a necessary and sufficient criterion for separability was established, but there seems to be no operational way of using this criterion as a general tool. Other studies of separability, such as those in [9,13–17], have found operationally useful necessary conditions and sufficient conditions for classes of densities or for special cases, but no general sufficient conditions with a breadth of applicability analogous to that of the Peres condition.

Broadly speaking, necessary conditions tend to be described in the computational basis, while sufficient conditions for two-level systems tend to be described in terms of the Pauli spin basis. That observation motivated the derivation of a change-of-basis formula in [18] that facilitates the strategy of checking whether necessary conditions derived in the computational basis are sufficient by using the (real) Pauli spin basis. This approach leads to general sufficient conditions for full separability, which essentially give the condition in [14] as a corollary, and also leads to necessary and sufficient conditions for full separability of a parametrized family of n-qubit densities that all satisfy the Peres condition. The difficulty with extending this approach to d-level systems is that the generally accepted definition of spin matrices as generators of rotations does not capture the computationally useful features of the Pauli matrices when $d\geqslant3$. One of the basic purposes of this paper is to propose a general definition of d-level spin matrices that possess many of those computational properties.

The Pauli matrices are special in that they are both Hermitian and unitary, and together with the identity matrix σ_0

*Present address: The Center for Quantum Computation, Clarendon Laboratory, Oxford University, Oxford, U.K.

they form a basis of the set of 2×2 matrices. Our strategy is to generalize the role of the Pauli matrices as a basis of unitary matrices at the expense of Hermiticity. We show the applicability of these proposed d-level spin matrices and in the Appendix examine the $d=3$ case in some detail, identifying properties analogous to those of the Pauli matrices. We also define directly a general characterization of certain classes of trace one projections of d-level systems. We use those projections to establish necessary and sufficient conditions for full separability of generalized Werner densities composed of any number n of d-dimensional subsystems for any prime d. In addition, we establish a general sufficient condition for full or partial separability of densities of any dimension. Analogous results for full separability were obtained in [18] for $d=2$ by essentially the same methodology.

Other authors [19] have used a different set of operators in the $d=3$ case, and some separability results were obtained recently in [15]. Our proposed class is different, and we show that stronger separability results can be obtained using these matrices and the strategy developed in [18].

II. A NECESSARY CONDITION

As mentioned above, the Peres partial transpose condition is a general necessary condition for separability [11]. In [18], a weaker but useful condition was derived using the Cauchy-Schwarz inequality. That result is generalized in Appendix A to give the following result. For each r, let (u_r,v_r) be either (j_r,k_r) or (k_r,j_r). Then for fully separable states ρ

$$(\sqrt{\rho_{j,j}}\sqrt{\rho_{k,k}})\geqslant|\rho_{u,v}|, \tag{3}$$

where ρ is written as a matrix in the computational basis defined by the tensor products of $|j_i\rangle\langle k_i|, 1\leqslant i\leqslant n$. As an application, consider the following generalization of the Werner density matrix [20] on the $N=d^n$ dimensional Hilbert space $H^{[N]}$:

$$W^{[N]}(s)=\frac{1-s}{d^n}I+s\tau$$

where I is the identity and τ is the projection defined by the state

$$|\psi^{[N]}\rangle=\frac{1}{\sqrt{d}}[|0\ldots0\rangle+|1\ldots1\rangle + \ldots+|(d-1)\ldots(d-1)\rangle]. \tag{4}$$

(In the sequel we let $\tilde{k}$ denote the repeated index $k\ldots k$.) In the computational basis $W^{[N]}_{j,j}(s)$ equals

$$\left(\frac{1-s}{d^n}+\frac{s}{d}\right)$$

when j is in $\{\tilde{k}:0\leqslant k<d\}$ and equals $(1-s)/d^n$ otherwise. The only nonzero off-diagonal elements are $W^{[N]}_{\tilde{j},\tilde{k}}(s)=(s/d)$. Choosing j and k appropriately in Eq. (3), we have the necessary condition $1\geqslant s(1+d^{n-1})$. To show that this condition is also sufficient, we will use the spin representation to prove $W^{[N]}(s)$ is fully separable when d is prime and $s=(1+d^{n-1})^{-1}$. In order to do that, however, we first need to define the spin representation.

III. COMPUTATIONAL AND SPIN BASES

Let $H^{[N]}$ denote an N-dimensional Hilbert space where $N=d_1\times d_2\times\cdots\times d_b$. In this section we define different bases for $N\times N$ matrices on $H^{[N]}$ based on different representations of $H^{[N]}$ as a tensor product space, and the discussion is purely mathematical. In the applications, we will be concerned with a specific representation $H^{[N]}=\otimes_{a=1}^{b}H^{[d_a]}$ and with the corresponding separability properties of densities on $H^{[N]}$. The bases used will depend on the order of the tensor product as will the representation of a density matrix as $\rho=\rho_1\otimes\cdots\otimes\rho_b$, the tensor product of densities ρ_k on the $H^{[d_k]}$. For example, we might want to examine separability of a density matrix on $H^{[90]}=H^{[6]}\otimes H^{[15]}$ using matrices consistent with that tensor product. In a subsequent application one might want $H^{[6]}$ to represent the tensor product of spin-$\frac{1}{2}$ and spin-1 particles, i.e., a tensor product of $H^{[2]}$ and $H^{[3]}$, and the order of the subtensor product should not affect the theory. We shall need the result that permuting the order of a tensor product corresponds to a conjugation operation and thus that the theory is generally applicable with only notational changes for particular applications. For completeness, we state this as a lemma.

Lemma 1. Let $N=d_1\times d_2\times\cdots\times d_b$ and suppose M is an $N\times N$ matrix with $M=C^{(1)}\otimes\cdots\otimes C^{(b)}$, where the $C^{(k)}$ are $d_k\times d_k$ matrices. Given a permutation of $\{1,\ldots,b\}$, denoted by σ, there is a matrix Q_σ such that $Q_\sigma M_\sigma Q_\sigma^{-1}=M$ for all such $C^{(k)}$'s where $M_\sigma=C^{[\sigma(1)]}\otimes\cdots\otimes C^{[\sigma(b)]}$.

