# Geometry of entanglement witnesses and local detection of entanglement

Arthur O. Pittenger and Morton H. Rubin
*Department of Mathematics and Statistics and Department of Physics, University of Maryland, Baltimore County, Baltimore, Maryland 21250*

(Received 8 August 2002; published 31 January 2003)

Let $H^{[N]}=H^{[d_1]}\otimes\cdots\otimes H^{[d_n]}$ be a tensor product of Hilbert spaces and let $\tau_0$ be the closest separable state in the Hilbert-Schmidt norm to an entangled state $\rho_0$. Let $\tilde{\tau}_0$ denote the closest separable state to $\rho_0$ along the line segment from $I/N$ to $\rho_0$ where $I$ is the identity matrix. Following A. O. Pittenger and M. H. Rubin [Linear Algebr. Appl. **346**, 75 (2002)] a witness $W_0$ detecting the entanglement of $\rho_0$ can be constructed in terms of $I$, $\tau_0$, and $\tilde{\tau}_0$. If representations of $\tau_0$ and $\tilde{\tau}_0$ as convex combinations of separable projections are known, then the entanglement of $\rho_0$ can be detected by local measurements. Gühne *et al.* [Phys. Rev. A **66**, 062305 (2002)] obtain the minimum number of measurement settings required for a class of two-qubit states. We use our geometric approach to generalize their result to the corresponding two-qudit case when $d$ is prime and obtain the minimum number of measurement settings. In those particular bipartite cases, $\tau_0=\tilde{\tau}_0$. We illustrate our general approach with a two-parameter family of three-qubit bound entangled states for which $\tau_0\neq\tilde{\tau}_0$ and we show that our approach works for $n$ qubits. We elaborated earlier [A. O. Pittenger, Linear Algebr. App. **359**, 235 (2003)] on the role of a ''far face'' of the separable states relative to a bound entangled state $\rho_0$ constructed from an orthogonal unextendible product base. In this paper the geometric approach leads to an entanglement witness expressible in terms of a constant times $I$ and a separable density $\mu_0$ on the far face from $\rho_0$. Up to a normalization this coincides with the witness obtained by Gühne *et al.* for the particular example analyzed there.

DOI: 10.1103/PhysRevA.67.012327 PACS number(s): 03.67.−a, 03.65.Ud

## I. MOTIVATION AND NOTATION

An important question for quantum information theory is how to determine if a given state is entangled. Physically, one would like to do this using local measurements and classical communications. Testing for entanglement is closely related to Bell's inequalities [1] and subsequent elaborations of Bell's inequalities [2]. Recently, other tests have been suggested, such as that in [3] which relies on the theory of positive operators and on eigenvalue estimation.

An alternative approach, which is experimentally realizable, is to define local correlated measurements motivated by some knowledge of the structure of $\rho$ itself, and this approach has been elaborated in [4]. To describe the problem, we first define the mathematical context. Specifically, we assume we are working with $n$ distinct systems so that $\rho$ is represented as an $N\times N$ density operating on the tensor product Hilbert space $H^{[N]}=H^{[d_1]}\otimes\cdots\otimes H^{[d_n]}$. The set $D$ of such $N\times N$ densities operating on $H^{[N]}$ is a compact convex subset of the real Hilbert space $M$ of $N\times N$ Hermitian matrices where the inner product is defined by $\langle A,B\rangle=\mathrm{Tr}[A^{\dagger}B]$. (Since the matrices are assumed to be Hermitian, the superscript † denoting the Hermitian conjugate appears to be redundant. However, we will have occasion to use the inner product for more general matrices.) The set of separable densities $S$ is defined as the convex hull of the separable projections $\pi_1\otimes\cdots\otimes\pi_n$, where $\pi_k$ is a projection on $H^{[d_k]}$. Since $S$ is a compact convex subset of $D$ one can test for entanglement by showing $\rho$ is separated from $S$ by a hyperplane in $M$ [5]. Geometrically the idea is clear. Mathematically it reduces to finding a Hermitian matrix $W$ with the property that $\mathrm{Tr}(W\rho)<0\leq\mathrm{Tr}(W\sigma)$ for every density $\sigma$ in $S$. The existence of such a $W$ is guaranteed by the general theory of convex sets in Hilbert spaces, and $W$ is known in the quantum information literature as an ''entanglement witness.'' A nice introduction to the subject and an overview of some of the literature can be found in [6].

In the context of two qubits Gühne *et al.* in [4] assume the general form of a two-parameter family of densities $\rho$ which includes a maximally entangled state $\rho_0$. They construct an entanglement witness using the eigenvector of the partial transpose of $\rho$ with the minimal (negative) eigenvalue and find that the resulting witness does not depend on either of the parameters. Since the separating hyperplane contains a face of the separable states, it is *optimal* in the sense that no witness detects a strictly larger set of entangled states. (See [7] for the definitions and [8] for an exposition related to the approach used in this paper.)

In [8], the authors showed how an entanglement witness $W_0$ sensing an inseparable $\rho_0$ can be constructed if one also knows the nearest separable state $\tau_0$:

$$\|\rho_0-\tau_0\|=\inf\{\|\rho_0-\sigma\|:\sigma\in S\}.$$

Since the norm is a continuous function and the set of separable densities is compact, $\tau_0$ exists, although actually computing it is not an easy problem in general. The entanglement witness is defined by

$$W_0=\tau_0+c_0I-\rho_0, \tag{1}$$

where $I$ is the $N\times N$ identity matrix and

$$c_0=\mathrm{Tr}(\tau_0(\rho_0-\tau_0)).$$

Details and examples of this construction are given in [8] where it is shown that $W_0$ is linked to the geometry via the induced inner product

$$\langle(\rho_0-\tau_0),(\rho-\tau_0)\rangle\equiv\mathrm{Tr}((\rho_0-\tau_0)(\rho-\tau_0))=-\mathrm{Tr}(W_0\rho). \tag{2}$$

In particular the separating hyperplane contains the "nearest" face of $S$ consisting of separable states $\sigma$ such that $\sigma-\tau_0$ is orthogonal to $\rho_0-\tau_0$. Equation (2) can be used to show that the extreme separable projections in the convex representation of $\tau_0$ must lie in the hyperplane, and that if any separable $\sigma$ in the nearest face has full rank then $W_0$ is optimal.

It was first shown in [9] that there is a neighborhood of the normalized identity or completely random state, $D_0=(1/N)I$, in which every state is separable. Given that fact, it follows from another compactness argument that there is a nearest separable density to $\rho_0$ along the line segment $[D_0,\rho_0]$:

$$\tilde{\tau}_0=(1-s_0)D_0+s_0\rho_0 \tag{3}$$

with $0<s_0<1$. While $\tau_0$ and $\tilde{\tau}_0$ differ in general, in certain examples they are the same, which simplifies the analysis. Thus we have the following general result.

*Theorem 1*. Suppose $\rho_0$ is inseparable. Using the notation above, the Hermitian matrix

$$W_0=I\left(c_0+\frac{1-s_0}{Ns_0}\right)+\tau_0-\frac{1}{s_0}\tilde{\tau}_0$$

is an entanglement witness for $\rho_0$ and is optimal if the nearest face contains a separable density of full rank. ■

Thus if one knew the convex representations of $\tau_0$ and $\tilde{\tau}_0$ in terms of tensor products of local projections, one could define specific coordinated local measurements that would experimentally detect the entanglement of $\rho_0$ via $\mathrm{Tr}(\rho_0W_0)$. Finding $\tau_0$ and $\tilde{\tau}_0$ is in general difficult but can be done in a variety of special cases. The examples we present include those analyzed in [4] as well as a two-parameter family of three-qubit bound entangled densities for which $\tau_0$ and $\tilde{\tau}_0$ differ. (A bound entangled state is entangled but has positive partial transposes.)

Another result in [4] is that three sets of coordinated local measurements is the minimum number required in their two-qubit context and an explicit representation of the three measurements was given. It was also asserted that at least $d+1$ such measurements would be required for a corresponding $d\times d$ system, but no suggestion for achieving that bound was provided. We show how the geometric approach to entanglement witnesses provides a unifying theme and leads to a concrete construction for the $d\times d$ case when $d$ is prime.

## II. TWO QUBITS

In the two-qubit case, the use of the nearest separable density clarifies some of the methodology and suggests the generalization to the $d\times d$ case. Following Ref. [4] we take

$$\rho=p\rho_a+(1-p)\sigma. \tag{4}$$

$\rho_a$ is defined by the state $a|00\rangle+b|11\rangle$, where $a$ and $b$ are real with $a^2+b^2=1$, $p$ is a parameter between 0 and 1, and $\sigma$ is a density close to the normalized identity, $\|\sigma-D_0\|<\delta$. The density $\sigma$ represents noise that is close to $D_0$, the completely random state. The idea is to define a separating hyperplane $W_0$ based on $\rho_0=\frac{1}{2}(|00\rangle+|11\rangle)(\langle 00|+\langle 11|)$ and investigate what inseparable states $\rho$ are detected by $W_0$.

It has been shown in a number of places that the closest separable state to $\rho_0$ is

$$\tau_0=\frac{2}{3}D_0+\frac{1}{3}\rho_0, \tag{5}$$

so that the roles of $\tau_0$ and $\tilde{\tau}_0$ coincide. (References and details are given in [8].) One computes $c_0=\mathrm{Tr}(\tau_0(\rho_0-\tau_0))=\frac{1}{6}$, and then Eq. (1) gives

$$W_0=\frac{1}{3}\begin{pmatrix}0&0&0&-1\\0&1&0&0\\0&0&1&0\\-1&0&0&0\end{pmatrix}. \tag{6}$$

This differs from the optimal witness found in [4] only because of the use of a different Bell state and is a special case of the general theorem above.

As an application we have the following result.

*Lemma 1*. A sufficient condition that $\rho=p\rho_a+(1-p)\sigma$, where $\|\sigma-D_0\|<\delta$, is not separable is that

$$\left(\frac{1+4\delta}{4ab+1+4\delta}\right)<p.$$

*Proof.*

$$\begin{aligned}\mathrm{Tr}(W_0\rho)&=p\,\mathrm{Tr}(W_0\rho_a)+(1-p)\mathrm{Tr}(W_0D_0)+(1-p)\\&\quad\times\mathrm{Tr}(W_0(\sigma-D_0))\\&=\frac{-2abp}{3}+\frac{1}{6}(1-p)+(1-p)\\&\quad\times\mathrm{Tr}(W_0(\sigma-D_0))\\&\leqslant\frac{-2abp}{3}+\frac{1}{6}(1-p)+(1-p)\frac{2\delta}{3},\end{aligned}$$

where we have used the Cauchy-Schwarz inequality in the last step. Setting the final expression to be less than 0, we obtain the desired inequality. Note that if $\delta=0$ and $a=1/\sqrt{2}$ we obtain the well-known sufficient condition $1/3<p$ for inseparability of $p\rho_0+(1-p)D_0$. ■