The motivation for this work comes from noticing the role of the 2×2 Hadamard matrix in working with density matrices for two-level systems. In the computational basis defined by the matrices $E_{j,k}=|j\rangle\langle k|$, $\rho=\Sigma_{j,k}\rho_{j,k}E_{j,k}$, while in the spin basis ρ is expressed in terms of the Pauli matrices, $\rho=\frac{1}{2}(\sigma_0+\sigma_m)$, where $\sigma_m=\Sigma m_j\sigma_j$ and $\sigma_1=\sigma_x$, $\sigma_2=\sigma_y$, and $\sigma_3=\sigma_z$. We can relate these two operator bases using the 2×2 Hadamard matrix,

$$\begin{pmatrix}\sigma_0 & \sigma_1\\ \sigma_3 & i\sigma_2\end{pmatrix}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}E_{0,0} & E_{0,1}\\ E_{1,1} & E_{1,0}\end{pmatrix}. \tag{5}$$

An interpretation of Eq. (5) is suggested by the usage in quantum computing. The Pauli matrices related to phase changes σ_0 and σ_3 are the Hadamard transforms of the projections $E_{0,0}$ and $E_{1,1}$, while the matrices σ_1 and $i\sigma_2$ related to state changes are the Hadamard transforms of the raising and lowering operators $E_{0,1}$ and $E_{1,0}$. That being the case, one could then regard Eq. (5) as defining the real Pauli matrices as Hadamard transforms of the corresponding computational basis matrices. The Hadamard matrix also connects the coefficients in the two bases if we rearrange the matrix elements of the density matrix in a nonstandard way:

$$\begin{pmatrix} 1 & m_1 \\ m_3 & -im_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{11} & \rho_{10} \end{pmatrix}. \tag{6}$$

Note that a systematic application of these ideas requires both the use of the real Pauli matrices and a reindexing of both the Pauli matrices and the computational basis matrices to conform to the observed connection.

Since the Hadamard matrix is the 2×2 Fourier transform, we can extend this interpretation of Eq. (5) to *d*-level systems by using the corresponding discrete Fourier transform. Define the *adjusted* basis $A=\{A_{j,k},0\leqslant j,k<d\}$ as the set of $d\times d$ matrices defined by $A_{j,k}=E_{j,j+k}$, where + denotes addition modulo *d*, and *define* the ''spin'' matrices $S=\{S_{j,k},0\leqslant j,k<d\}$ using the analogue of Eq. (5) and the finite Fourier transform. Thus $(S)\equiv F(A)$ where $F(j,k)=\exp(2\pi ijk/d)=\eta^{jk}$ with $\eta=\exp(2\pi i/d)$. (We will make the dependence on *d* explicit below.) In detail,

$$S_{j,k}=\sum_{r=0}^{d-1} F(j,r)A_{r,k} \tag{7}$$

is a sum of products of scalars times matrices. Since *F* is invertible, it follows that *S* is also a basis for the $d\times d$ matrices. Note that Eq. (5) is a special case of Eq. (7) with $d=2$ and $\eta=-1$.

To illustrate these ideas, it is useful to write out the results for $d=3$ in detail. Then $\eta=\exp(2\pi i/3)$ and

$$S_{00}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} S_{01}=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} S_{02}=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$S_{10}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \eta & 0 \\ 0 & 0 & \eta^2 \end{pmatrix} S_{11}=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \eta \\ \eta^2 & 0 & 0 \end{pmatrix} S_{12}=\begin{pmatrix} 0 & 0 & 1 \\ \eta & 0 & 0 \\ 0 & \eta^2 & 0 \end{pmatrix}$$

$$S_{20}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \eta^2 & 0 \\ 0 & 0 & \eta \end{pmatrix} S_{21}=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \eta^2 \\ \eta & 0 & 0 \end{pmatrix} S_{22}=\begin{pmatrix} 0 & 0 & 1 \\ \eta^2 & 0 & 0 \\ 0 & \eta & 0 \end{pmatrix}.$$

The spin matrices *S* not only form a basis for $d\times d$ matrices, but share many other properties with the real Pauli matrices, which we record next. We should note that the matrices $S_{j,k}$ were also defined in an earlier work by Fivel [21] on Hamiltonians on discrete spaces, and many of the properties listed below were first established there.

Proposition 1. Fix $d\geqslant 2$ and let *S* denote the corresponding set of spin matrices.

(i) *S* is an orthogonal basis of unitary matrices with respect to the trace inner product.

(ii) If *d* is odd, each matrix in *S* is in SU(*d*), while if *d* is even, $S_{j,k}$ is in SU(*d*) if and only if $j+k$ is even.

(iii) $S_{j,k}=(S_{1,0})^j(S_{0,1})^k$, $(S_{j,k})^\dagger=\eta^{jk}S_{d-j,d-k}=(S_{j,k})^{d-1}$ and $[S_{j,k},S_{r,s}]=(\eta^{kr}-\eta^{js})S_{j+r,k+s}$ using addition mod*d*.

(iv) $\mathrm{tr}(S_{j,k})=0$ for all $(j,k)\neq(0,0)$.

Proof. The key observation, noted in [21], is that the matrices are generated by $S_{1,0}$ and $S_{0,1}$: $S_{j,k}=(S_{1,0})^j(S_{0,1})^k$ with $S_{0,1}S_{1,0}=\eta S_{1,1}$. All of the remaining assertions, including orthogonality, follow from those relations and from easy computations. A useful consequence of the manipulations is

$$(S_{j,k})^m=\eta^{(jk)m(m-1)/2}S_{mj,mk}. \tag{8}$$

Unlike the Pauli matrices, these spin matrices need not be Hermitian; for example, when $d=3$ only the identity matrix is Hermitian. Thus when computing the coefficients of a density matrix in these bases, as we do next, the Hermitian conjugation notation has to be retained. Note that the assertion (iii) in Corollary 1 corresponds to the usual inequality relating the L_2 magnitude of a Fourier transform and the L_2 magnitiude of the original function.

Corollary 1. (i) The matrix elements of a $d\times d$ density matrix ρ in the different bases are related by $(s)=F^*(a)$.

(ii) $s_{0,0}=1$, $s_{d-j,d-k}=\eta^{jk}s^*_{j,k}$ and $(1/d)(Fs)_{j,0}=\rho_{j,j}\geqslant 0$.

(iii) $\Sigma_{j,k}|s_{j,k}|^2=d\Sigma|\rho_{j,k}|^2$ and $\sqrt{\Sigma_{j,k}|s_{j,k}|^2}\sqrt{\Sigma_{j,k}|\rho_{j,k}|^2}\geqslant 1/\sqrt{d}$.

(iv) $|s_{j,k}|\leqslant 1$.