Having defined $W_0$ we need to show that the measurement can be effected by three types of coordinated local measurements. We combine Eq. (1) and Eq. (5) to obtain

$$W_0=\frac{2}{3}I-2\tau_0 \tag{7}$$

and then use the representation of $\tau_0$ as a convex combination of six separable extreme points in the face of the states of $S$ in the separating hyperplane:

$$\tau_0=\frac{1}{6}\Bigg[\left(\frac{\sigma_0+\sigma_z}{2}\otimes\frac{\sigma_0+\sigma_z}{2}\right)+\left(\frac{\sigma_0-\sigma_z}{2}\otimes\frac{\sigma_0-\sigma_z}{2}\right)$$
$$+\left(\frac{\sigma_0+\sigma_x}{2}\otimes\frac{\sigma_0+\sigma_x}{2}\right)+\left(\frac{\sigma_0-\sigma_x}{2}\otimes\frac{\sigma_0-\sigma_x}{2}\right)$$
$$+\left(\frac{\sigma_0+\sigma_y}{2}\otimes\frac{\sigma_0-\sigma_y}{2}\right)+\left(\frac{\sigma_0-\sigma_y}{2}\otimes\frac{\sigma_0+\sigma_y}{2}\right)\Bigg].\tag{8}$$

Thus one takes coordinated local measurements along the $x$, $y$, and $z$ axes of the Bloch sphere to compute $\mathrm{Tr}(W_0\rho)=\frac{2}{3}-2\,\mathrm{Tr}(\tau_0\rho)$. As shown in [4], this is the minimal number of coordinated local measurements that are required.

### III. THE $d\times d$ CASE

The approach used above immediately generalizes to the bipartite $d\times d$ case when $d$ is prime ($d\neq 2$): we take an entangled ‘‘base’’ state $\rho_0$ for which we can compute the nearest separable state $\tau_0$ and thus $W_0$. We again consider the family of densities $\rho=p\rho_a+(1-p)\sigma$, where $\sigma$ is close to the state $D_0$, and define

$$\rho_a=|\psi_a\rangle\langle\psi_a|\quad\text{where}\quad|\psi_a\rangle=\sum_{k=0}^{d-1}a_k|kk\rangle$$

with real $a_k$ such that $\Sigma_k a_k^2=1$. $\rho_0$ is the state with $a_k=1/\sqrt{d}$, and

$$\tau_0=\frac{d}{d+1}D_0+\frac{1}{d+1}\rho_0\tag{9}$$

is the closest separable state. (See [10] for the general result and references.) Again, $\tau_0$ coincides with $\tilde{\tau}_0$, simplifying the problem [8,11–13]. From Eq. (1) the optimal witness for $\rho_0$ is $W_0=2/(1+d)I-d\tau_0$, where $c_0=(d-1)/d(d+1)$. The problem now reduces to finding analogs of the Pauli matrices that can be used to represent $\tau_0$ as an appropriate convex combination of projections, as in Eq. (8). Fortunately that analysis has already been done.

In Ref. [14] the authors observed that the (real) Pauli matrices can be viewed as discrete Fourier transforms of four ‘‘computational’’ basis matrices. Using an analogous basis for $d\times d$ matrices and the corresponding discrete Fourier transform, one is able to define $d^2$ orthogonal unitary matrices

$$U_d\equiv\{S_u\ :\ u=(j,k),\quad 0\leqslant j,k<d\},$$

where $S_e=S_{(0,0)}$ is the $d\times d$ identity. (These same matrices were derived independently and in a different manner by Fivel [15] who used them in a study of Hamiltonians on a discrete state space. He also derived several of the properties we include below.) As with the two-qubit case, one can define sets of tensor products of projections, and it turns out that $\tau_0$ can be written as a convex combination of $d+1$ such sets in strict analogy with the representation in Eq. (8). These $d+1$ sets of projections correspond to the coordinated local measurements required in [4] for local detection of entanglement of $d\times d$ states.

We briefly summarize the necessary properties of these $d$-level ‘‘spin’’ matrices and relegate proofs to the Appendix. By definition

$$S_{(j,k)}=\sum_{r=0}^{d-1}\eta^{jr}|r\rangle\langle r+k|,$$

where addition is modulo $d$ and $\eta=\exp(2\pi i/d)$.

$$\mathrm{Tr}[S^{\dagger}_{(j_1,k_1)}S_{(j_2,k_2)}]=d\,\delta_{j_1,j_2}\delta_{k_1,k_2}$$

expresses orthogonality, and thus $U_d$ is a basis for $d\times d$ matrices.

Using tensor products of the $U_d$ spin matrices, we find that for prime $d$,

$$\tau_0=\frac{1}{d+1}\left[\frac{1}{d^2}\sum_{k=0}^{d-1}S_{k(d-k),00}+\sum_{j=0}^{d-1}\left(\frac{1}{d^2}\sum_{k=0}^{d-1}S_{(kj)(kd-kj),kk}\right)\right],\tag{10}$$

where $S_{ij,kl}=S_{i,k}\otimes S_{j,l}$, and it remains to show that each of the $k$ summations can be written as a sum of tensor products of complete sets of projections. When $d$ is odd and $u=(j,k)\neq(0,0)$,

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

is a (Hermitian) projection, and $\{P_u(r)\ :\ 0\leqslant r<d\}$ is a complete set of orthogonal projections. If $u_j=(j,1)$ and $v_j=(d-j,1)$ for $0\leqslant j<d$, then (suppressing the subscript on $u_j$ and $v_j$)

$$\frac{1}{d^2}\sum_{k=0}^{d-1}S_{(kj)(kd-kj),kk}=\frac{1}{d}\sum_{r=0}^{d-1}P_u(r)\otimes P_v(d-r).$$

The first summation (10) has an analogous representation if $u=(1,0)$ and $v=(d-1,0)$.

This completes the proof: the entanglement witness $W_0$ can be realized in terms of the identity and a separable density which in turn can be written as a convex combination of $d+1$ sums of tensor products of complete (local) projections. This attains the lower bound for the number of coordinated local measurements as asserted in [4].

As in the two-qubit case, the entanglement witness $W_0$ detects entanglement for a range of densities of the form $\rho=p\rho_a+(1-p)\sigma$. The computation is similar to that for Lemma 1, and we omit the details.

*Lemma 2.* $\rho=p\rho_a+(1-p)\sigma$ is inseparable provided

$$\frac{1-p}{p}\left(1-\frac{1}{d}+\delta\sqrt{2d(d-1)}\right)<\left(\sum_{k=0}^{d-1}a_k\right)^2-1,$$

where $\|\sigma-D_0\|<\delta$. When $d=2$, this reduces to the inequality in Lemma 1. ■

## IV. A THREE-QUBIT EXAMPLE

The geometric approach also works for a particular two-parameter family of three qubits which have positive partial transforms but are inseparable. Since these densities are not generated by complete unextendible product base (UPB) sets, it is not clear that other techniques can be used to define an appropriate entanglement witness.

Let $-1/8 \leqslant c,\ d \leqslant 1/8$, and define the three-qubit density matrix

$$\rho(c,d) = \begin{pmatrix} 1/8 & 0 & 0 & 0 & 0 & 0 & 0 & 1/8 \\ 0 & 1/8 & 0 & 0 & 0 & 0 & 1/8 & 0 \\ 0 & 0 & 1/8 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 1/8 & d & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 1/8 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 1/8 & 0 & 0 \\ 0 & 1/8 & 0 & 0 & 0 & 0 & 1/8 & 0 \\ 1/8 & 0 & 0 & 0 & 0 & 0 & 0 & 1/8 \end{pmatrix}.$$

It is convenient to identify $\rho(c,d)$ with the four-vector $\langle d,c,1/8,1/8\rangle$ defined by the negative diagonal. We will use this notation for densities with analogous structure. Further, it simplifies calculations to use $m=(c+d)/2$ and $t=(c-d)/2$, and we abuse notation by writing $\rho(m,t)$ for the same density and $\langle m-t,m+t,1/8,1/8\rangle$ for its four-vector. The following result is proved in [16] for analogous densities $\rho(c,d)$ for $n$ qubits defined by the $2^{n-1}$ vector with equal numbers of $c$'s and $d$'s in the interval $[-1/2^n,1/2^n]$ and $2^{n-2}$ entries of $1/2^n$, $\langle d,\ldots,d,c,\ldots,c,1/2^n,\ldots,1/2^n\rangle$.

*Proposition 1.* $\rho(c,d)$ has positive partial transposes and is completely separable if and only if $c=d$ $(t=0)$. ■

In the $d\times d$ cases analyzed above, the line segment from $D_0$ to $\rho_0$ was orthogonal to the nearest separable face, and that property characterized $\tau_0$, the nearest separable density to $\rho_0$. Unfortunately, as shown in [8], that perpendicularity is lost when one goes to three systems and the nearest separable state $\tilde{\tau}_0$ to $\rho_0$ on the line segment $[D_0,\rho_0]$ does not coincide with the closest separable state $\tau_0$. However, one can still take advantage of the geometry *provided* $\tilde{\tau}_0$ lies in the nearest separable face to $\rho_0$.

To pursue this idea for $\rho(c,d)$, we need some additional notation. Without loss of generality we take $c>d$ so that $t>0$, and let $\sigma_1=\sigma_x$ and $\sigma_2=\sigma_y$. Let $\sigma_0$ denote the $2\times 2$ identity and define

$$P^{\pm}_{jkl}=\frac{1}{8}[\sigma_0\otimes\sigma_0\otimes\sigma_0\pm\sigma_j\otimes\sigma_k\otimes\sigma_l], \tag{11}$$

where $j$, $k$, and $l$ will take the values 1 or 2. It is an easy exercise to represent such a $P^{\pm}_{jkl}$ as an average of four projections and to confirm that

$$\rho(m,t)=\left(\frac{1}{2}+4m\right)P^{+}_{111}+\left(\frac{1}{2}-4m\right)P^{-}_{221}+4t(P^{-}_{212}+P^{+}_{122}) \\ -8tD_0.$$

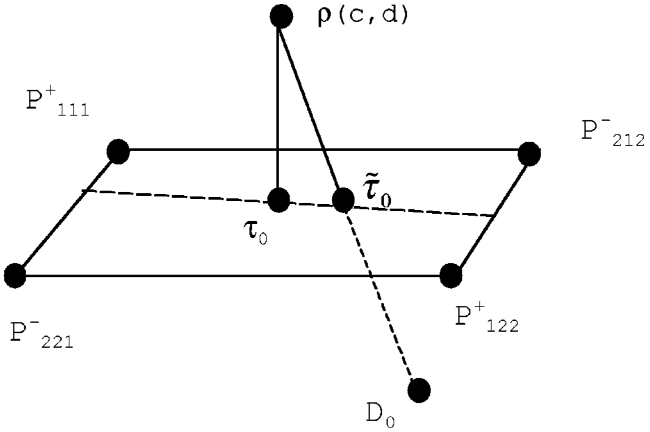

FIG. 1. The plane containing $\tau_0$, $\tilde{\tau}_0$ and the four separable densities of Eq. (3) is illustrated. The separable states lie below the plane and the random state $D_0$ is shown.