Proof. We expand an arbitrary density matrix in the two bases:

$$\rho=\sum_{j,k} a_{j,k}A_{j,k}=\frac{1}{d}\sum_{j,k} s_{j,k}S_{j,k},$$

where $a_{j,k}=\mathrm{Tr}(A^\dagger_{j,k}\rho)$ gives $a_{j,k}=\rho_{j,j+k}$, using addition mod*d*, and $s_{j,k}=\mathrm{Tr}(S^\dagger_{j,k}\rho)$. Then from Eq. (7), $s_{j,k}=\Sigma_{r=0}^{d-1}F^*(j,r)a_{r,k}$, which proves (i). Note that we have to include a complex conjugation in the formula, which is unnecessary in the $d=2$ case, since the Hadamard matrix has real entries. The assertions in (ii) follow from the definitions and from the fact that ρ is Hermitian with trace equal to one. The relations in (iii) follow from $\mathrm{Tr}((s)^\dagger(s))=\mathrm{Tr}((a)^\dagger(F^*)^\dagger(F^*)(a))=d\,\mathrm{Tr}((a)^\dagger(a))=d\,\mathrm{Tr}(\rho^2)$, and from $\mathrm{Tr}(\rho^2)=\Sigma_k\lambda_k^2\geqslant\Sigma_k 1/d^2=1/d$, where the λ_k are the non-negative eigenvalues of the density ρ. Finally, (iv) follows from $|s_{j,k}|^2=|\mathrm{Tr}(\rho^{1/2}S^\dagger_{j,k}\rho^{1/2})|^2\leqslant\mathrm{Tr}(\rho)Tr(S_{j,k}S^\dagger_{j,k}\rho)=1$.

Now let $N=d_1\times d_2\times\cdots\times d_b$ with $d_i\geqslant 2$ and with the order of multiplication fixed throughout the discussion. We use the underlying and fixed tensor product representation of $H^{[N]}$ to define the sets of computational and adjusted bases $E^{[N]}$ and $A^{[N]}$ for $N\times N$ matrices as

$$E^{[N]}_{j,k}=E^{(1)}_{j_1,k_1}\otimes\cdots\otimes E^{(b)}_{j_b,k_b} \quad\text{and}\quad A^{[N]}_{j,k}=A^{(1)}_{j_1,k_1}\otimes\cdots\otimes A^{(b)}_{j_b,k_b},$$

where *j* and *k* correspond to their *b* tuples and the superscripts in parentheses identify the corresponding d_i. It follows that $A^{[N]}_{j,k}=E^{[N]}_{j,j\oplus k}$ where the addition of the indices is defined by

$$j\oplus k\equiv(j_1+k_1 \bmod d_1,\ldots,j_b+k_b \bmod d_b). \tag{9}$$

The corresponding set of spin matrices $S^{[N]}$ is then defined by $(S^{[N]})=F^{[N]}(A^{[N]})$ or

$$S^{[N]}_{j,k}=\sum_{r=0}^{N-1} F^{[N]}(j,r)A^{[N]}_{r,k},$$

where $F^{[N]}=F^{(1)}\otimes\cdots\otimes F^{(b)}$ is the usual tensor product of the Fourier transforms $F^{(k)}$ that depend on d_k. Since we will be taking powers of the η's, we will use subscripts to denote the dependency of η on d_k: $\eta_k=\exp(2\pi i/d_k)$. It is easy to show that an equivalent definition of $S^{[N]}$ is given by

$$S^{[N]}_{j,k}=\otimes_{i=1}^{b}(F^{(i)}A^{(i)})_{j_i,k_i}. \tag{10}$$

Linearity again implies that if $\rho^{[N]}$ is a density matrix on the $N\times N$ Hilbert space $H^{[N]}$ with

$$\rho^{[N]}=\sum_{j,k} a^{[N]}_{j,k}A^{[N]}_{j,k}=\frac{1}{N}\sum_{j,k} s^{[N]}_{j,k}S^{[N]}_{j,k},$$

then

$$(s^{[N]})=F^{*[N]}(a^{[N]}) \tag{11}$$

and $a^{[N]}_{j,k}=\rho^{[N]}_{j,(j\oplus k)}$. Thus we have two different representations for a density matrix $\rho^{[N]}$, and both of them depend on the underlying tensor product representation of $H^{[N]}$.

IV. σ VARIATIONS

A fully separable density matrix can be represented as a convex combination of tensor products of pure states or trace one projections, and we need to represent such $d\times d$ projections in a systematic fashion in the spin basis. (All projections in this paper are trace one projections.) In the Appendix we show how all trace one projections for $d=3$ can be represented in a form completely analogous to the $d=2$ case, but for our immediate purposes we only need to characterize a subclass. The motivation is given by writing the particular $d=2$ projections $\frac{1}{2}(\sigma_0\pm\sigma_k)$ as $P_k(r)=\frac{1}{2}\Sigma^1_{m=0}[(-1)^r\sigma_k]^m$, where $r=0$ or $r=1$. Then $P_k(r)$ is the average of the cyclic subgroup generated by $(-1)^r\sigma_k$, and since $[(-1)^r\sigma_k]^2=\sigma_0$, the key property $P_k(r)P_k(r)=P_k(r)$ reduces to an exercise in group theory. The generalization of this idea to arbitrary d is immediate, and we first treat the case when d is prime.

Proposition 2. Let $d=p\geqslant 2$ be prime. Let $u=(j,k)\neq(0,0)$ denote the index of a spin matrix S_u, and let r be an integer. Then if $p>2$, the matrix

$$P_u(r)\equiv\frac{1}{p}\sum_{m=0}^{p-1}(\eta^rS_u)^m \tag{12}$$

is a projection with unit trace. The assertion is also valid for $p=2$ provided iS_u is used in lieu of S_u throughout when $u=(1,1)$.

Proof. A matrix P is a pure state or a trace one projection if it is Hermitian, has trace one, and $P^2=P$. First, $(\eta^rS_u)^m$ is proportional to $S_{mj,mk}$; consequently, it cannot be proportional to $S_{0,0}$ for $0<m<p$. Therefore only $S_{0,0}$ contributes to the trace of $P_r(u)$, confirming the trace condition. Using Eq. (8) it follows that $[(\eta^rS_u)^m]^\dagger=(\eta^rS_u)^{p-m}$ and that when p is odd $(\eta^rS_u)^m(\eta^rS_u)^{p-m}=(S_u)^p=(\eta^{jk})^{[p(p-1)]/2}S_{0,0}=S_{0,0}$. Thus $P_r(u)$ is Hermitian. The verification that $P_r(u)^2=P_r(u)$ follows from an easy computation. The assertion that $(\eta^{jk})^{[p(p-1)]/2}=1$ fails for prime p only when $p=2$ and $j=k=1$. Thus the reintroduction of i and of $-\sigma_y=iS_{1,1}$ is required to complete the proof.