As it happens, a study of the $m=0$ case is key to the analysis, and we take as a candidate for $\tilde{\tau}_0(0,t)$ the normalization of the first part of $\rho(0,t)$:

$$\tilde{\tau}_0(0,t)=\frac{1}{1+8t}\left[\frac{1}{2}(P^{+}_{111}+P^{-}_{221})+4t(P^{-}_{212}+P^{+}_{122})\right]. \tag{12}$$

$\tilde{\tau}_0(0,t)$ is obviously separable but not so obviously the last separable state on $[D_0,\rho(0,t)]$. We confirm that property later. To see if $\tau_0(0,t)$ lies in the same face as $\tilde{\tau}_0(0,t)$, we take normalized combinations of the four $P^{\pm}_{jkl}$ in the equations above and minimize the distance to $\rho(0,t)$, finding the separable density with four-vector

$$\left\langle -\frac{t}{2},\frac{t}{2},\frac{1}{8}-\frac{t}{2},\frac{1}{8}-\frac{t}{2}\right\rangle.$$

Using this for $\tau_0(0,t)$ we find $c_0(0,t)=t/4$ and $W_0(0,t)=(t/4)W_0$, where

$$W_0=\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & -1 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & -1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & -1 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

These heuristics work splendidly, and we also find that $W_0$ detects the entanglement of all $\rho(c,d)$ with $d<c$. This is illustrated in Fig. 1 where the separating plane is shown. Of course, the geometry is more complicated because the hyperplane is not two dimensional. As $t$ decreases to 0, $\rho(0,t)$ moves to the center of the line segment $[P^{+}_{111},P^{-}_{221}]$. As $t$ becomes negative $(d>c)$, $\tau_0$ and $\tilde{\tau}_0$ move onto a new plane, where $P^{+}_{212}$ and $P^{-}_{122}$ replace $P^{-}_{212}$ and $P^{+}_{122}$. Recall that $D_0$ lies at the center of $[P^{+}_{ijk},P^{-}_{ijk}]$. The case $m\neq 0$ is easily visualized.

*Proposition 2*. Let $d<c$. Then $\tau_0(m,t)$ with four-vector $\langle m-t/2,m+t/2,1/8-t/2,1/8-t/2\rangle$ is the closest separable density to $\rho(m,t)$. $W_0$ is an entanglement witness for every density in $\{\rho(c,d)\,:\,-1/8\leqslant d<c\leqslant 1/8\}$.

*Proof*. Set $m=0$ and let $\pi=\pi_1\otimes\pi_2\otimes\pi_3$ denote any separable projection. Since $\mathrm{Tr}(W_0\rho(0,t))<0$ by construction, it suffices to confirm that $\mathrm{Tr}(W_0\mu)\geqslant 0$. Defining $\pi_k=|\psi_k\rangle\langle\psi_k|$, where

$$|\psi_k\rangle=\begin{bmatrix}\cos\theta_k\\ e^{i\phi_k}\sin\theta_k\end{bmatrix},$$

we obtain

$$2\,\mathrm{Tr}(W_0\mu)=2-\sin(2\theta_1)\sin(2\theta_2)\sin(2\theta_3)C(\varphi_1,\varphi_2,\varphi_3), \tag{13}$$

where

$$C(\varphi_1,\varphi_2,\varphi_3)=\cos(\varphi_1+\varphi_2+\varphi_3)+\cos(\varphi_1+\varphi_2-\varphi_3)+\cos(\varphi_1-\varphi_2+\varphi_3)-\cos(\varphi_1-\varphi_2-\varphi_3).$$

The phase angles $\varphi_k$ can take any value while $0\leqslant\theta_k\leqslant\pi/2$. Confirming that the right side of Eq. (13) is non-negative is a familiar Bell-inequality computation and proves the assertion when $m=0$. It follows from comments after Eq. (2) that $\tilde{\tau}_0(0,t)$ has to lie in the separating plane and is thus the closest separable state to $\rho(0,t)$ along $[D_0,\rho(0,t)]$, justifying the notation and the assumption made earlier.

The generalization to nonzero $m$ is straightforward. Using the asserted form for $\tau_0(m,t)$, it is easy to check that $\tau_0(m,t)$ is separable, that $\rho(m,t)-\tau_0(m,t)=\rho(0,t)-\tau_0(0,t)$, and also that $c_0(m,t)=t/4$. It follows that $\tau_0(m,t)$ is the closest separable state to $\rho(m,t)$ and $W_0(m,t)=W_0(0,t)$, completing the proof. ■

From $\rho(m,t)=(1+8t)\tilde{\tau}_0(m,t)-8tD_0$ and the form of $\tau_0(m,t)$ we can express the entanglement witness in terms of the identity and explicit separable states:

$$W_0(0,t)=t\left[\frac{5}{4}I-2(P^{+}_{111}+P^{-}_{221}+P^{-}_{212}+P^{+}_{122})\right].$$

Again we have shown that local detection of entanglement can be defined using the explicit representations of $\tau_0$ and $\tilde{\tau}_0$ as convex combinations of separable projections.

## V. GENERALIZATION TO *N* QUBITS

In Ref. [16] $\tilde{\tau}_0$ was computed for the $\rho_0$ generated from the $n$-qubit Greenberger-Horne-Zeilinger GHZ state defined by

$$\rho_0=|\psi_0\rangle\langle\psi_0|,\quad\text{where }\ |\psi_0\rangle=\frac{1}{\sqrt{2}}(|\tilde{0}\rangle+|\tilde{1}\rangle),$$

and $\tilde{j}=(j,\ldots,j)$. It was shown that

$$\tilde{\tau}_0=(1-s_0)D_0+s_0\rho_0 \tag{14}$$

$$=s_0\Delta+(1-s_0)Q, \tag{15}$$

where $s_0=1/(2^{n-1}+1)$, $\Delta=\frac{1}{2}(|\tilde{0}\rangle\langle\tilde{0}|+|\tilde{1}\rangle\langle\tilde{1}|)$, and $Q$ is a $2^n\times 2^n$ matrix with entries $1/2^n$ on the diagonal and in the upper and lower corners. It is clear that $\Delta$ is a convex combination of two separable states. In [16] $Q$ was expressed in terms of $2^{n-1}$ separable states. In [8] we also computed $\tau_0$ and it can be shown that $\tau_0$ can be expressed as a convex combination of $\Delta$ and $Q$. This is another example of a case when $\tau_0\neq\tilde{\tau}_0$ but both densities lie on the near face. Applying Theorem 1 the optimal entanglement witness can be written as

$$W_0=aI-b\Delta-cQ \tag{16}$$

with $a$, $b$, and $c$ positive. In the two-qubit case this result reduces to Eq. (6).

## VI. FAR-FACE CONSTRUCTIONS

There are cases when an entanglement witness can be defined in terms of the identity and a separable state without computing the nearest separable density explicitly. In [17] a technique is described for the construction of inseparable densities with positive partial transposes, using orthogonal unextendible product bases. This clever approach assumes a set of $m$ separable orthonormal states $B=\{|\varphi_k\rangle,1\leqslant k\leqslant m\}$ where each $|\varphi_k\rangle$ is a tensor product of states in their respective Hilbert spaces and where the orthogonal space $B^{\perp}$ contains no separable projections. If $\mu_k=|\varphi_k\rangle\langle\varphi_k|$ and one defines

$$\mu_0=\frac{1}{m}\sum_{k=1}^{m}\mu_k, \tag{17}$$

then

$$\rho_0=\frac{N}{N-m}D_0-\frac{m}{N-m}\mu_0$$

can be shown to be an inseparable density with positive partial transpose. A number of examples of orthogonal UPBs are given in [17] and in subsequent papers such as [18] and [19]. The ideas in [4] also apply in this context and are illustrated there using the two-qutrit example "TILES" of [17].

In [20] some consequences of the geometric structure implicit in this approach are developed. For example, it is clear from the equation above that $D_0$ lies on the line segment $[\mu_0,\rho_0]$. If one denotes by $F_0$ the face of the separable densities $S$ containing $\mu_0$, then, in the context of the real Hilbert space $M$, $F_0$ is orthogonal to that line. It is shown in [6] by a compactness argument that there is a positive $\epsilon$ such that

$$0<\frac{\epsilon}{m}=\inf\{\mathrm{Tr}[\mu_0\sigma],\quad\sigma\in S\}$$

and thus that the face $G_0 \equiv \{\sigma \in S : \mathrm{Tr}[\mu_0 \sigma] = \epsilon/m\}$ is nonempty. In this context it is shown in [20] that

$$0 < s_0 \equiv 1 - \frac{\epsilon N}{m} < 1.$$

A consequence of this approach is that a separating witness $W_0$ for $\rho_0$ can be defined using Eq. (1) with

$$\hat{\tau}_0 = (1 - s_0) D_0 + s_0 \rho_0 .$$

In this construction $\hat{\tau}_0$ is not necessarily separable but is defined by the intersection of $[\mu_0, \rho_0]$ and a hyperplane containing the "near face" $G_0$. Since both $\rho_0$ and $\hat{\tau}_0$ can be written explicitly in terms of $\mu_0$, which is separable, then once $\epsilon$ is known we can again express the entanglement witness in terms of the identity $I$ and a separable density whose convex representation is known:

$$W_0 = \frac{\epsilon N}{N - m} \left( \mu_0 - \frac{\epsilon}{m} I \right).$$

Thus, the required coordinated local measurements are defined explicitly by the original set $B$ and there will be no more than $m$ different settings. Geometrically $W_0$ is expressed in terms of the identity and $\mu_0$, which lives in the far face $F_0$, on the "other side" of $D_0$ from $\rho_0$. In the special case discussed in [4], this is the same witness as derived there, up to a multiplicative constant.

Consider separable densities $\mu_b = \Sigma_k p_k \mu_k$ in the face $F_0$ that are also close to $\mu_0$. Let $b$ denote the reciprocal of the largest of the coefficients $p_k$. Then it is easy to define inseparable densities

$$\rho_b = \frac{N D_0 - b \mu_b}{N - b}$$

with positive partial transposes that are on the boundary of the set of densities $D$ and are close to $\rho_0$. Moreover, $W_0$ can also serve as an entanglement witness for these densities. In fact, using the same notation as above, one can get a "frustum" of states of the form

$$\rho = (1 - p)\sigma + p \rho_b$$

which lie in $D$ on the $\rho_0$ side of the hyperplane defined by $W_0$, provided

$$\frac{p(m-b)}{N-b} + \frac{1-p}{N} + \frac{(1-p)\delta}{\sqrt{m}} < \frac{\epsilon}{m}, \tag{18}$$

where $\|\sigma - D_0\| < \delta$. We omit the details, repeating instead that the Euclidean geometry of $M$ provides an extremely useful context for examining questions of this sort and that the use of Eq. (1) gives a unifying geometric approach for constructing entanglement witnesses.