As an example of the notation, it is easy to check that if $k=0$, then $P_{j,0}(r)$ is one of the diagonal projections $E_{i,i}$. Other projections are less sparse, however. For example, when $d=3$ and $k\neq 0$, $P_{j,k}(r)$ has no zero entries in the computational basis representation.

In the preceding proof, we exploited the fact that for d, an odd prime, the powers of each matrix S_u, $u\neq(0,0)$, form a cyclic subgroup of order d. When d is not prime we can get analogous results using a similar proof, but there are restrictions on the indices that arise since the coefficient of the identity matrix in Eq. (8) when $m=d$ need not be unity. In Proposition 2 this led to the introduction of the factor $i=\exp(\pi i/2)$ when $d=2$, and that modification is a special case of a more general situation.

Proposition 3. Suppose d is composite. Let $u=(j,k)$ be (0,1), (1,0) or else an index such that $j\neq 0$ and $k\neq 0$ have no common factors. Suppose d is odd or jk is even. Then if r is an integer,

$$P_u(r)=\frac{1}{d}\sum_{m=0}^{d-1}(\eta^rS_u)^m$$

is a projection with unit trace. If d is even and jk is odd, then

$$P_u(r)=\frac{1}{d}\sum_{m=0}^{d-1}(\alpha\eta^rS_u)^m$$

is a projection with unit trace, where $\alpha=e^{\pi i/d}$.

Proof. Suppose $(\eta^rS_u)^m$ or $(\alpha\eta^rS_u)^m$ is proportional to $S_{0,0}$ for $0<m<d$, so that $mj=rd$ and $mk=sd$ for some integers r and s. Since j and k are relatively prime, there are integers a and b such that $aj+bk=1$ [22], and it follows that $m=ard+bsd=(ar+bs)d$, contradicting $m<d$. Thus $P_u(r)$ has trace one. Using Eq. (8) when $m=d$, we find that the coefficient of $S_{0,0}$ is one in the first case, while in the second case the extra factor of $\alpha^d=(-1)$ is necessary to make the overall coefficient equal to one. In both cases it follows from that key result, as in Proposition 2, that $P^2_u(r)=P_u(r)$ and that $P_u(r)$ is Hermitian, completing the proof.

An important relationship between these subgroup projections and the generating spin matrix follows from the definitions. Since it is easy to check that $\{P_u(r),0\leqslant r<d\}$ defines an orthogonal family of trace one projections, the next result gives the spectral decomposition of $(\eta^rS_u)^t$ explicitly.

Corollary 2. For any integer $t\geqslant 0$ and any $d\geqslant 2$,

$$(\eta^rS_u)^t=\sum_{m=0}^{d-1}\eta^{-mt}P_u(m+r), \tag{13}$$

subject to the usual caveat about α. In particular, $S_{0,0}=\sum_{m=0}^{d-1}P_u(m+r)$.

Proof. As required,

$$\sum_{m=0}^{d-1}\eta^{-mt}P_u(m+r)=\frac{1}{d}\sum_k(\eta^r S_u)^k\sum_m\eta^{-mt}\eta^{mk}$$

$$=(\eta^r S_u)^t.$$

Next consider a Hilbert space that is the direct product of b Hilbert spaces with dimensions $d_1,\ldots,d_b$. Projections in the constituent d_i dimensional spaces also define projections in tensor product spaces, and the proof of the following is immediate. As before, we let the superscript k denote the dependence on d_k.

Corollary 3. Let $N=d_1\times d_2\times\cdots\times d_b$ and let $H^{[N]}=\otimes_{a=1}^{b}H^{[d_a]}$ be an N-dimensional Hilbert space. Let u denote a b-dimensional vector of index pairs $u_i=(j_i,k_i)$ where $0\leqslant j_i,k_i\leqslant d_i-1$, and let $r=(r_1,\ldots,r_b)$ where the r_i are integers. Then if the $P_{u_k}^{(k)}(r_k)$ are trace one projections on $H^{[d_k]}$,

$$P_u(r)=\bigotimes_{k=1}^{b}P_{u_k}^{(k)}(r_k)$$

is a trace one projection on $H^{[N]}$, provided αS_u is used in place of S_u when d is even and $u=(j,k)$ with jk odd. Furthermore, if $\eta(r)\equiv\Pi_{k=1}^{b}\eta_k^{r_k}$ and t is a non-negative integer,

$$(\eta(r)S_u^{[N]})^t=\sum_{l_1=0}^{d_1-1}\cdots\sum_{l_b=0}^{d_b-1}\bigotimes_{k=1}^{b}\eta_k^{-l_kt}P_{u_k}^{(k)}(l_k+r_k),\tag{14}$$

and in particular

$$S_{0,0}^{[N]}=\sum_{l_1=0}^{d_1-1}\cdots\sum_{l_b=0}^{d_b-1}\bigotimes_{k=1}^{b}P_{u_k}^{(k)}(l_k+r_k).$$

In order to show separability results for Werner densities, we need to identify a special class of fully separable density matrices in the tensor product space $H^{[N]}(d)$ of n d-dimensional Hilbert spaces, where $N=d^n$. This approach is motivated by results in [18] and is our final variation on the Pauli σ matrices.

Proposition 4. Let $d\geqslant 2$ and let $u^{(n)}=(u_1,\ldots,u_n)$ and $r^{(n)}=(r_1,\ldots,r_n)$ denote vectors of indices and values as defined in the preceding propositions. Then, provided αS_u is used in place of S_u when d is even and $u=(j,k)$ with jk odd,

$$\rho(u^{(n)},r^{(n)})=\frac{1}{d^n}\Bigg((S_{0,0}\otimes\cdots\otimes S_{0,0})+\sum_{m=1}^{d-1}[(\eta^{r_1}S_{u_1})^m\otimes\cdots\otimes(\eta^{r_n}S_{u_n})^m]\Bigg)$$

is a fully separable density matrix on $H^{[N]}(d)$.