We should note that the effect of dropping the hypothesis that the states in $B$ are orthogonal is also discussed in [20], and weaker conditions on the states in $B$ are given which allow the construction above of inseparable states to be generalized. In particular, one can perturb the orthogonal UPB case, losing orthogonality but preserving enough of the structure to allow the analysis to go through. The cost of this generalization, however, is that the resulting states do not automatically have positive partial transposes.

## VII. SUMMARY

In this paper we have used a geometric definition of an entanglement witness $W_0$ detecting an inseparable state $\rho_0$ to show that $W_0$ always has a representation leading to entanglement detection using coordinated local measurements. This approach gives essentially the same witnesses and the same coordinated local measurements as derived in [4] for their particular two-qubit case. When coupled with the generalized "spin" matrices defined in [14], it also achieves the lower bound asserted in [4] for the number of coordinated local measurements for the analogous $d \times d$ case, at least when $d$ is prime. We also illustrated the use of the geometry by applying the methodology to a two-parameter family of three-qubit bound entangled states for which $\tau_0$ and $\tilde{\tau}_0$ differ. The strength of the geometrical approach is further illustrated by applying it to the $n$-qubit case. In the case of inseparable densities constructed using orthogonal UPBs, the geometric approach also applies, but produces a representation using a "far-face" separable density.

## ACKNOWLEDGMENTS

This work was supported in part by NSF and ONR.

## APPENDIX

By definition the $S_{(j,k)}$ "spin" matrix is

$$S_{(j,k)} = \sum_{r=0}^{d-1} \eta^{jr} |r\rangle\langle r+k|,$$

where addition is modulo $d$ and $\eta = \exp(2\pi i/d)$. If $u$ denotes $(j,k)$, then $S_u$ has trace 0 unless $u$ equals $e \equiv (0,0)$. Orthogonality follows from:

$$\begin{aligned}
&\mathrm{Tr}[S^\dagger_{(j_1,k_1)} S_{(j_2,k_2)}] \\
&\quad = \mathrm{Tr}\left[ \sum_r \sum_s \eta^{-j_1 r} \eta^{j_2 s} (|r+k_1\rangle\langle r|)(|s\rangle\langle s+k_2|) \right] \\
&\quad = \mathrm{Tr}\left[ \sum_r \eta^{(j_2 - j_1) r} |r+k_1\rangle\langle r+k_2| \right] \\
&\quad = d\,\delta_{j_1,j_2} \delta_{k_1,k_2}.
\end{aligned}$$

Similarly, one can calculate some useful relations such as $S_{0,1}S_{1,0} = \eta S_{1,0}S_{0,1}$, $S_{j,k} = (S_{1,0})^j (S_{0,1})^k$, $(S_{j,k})^m = \eta^{jkm(m-1)/2} S_{mj,mk}$, and $S^\dagger_{j,k} = \eta^{jk} S_{d-j,d-k}$. Unlike the Pauli matrices, the $S_u$ are not necessarily Hermitian, but they are unitary and can play a role analogous to that played by the Pauli matrices.

Any $d\times d$ density $\alpha$ can thus be written as a linear combination of these spin matrices, and we have

$$\alpha=\frac{1}{d}\left[S_e+\sum_{u\neq e}s_uS_u\right],$$

where we use $u=(j,k)$ in

$$s_u=\mathrm{Tr}[S_u^\dagger\alpha]=\sum_r\eta^{-jr}\alpha_{r,r+k}.$$

To represent a density such as $\tau_0$ defined in Eq. (9) on the tensor product space $H^{[d]}\otimes H^{[d]}$, we use the set of tensor products of the spin matrices as an orthogonal basis. A direct calculation or an invocation of Eq. (16) of Ref. [14] gives

$$\tau_0=\frac{1}{d^2}\left[\frac{d}{d+1}S_{00,00}+\frac{1}{d+1}\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}S_{i(d-i),kk}\right],$$

where $S_{ij,kl}=S_{i,k}\otimes S_{j,l}$. It is at this point that we require $d$ be prime. Then for given $i$ and $k\neq0$ there is a unique $j$ such that $i=jk$ (mod $d$), and we can rewrite $\tau_0$ in the form

$$\begin{aligned}\tau_0=\frac{1}{d+1}&\left[\frac{d}{d^2}S_{00,00}+\frac{1}{d^2}\sum_{i=0}^{d-1}S_{i(d-i),00}\right.\\&\left.+\frac{1}{d^2}\sum_{k=1}^{d-1}\sum_{j=0}^{d-1}S_{(kj)(kd-kj),kk}\right]\\=\frac{1}{d+1}&\left[\frac{1}{d^2}\sum_{k=0}^{d-1}S_{k(d-k),00}\right.\\&\left.+\sum_{j=0}^{d-1}\left(\frac{1}{d^2}\sum_{k=0}^{d-1}S_{(kj)(kd-kj),kk}\right)\right].\end{aligned}$$

It remains to show that each of the expressions involving a $k$ summation is a summation of tensor products of projections from a complete set of orthogonal projections. That is, each summation corresponds to correlated local measurements, and $\tau_0$ is realized by $d+1$ such summations.