Proof. The assertion is true for $n=1$ and suppose it holds for n. Let $u^{(n+1)}$ and $r^{(n+1)}$ be given index and parameter vectors. Since we require only the n'th and $(n+1)'$st indices in the proof, we leave the other indices fixed and implicit and let $\rho(u_n,r_n)$ denote $\rho(u^{(n)},r^{(n)})$. By the induction hypothesis

$$\frac{1}{d}\sum_{s=0}^{d-1}\rho(u_n,r_n+s)\otimes P_{u_{n+1}}^{(n+1)}(r_{n+1}-s)$$

is fully separable. Multiplying out and collecting terms produces expressions of the form

$$[(\eta^{r_1}S_{u_1})^{m_1}\otimes\cdots\otimes(\eta^{r_n}S_{u_n})^{m_1}]\otimes(\eta^{r_{n+1}}S_{u_{n+1}})^{m_2}\frac{1}{d}\sum_{s=0}^{d-1}\eta^{s(m_1-m_2)}.$$

By the same analysis used earlier, terms with $m_1=m_2$ have an overall coefficient of 1 while all other terms have a coefficient of 0, and that completes the proof of the induction step.

V. APPLICATIONS

We now have the tools to prove a general sufficient condition for full and partial separability that extends the results in [18]. It has been shown in earlier work [16,17] that for finite dimensional systems there is a neighborhood of the completely random state in which every density matrix is fully separable. That result together with the results in [14] and [15] obtaining a lower bound on the size of this neighborhood (for $N=2^n$ and $N=3^n$, respectively) follow as corollaries to Theorem 1.

As usual $H^{[N]}$ will denote an N-dimensional Hilbert space that can be written as a tensor product: $H^{[N]}=H^{[d_1]}\otimes\cdots\otimes H^{[d_b]}$, where the $H^{[d_k]}$ are d_k-dimensional spaces and $N=d_1\times d_2\times\cdots\times d_b$. We define $D\equiv(d_1,\ldots,d_b)$ and refer to $H^{[d_1]}\otimes\cdots\otimes H^{[d_b]}$ as the D tensor product version of $H^{[N]}$. Since $H^{[N]}$ may be represented as a tensor product space in different ways, the kind of separability to be discussed depends on the representation. For example, if $N=3^n$ and $H^{[N]}$ is represented as the tensor product of n three-dimensional spaces, we are discussing full separability. If subsets of the trits are taken together and represented in 3^k-dimensional spaces, we are discussing the corresponding partial separability. By virtue of Lemma 1, we know that the fundamental mathematics involved does not depend on the order in which the tensor products are taken or which trits are grouped together. In expressing the condition of the theorem, we use the D spin coefficients to introduce an L_1 norm on the space of $N\times N$ densities, and we will refer to that hereafter as the D spin norm and to the related separability as D separability.

Theorem 1. Let $H^{[N]}$ denote an N-dimensional Hilbert space with $N=d_1\times d_2\times\cdots\times d_b$. Suppose $H^{[N]}=H^{[d_1]}\otimes\cdots\otimes H^{[d_b]}$, where the $H^{[d_k]}$ are d_k-dimensional Hilbert spaces. If ρ is a density matrix on $H^{[N]}$, then ρ is $D\equiv(d_1,\ldots,d_b)$ separable provided

$$\|\rho\|_{1,D} \equiv \sum_{(j,k)\neq(0,0)} |s_{j,k}^{[N]}| \leqslant 1, \tag{15}$$

where ρ has the spin representation

$$\frac{1}{N}\sum_{j,k} s_{j,k}^{[N]} S_{j,k}^{[N]}$$

defined in term of the D tensor product $S_{j,k}^{[N]} = \otimes_{i=1}^{b} S_{j_i,k_i}^{(i)}$. It follows that in the set of density matrices on $H^{[N]}$ there is a neighborhood relative to D of the random state $(1/N)S_{0,0}^{[N]}$ in which every density matrix is D separable.

Proof. If d_i is prime or j_i and k_i are relatively prime, the factor $S_{j_i,k_i}^{(i)}$ can be written as a weighted sum of projections as in Corollary 2. If d_i is composite and the indices j_i and k_i are not relatively prime, then up to a factor of $\eta_i^{t_i}$, $S_{j_i,k_i}^{(i)}$ can be written as $(\eta_i^r S_u^{(i)})^s$ for some $u=(\overline{j_i},\overline{k_i})$ with $\overline{j_i}$ and $\overline{k_i}$ relatively prime, and thus $S_{j_i,k_i}^{(i)}$ can also be written as a weighted sum of projections. Now, since ρ is a density, either $S_{j,k}^{[N]}$ is Hermitian and thus $s_{j,k}^{[N]}$ is real, or $S_{j,k}^{[N]}$ appears in a pair $s_{j,k}^{[N]} S_{j,k}^{[N]} + s_{j,k}^{*[N]} (S_{j,k}^{[N]})^{\dagger}$. In the second case we use Eq. (14) in Corollary 3 and the preceding comments to collect the various factors of $\eta_i^{t_i}$ together and obtain

$$\begin{aligned} & s_{j,k}^{[N]} S_{j,k}^{[N]} + s_{j,k}^{*[N]} (S_{j,k}^{[N]})^{\dagger} \\ &= \sum_{l_1=0}^{d_1-1} \cdots \sum_{l_b=0}^{d_b-1} \bigotimes_{k=1}^{b} P_{u_k}^{(k)}(l_k) \{ \beta_{j,k} s_{j,k}^{[N]} \eta^*(l) \\ &\quad + \beta_{j,k}^* s_{j,k}^{*[N]} \eta(l) \} \\ &= |s_{j,k}^{[N]}| \sum_{l_1=0}^{d_1-1} \cdots \sum_{l_b=0}^{d_b-1} \bigotimes_{k=1}^{b} P_{u_k}^{(k)}(l_k) \\ &\quad \times \{ \exp(i\theta_{j,k}) \eta^*(l) + \exp(-i\theta_{j,k}) \eta(l) \}, \end{aligned}$$

where $\theta_{j,k}$ denotes the phase of $\beta_{j,k} s_{j,k}^{[N]}$ and l denotes the b vector with components l_k. The caveat that $\alpha_i S_u$ is in the projections $P_{u_k}^{(i)}(l_k)$ in lieu of S_u when d_i is even and $u=(j_i,k_i)$ with $j_i k_i$ odd applies throughout the proof and will not be explicitly cited. Since α_i has magnitude 1, only the phase factor will be affected. Using the last assertion in Corollary 3, we can write $|s_{j,k}^{[N]}| S_{0,0}^{[N]} + \frac{1}{2}(s_{j,k}^{[N]} S_{j,k}^{[N]} + s_{j,k}^{*[N]} (S_{j,k}^{[N]})^{\dagger})$ as

$$\begin{aligned} & |s_{j,k}^{[N]}| \sum_{l_1=0}^{d_1-1} \cdots \sum_{l_b=0}^{d_b-1} \bigotimes_{k=1}^{b} P_{u_k}(l_k) \\ & \quad \times \{ 1 + \cos[\theta_{j,k} - \arg(\eta(l))] \}. \end{aligned}$$

Since the expression in brackets is non-negative, the right-hand side is a non-negative multiple of a D-separable density. In the case when $S_{j,k}^{[N]}$ is Hermitian we derive the same expression with the same conclusion. It follows that ρ can be written as a convex combination of fully separable densities plus the residual term

$$\left(1 - \sum_{(j,k)\neq(0,0)} |s_{j,k}^{[N]}| \right) \frac{1}{N} S_{0,0}^{[N]}.$$

The hypothesis guarantees that the coefficient of $(1/N)S_{0,0}^{[N]}$ is non-negative, and that completes the proof of D separability.

As another application of the machinery, we can prove for prime p that the necessary condition $s \leqslant (1+p^{n-1})^{-1}$ is sufficient for full separability of the generalized Werner density matrix $W^{[N]}(s) = [(1-s)/N]\ I + s\tau$. We have $N=p^n$, I is the identity, τ is the projection defined by the state

$$|\psi^{[N]}\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} |\tilde{k}\rangle$$

and $\tilde{k}$ denotes the n-long repeated index $k \ldots k$. Given this special structure we find

$$\begin{aligned} W^{[N]}(s) &= \frac{1-s}{p^n} I + \frac{s}{p} \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} |\tilde{j}\rangle\langle\tilde{k}| \\ &= \frac{1-s}{p^n} I + \frac{s}{p} \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} A_{\tilde{j},\tilde{k}}^{[N]}, \end{aligned}$$

where we have used the modular vector addition defined in Eq. (9). Computing the spin coefficients gives $s_{0,0}=1$, $s_{j,m}=0$ if m is not a $\tilde{k}$ with $0 \leqslant k < p$, and otherwise

$$s_{j,\tilde{k}} = \sum_r F^*(j,r) \frac{s}{p} \delta(r, Ind),$$

where $Ind = \{\tilde{r} : 0 \leqslant r < p\}$. Using the dot product of the index vectors $j \cdot r = \Sigma j_k r_k \bmod p$,

$$\begin{aligned} s_{j,\tilde{k}} &= \sum_r \exp\left(\frac{-2\pi i}{p} (j \cdot r) \right) a_{r,\tilde{k}} \\ &= \frac{s}{p} \left[1 + \sum_{r=1}^{p-1} \exp\left(\frac{-2\pi i}{p} (j \cdot \tilde{r}) \right) \right]. \end{aligned}$$

Let $Ind(p,n) = \{j : \Sigma_{r=0}^{N-1} j_r = 0 \bmod p\}$. Then it is easy to check that $s_{j,\tilde{k}} = s$ if and only if j is in $Ind(p,n)$ and that there are exactly p^{n-1} such indices. All other $s_{j,\tilde{k}}$ equal zero, and we can write $W^{[N]}(s)$ in the spin basis as

$$W^{[N]}(s) = \frac{1-s}{p^n} S_{0,0}^{[N]} + \frac{s}{p^n} \sum_{j \in Ind(p,n)} \sum_{k=0}^{p-1} S_{j,\tilde{k}}^{[N]}. \tag{16}$$

Theorem 2. Let p be prime and $N=p^n$. Then the generalized Werner density matrix $W^{[N]}(s)$ is fully separable on $H^{[n]}(p)$ if and only if $s \leqslant (1+p^{n-1})^{-1}$.

Proof. As shown above, necessarily $s \leqslant (1+p^{n-1})^{-1}$. Checking the preceding derivation, note that

$$\frac{1}{p} \sum_{j=0}^{p-1} E_{\tilde{j},\tilde{j}} = \frac{1}{p} \sum_{j=0}^{p-1} A_{\tilde{j},\tilde{0}}^{[N]} = \frac{1}{p^n} \sum_{j \in Ind(p,n)} S_{j,0}^{[N]}$$

is a sum of fully separable projections. Taking $s=(1+p^{n-1})^{-1}$ we can write $W^{[n]}(s)$ as

$$W^{[n]}(s)=\frac{1}{1+p^{n-1}} \times\left[\frac{1}{p}\sum_{j=0}^{p-1}E_{\tilde{j},\tilde{j}}+\sum_{j\in Ind(p,n)}\frac{1}{p^n}\left(S_{\tilde{0},\tilde{0}}+\sum_{k=1}^{p-1}S_{j,\tilde{k}}\right)\right].$$

For each $k\neq 0$, $Ind(p,n)$ is mapped in a one-to-one manner onto itself by $j\rightarrow j$ where $(kj)_r=kj_r \bmod p$. Thus

$$W^{[n]}(s)=\frac{1}{1+p^{n-1}}\left\{\frac{1}{p}\sum_{j=0}^{p-1}E_{\tilde{j},\tilde{j}} +\sum_{j\in Ind(p,n)}\left[\frac{1}{p^n}\left(S_{\tilde{0},\tilde{0}}+\sum_{k=1}^{p-1}S_{kj,\tilde{k}}\right)\right]\right\}. \quad (17)$$

But since

$$(S_{j_1,1})^k\otimes\cdots\otimes(S_{j_n,1})^k=\eta^{k\Sigma j_i}S_{kj,\tilde{k}}=S_{kj,\tilde{k}}$$

for j in $Ind(p,n)$, each j sum in Eq. (17) is fully separable by Proposition 4, completing the proof.

It follows for the Werner densities that at the extreme value $s=(1+p^{n-1})^{-1}$, $\Sigma_{(j,k)\neq(0,0)}|s^{[N]}_{j,k}|=p(1-p^{-n})/(1+p^{-(n-1)})$, where the coefficients are based on the decomposition $D=(p,\ldots,p)$. When $p=n=2$, that value is 1, showing that the global bound of Theorem 1 is attained. However, for larger n and prime $p\geqslant 2$ the condition $\|\rho\|_{1,D}\leqslant 1$ is too strong for that class, and the special structure of the Werner densities allowed a more refined analysis of $D=(p,\ldots,p)$ separability.

It was shown in the qubit case in [18] that for each n and given $\epsilon>0$, there exists a $D=(2,\ldots,2)$-inseparable density on $H^{[2^n]}$ that has $\|\rho\|_{1,D}<1+\epsilon$. Thus for each fixed n the sufficient condition of Theorem 1 is the best possible for full separability of qubits. We conjecture that the same is true in general: given any separability vector D and $\epsilon>0$ there exists a D-inseparable density ρ with $\|\rho\|_{1,D}<1+\epsilon$.