We begin by defining a complete set of projections in terms of the spin matrices, a construction which corresponds to that in the spin 1/2 context.

*Lemma 3*. Let $d>2$ be prime and let $e\neq u=(j,k)$. Then if

$$P_u(r)\equiv\frac{1}{d}\sum_{m=0}^{d-1}(\eta^rS_u)^m=\frac{1}{d}\sum_{m=0}^{d-1}\eta^{mr}\eta^{jkm(m-1)/2}S_{mu},$$

$\{P_u(r):0\leqslant r<d\}$ is a complete set of trace-1, orthogonal (Hermitian) projections [14].

*Proof*. $P_u(r)$ has trace 1 since the only term with nonzero trace is the $m=0$ term. From the definition

$$\begin{aligned}&P_u(r)P_u(s)\\&\quad=\frac{1}{d^2}\sum_{m=0}^{d-1}\sum_{n=0}^{d-1}\eta^{mr+ns}\eta^{jk[m(m-1)+n(n-1)]/2}S_{mu}S_{nu}\\&\quad=\frac{1}{d^2}\sum_{m=0}^{d-1}\sum_{n=0}^{d-1}\eta^{(m+n)r}\eta^{jk[m(m-1)+n(n-1)]/2}\eta^{jkmn}\\&\qquad\times S_{(m+n)u}\eta^{n(s-r)}.\end{aligned}$$

Make the substitution $t=m+n$ in the last expression and collect terms to obtain

$$P_u(r)P_u(s)=\left(\frac{1}{d}\sum_{n=0}^{d-1}\eta^{n(s-r)}\right)\frac{1}{d}\sum_{t=0}^{d-1}\eta^{tr}\eta^{jkt(t-1)/2}S_{tu},$$

thereby obtaining both the orthogonality and $P_u(r)P_u(r)=P_u(r)$. Finally,

$$\begin{aligned}(P_u(r))^\dagger&=\frac{1}{d}\sum_{m=0}^{d-1}\eta^{-mr}(S_u^\dagger)^m=\frac{1}{d}\sum_{m=0}^{d-1}\eta^{-mr}(\eta^{jk}S_{-u})^m\\&=\frac{1}{d}\sum_{m=0}^{d-1}\eta^{-mr+mjk+jkm(m-1)/2}S_{-mu}\\&=\frac{1}{d}\sum_{n=0}^{d-1}\eta^{nr+jkn(n-1)/2}S_{nu}=P_u(r).\end{aligned}$$

These steps actually introduce a factor of the form $\eta^{jkd(d-1)/2}$ which equals 1 for odd integers. However, if $d$ is even and $j$ and $k$ are odd, $\eta^{jkd(d-1)/2}\neq1$, and the definition of $P_u(r)$ must be modified. ■

Having defined complete sets of projections, we are ready for the final technical result.

*Proposition 3*. Let $u_j=(j,1)$ and $v_j=(d-j,1)$ for $0\leqslant j<d$. Then

$$\frac{1}{d}\sum_{r=0}^{d-1}P_{u_j}(r)\otimes P_{v_j}(d-r)=\left(\frac{1}{d^2}\sum_{k=0}^{d-1}S_{(kj)(kd-kj),kk}\right).$$

If $x=(1,0)$ and $y=(d-1,0)$, then

$$\frac{1}{d}\sum_{r=0}^{d-1}P_x(r)\otimes P_y(d-r)=\frac{1}{d^2}\sum_{k=0}^{d-1}S_{k(d-k),00}.$$

*Proof*. The proof is just a matter of navigating the notation. Suppressing the subscript,

$$\frac{1}{d}\sum_{r=0}^{d-1} P_u(r)\otimes P_v(d-r)$$

$$=\frac{1}{d^3}\sum_{k,n}(S_u)^k\otimes(S_v)^n\sum_r \eta^{(k-n)r}$$

$$=\frac{1}{d^2}\sum_k S_{ku}\otimes S_{kv}\,\eta^{[jk(k-1)/2+(d-j)k(k-1)/2]}$$

$$=\frac{1}{d^2}\sum_m S_{ku}\otimes S_{kv}$$

$$=\frac{1}{d^2}\sum_{k=0}^{d-1} S_{(kj)(kd-kj),kk}$$

as required. The proof of the remaining assertion is similar, and we omit the details. ■

[1] J. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, London, 1993).

[2] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[3] Artur Ekert and Pawel Horodecki, e-print quant-ph/0111064.

[4] O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).

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

[6] B. M. Terhal, J. Theor. Comp. Sci. **287**(1), 313 (2002).

[7] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[8] A. O. Pittenger and M. H. Rubin, Linear Algebr. Appl. **346**, 75 (2002).

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

[10] A. O. Pittenger and M. H. Rubin, Opt. Commun. **179**, 447 (2000).

[11] R. B. Lockhart and M. J. Steiner, Phys. Rev. A **65**, 022107 (2002).

[12] R. B. Lockhart, M. J. Steiner, and K. Gerlach, QIC, **2**, 333 (2002).

[13] C. Witte and M. Trucks, Phys. Lett. A **257**, 14 (1999).

[14] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 032313 (2000).

[15] D. I. Fivel, Phys. Rev. Lett. **74**, 835 (1995).

[16] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 042306 (2000).

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

[18] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, e-print quant-ph/9908070.

[19] D. P. Vincenzo and B. M. Terhal, e-print quant-ph/0008055; Proceedings of the XIII International Congress on Mathematical Physics (to be published).

[20] A. O. Pittenger, Linear Algebr. Appl. **359**, 235 (2003).