Note added in proof. Theorem 2 has been shown to hold for all integers $\geqslant 2$ in Ref. [24].

ACKNOWLEDGMENTS

A. O. Pittenger gratefully acknowledges the hospitality of the Center for Quantum Computation at Oxford University and support from UMBC and the National Security Agency. M. H. Rubin wishes to thank the Office of Naval Research and the National Security Agency for support of this work.

APPENDIX A: PROOF OF EQ. (3)

In [18] a weaker but useful condition for qubits was derived using the Cauchy-Schwarz inequality. In this Appendix we extend that analysis to a more general context. For specificity, assume that $H^{[N]}=H^{[d_1]}\otimes H^{[d_2]}\otimes H^{[d_3]}$, with $N=d_1d_2d_3$, and that a given density matrix ρ on $H^{[N]}$ is separable with respect to that tensor product structure. Then ρ can be written as a convex combination of density matrices $\rho^{(r)}(a)$ on the factor spaces. In the computational basis on $H^{[d_r]}$ denoted by $|j_i\rangle_r, 1\leqslant i\leqslant d_r$, the matrix elements of ρ may be written as

$$\rho_{j_1j_2j_3,k_1k_2k_3}=\sum_a p(a)\rho^{(1)}_{j_1,k_1}(a)\rho^{(2)}_{j_2,k_2}(a)\rho^{(3)}_{j_3,k_3}(a).$$

Since each $\rho^{(r)}(a)$ is a density matrix, positivity requires that $\sqrt{\rho^{(r)}_{j_r,j_r}(a)}\sqrt{\rho^{(r)}_{k_r,k_r}(a)}\geqslant|\rho^{(r)}_{j_r,k_r}(a)|$ for each r and a. Then using the Cauchy-Schwarz inequality we have

$$\begin{aligned}[\rho_{j_1j_2j_3,j_1j_2j_3}\rho_{k_1k_2k_3,k_1k_2k_3}]^{1/2}&=\left[\sum_a p(a)\left(\sqrt{\rho^{(1)}_{j_1,j_1}(a)\rho^{(2)}_{j_2,j_2}(a)\rho^{(3)}_{j_3,j_3}(a)}\right)^2\right]^{1/2}\left[\sum_a p(a)\left(\sqrt{\rho^{(1)}_{k_1,k_1}(a)\rho^{(2)}_{k_2,k_2}(a)\rho^{(3)}_{k_3,k_3}(a)}\right)^2\right]^{1/2}\\ &\geqslant\sum_a p(a)\sqrt{\rho^{(1)}_{j_1,j_1}(a)\rho^{(1)}_{k_1,k_1}(a)\rho^{(2)}_{j_2,j_2}(a)\rho^{(2)}_{k_2,k_2}(a)\rho^{(3)}_{j_3,j_3}(a)\rho^{(3)}_{k_3,k_3}(a)}\\ &\geqslant\sum_a p(a)|\rho^{(1)}_{j_1,k_1}(a)||\rho^{(2)}_{j_2,k_2}(a)||\rho^{(3)}_{j_3,k_3}(a)|\\ &\geqslant|\rho_{v_1v_2v_3,u_1u_2u_3}|\end{aligned}$$

where, because of the Hermiticity of the density matrices, (v_r,u_r) may be either (j_r,k_r) or (k_r,j_r). This proof obviously generalizes to any number of factor spaces, yielding Eq. (3).

APPENDIX B: TRACE ONE PROJECTIONS FOR $d=3$

By emphasizing selected properties of projections for $d=2$, we can obtain a representation of all (trace one) projec-

tions in spin notation for $d>2$. We concentrate on $d=3$. To motivate the approach, recall from Eq. (6) that when $d=2$, $m_3=(1)\rho_{0,0}+(-1)\rho_{1,1}$, so that this particular spin coordinate is a convex combination of $(+1)$ and (-1), another way of stating the well-known correspondence between m_3, the coefficient of σ_z, and the diagonal of ρ. If ρ is also a projection, then in the computational coordinates, $\rho_{j,k}=b_j b_k \exp[i(\varphi_j-\varphi_k)]$, so that fixing m_3 fixes $\rho_{0,0}=b_0^2$ and $\rho_{1,1}=b_1^2$, and only the phase factor $\theta=\varphi_0-\varphi_1$ is unspecified. Using the change-of-basis formula, the two remaining spin coefficients of a projection with prescribed m_3 are thus given in terms of the parameter θ by

$$\begin{pmatrix} m_1 \\ -im_2 \end{pmatrix}=\begin{pmatrix} s_{0,1} \\ s_{1,1} \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} b_0 b_1 e^{i\theta} \\ b_0 b_1 e^{-i\theta} \end{pmatrix},$$

where $0\leqslant\theta<2\pi$. If we let t_k denote the value of $s_{k,1}$ when $\theta=0$, we can rewrite the preceding equation as

$$\begin{pmatrix} s_{0,1} \\ s_{1,1} \end{pmatrix}=\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} t_0 \\ t_1 \end{pmatrix}.$$

Making the obvious definitions, this gives $\vec{s}=M_2(\theta)\vec{t}$, and we also find that

$$M_2(\theta)=\begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{pmatrix}=\cos(\theta)\sigma_0+i\sin(\theta)\sigma_x.$$

The geometry of this result is that if $-1<m_3<1$, then the remaining spin coefficients in the projections associated with m_3 can be identified with the range of a one parameter family of invertible mappings $\{M_2(\theta)\}$ acting on $\vec{t}$ and are represented by the intersection of the surface of the Bloch sphere with a horizontal plane at height m_3.

The same pattern of results holds for $d=3$. Since $s_{2,0}=s_{1,0}^*$, the diagonal of a given ρ is in one-to-one correspondence with $s_{1,0}$ via the equation $s_{1,0}=\rho_{0,0}(1)+\rho_{1,1}(\eta^2)+\rho_{2,2}(\eta)$. That is, $s_{1,0}$ is a convex combination of the vertices of an equilateral triangle in the complex plane and thus *uniquely* corresponds to the weights of the vertices, weights that are the entries of the diagonal of ρ. For larger values of d, the geometry is more complicated. For example if $d=4$, the diagonal of a given ρ corresponds to two spin coefficients: $-1\leqslant s_{2,0}\leqslant+1$ and $s_{1,0}$, which is restricted to a rectangle in the complex plane with vertices $\pm(1+s_{2,0})/2 \pm i(1-s_{2,0})/2$. In general the diagonal of a density matrix ρ corresponds to $d/2$ spin coefficients $s_{j,0}$, $j\neq0$, when d is even and $(d-1)/2$ spin coefficients when d is odd.

Once $s_{1,0}$ is fixed in the $d=3$ case, there are three complex parameters remaining to be specified: $s_{0,1}, s_{1,1}$, and $s_{2,1}$, since the other four spin coefficients are forced by the restriction $s_{3-j,3-k}=\eta^{jk}s_{j,k}^*$. If ρ is a projection, $\Sigma|s_{j,k}|^2=3\Sigma|\rho_{j,k}|^2=3$, and thus $|s_{2,0}|^2+\Sigma|s_{k,1}|^2=1$, tempting one to look for an analogue of the Bloch sphere to represent all densities. However, the normalization arising from $\mathrm{tr}(\rho^2)=1$ is only a necessary condition on the parameters, and examples show it is not sufficient. (See also [19].) Instead we follow the $d=2$ paradigm and describe trace one projections associated with a *fixed* $s_{1,0}$. If ρ is such a projection, then in the computational coordinates $\rho=|u\rangle\langle u|$, where $|u\rangle$ denotes a normalized three vector with $u_k=b_k e^{i\varphi_k}$ and $\Sigma|b_k|^2=1$. Fixing $s_{1,0}$ fixes the b_k's, and it follows from Corollary 1 and the structure of ρ that

$$\begin{pmatrix} s_{0,1} \\ s_{1,1} \\ s_{2,1} \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 \\ 1 & \eta^2 & \eta \\ 1 & \eta & \eta^2 \end{pmatrix}\begin{pmatrix} e^{i\theta_0} & 0 & 0 \\ 0 & e^{i\theta_1} & 0 \\ 0 & 0 & e^{i\theta_2} \end{pmatrix}\begin{pmatrix} b_0 b_1 \\ b_1 b_2 \\ b_2 b_0 \end{pmatrix},$$

where $\theta_k=\varphi_k-\varphi_{k+1}$ with addition modulo 2π and with the normalization $\Sigma\theta_k=0 \bmod 2\pi$. Again, letting t_k denote the value of $s_{k,1}$ when the θ_k's are chosen to be zero, this time we obtain a two-parameter family of projections associated with a given value of $s_{1,0}$. Letting $\vec{s}$ denote the column vector of parameters, $\vec{t}$ the column vector with components t_k, and θ the three-vector of phase parameters, we have $\vec{s}=M_3(\theta)\vec{t}$, where

$$\begin{aligned} M_3(\theta)=&\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \eta^2 & \eta \\ 1 & \eta & \eta^2 \end{pmatrix}\begin{pmatrix} e^{i\theta_0} & 0 & 0 \\ 0 & e^{i\theta_1} & 0 \\ 0 & 0 & e^{i\theta_2} \end{pmatrix} \\ &\times\begin{pmatrix} 1 & 1 & 1 \\ 1 & \eta & \eta^2 \\ 1 & \eta^2 & \eta \end{pmatrix} \\ =&\sum_{k=0}^{2} f(k,\theta)S_{0,k}. \end{aligned} \tag{B1}$$

If $\theta+\phi$ is defined as component-wise addition, then it is easy to check that $\{M_3(\theta)\}$ also defines an Abelian group of invertible mappings,

$$M_3(\theta)M_3(\phi)=M_3(\theta+\phi),$$

giving the functional equation $\Sigma_k f(k,\theta)f(j-k,\phi)=f(j,\theta+\phi)$ in analogy with the corresponding result when $d=2$. We have thus established a correspondence between all trace one projection matrices with given diagonal and the range of a two-parameter family of mappings acting on $\vec{t}$. (We are endebted to Rasmus Hansen for bringing to our attention [23], which contains an analysis of the geometry of the convex space of $d=3$ densities. The pretransform characterization of the projections associated with a given diagonal is similar to the results derived here.)

In the $d=2$ case, the choices of $m_z=\pm1$ produce special cases of projections, and the same is true when $d=3$. If $s_{1,0}$ is one of the extreme points 1, η, or η^2, then two of the b_k's equal zero and all of the $s_{k,1}$'s equal zero. It follows that for $r=0$, 1, and 2, $\frac{1}{3}[S_{0,0}+\eta^r S_{1,0}+(\eta^r S_{1,0})^\dagger]$ is a trace one projection, and those are the three subgroup projections $P_{1,0}(r)$. A degeneracy that has no analogue in the $d=2$ case occurs when $s_{1,0}$ lies between two extreme points on an edge. Then exactly one of the b_k's equals zero, and there is a one-parameter family of projections associated with $s_{1,0}$.

The most interesting cases occur when $s_{1,0}$ lies in the interior of the equilateral triangle. In particular when $s_{1,0}=0$, the b_k's are equal to $1/\sqrt{3}$, and by choosing the components of θ appropriately from $\{0,2\pi/3,4\pi/3\}$ we find the remaining subgroup projections $P_u(r)$. Thus our entire analysis of separability in the $d=3$ case uses only the projections associated with the origin and with the vertices of the equilateral triangle.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).

[3] P. Shor, SIAM J. Comput. **26**, 1484 (1997).

[4] C. H. Bennett, *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[5] C. H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).

[6] D. DiVincenzo *et al.*, LANL e-print quant-ph/9910026.

[7] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[8] G. Vidal, LANL e-print quant-ph/9807077.

[9] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).

[10] W. Dur and J. I. Cirac, LANL e-print quant-ph/9911044.

[11] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

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

[13] R. Schack and C. M. Caves, e-print quant-ph/9904109.

[14] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999).

[15] C. M. Caves and G. J. Milburn, e-print quant-ph/9910001 (1999).

[16] R. Tarrach and G. Vidal, Phys. Rev. A **58**, 826 (1998).

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

[18] A. O. Pittenger and M. H. Rubin, e-print quant-ph/9912116.

[19] Arvind, K. S. Mallesh, and N. Mukunda, J. Phys. A **30**, 2417 (1997).

[20] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[21] D. I. Fivel, Phys. Rev. Lett. **74**, 835 (1995). We are indebted to David DiVincenzo for bringing this paper to our attention. See also the problems of J. Preskill, http://www.theory.caltech.edu/ preskill/ph229.

[22] G. E. Andrews, *Number Theory* (Dover Publications, New York, 1971).

[23] F. J. Bloore, J. Phys. A **9**, 2059 (1976).

[24] A. O. Pittenger and M. H. Rubin, Opt. Commun. (to be published); e-print quant-ph/0001110.