Generalized Circulant Densities and a Sufficient Condition for Separability

Dariusz Chruściński
Institute of Physics, Nicolaus Copernicus University,
Grudziądzka 5/7, 87–100 Toruń, Poland

Arthur O. Pittenger
Department of Mathematics and Statistics,
University of Maryland, Baltimore County, Baltimore, MD 21250

Abstract

In a series of papers with Kossakowski, the first author has examined properties of densities for which the *positive partial transposition* (PPT) property can be readily checked. These densities were also investigated from a different perspective by Baumgartner, Hiesmayr and Narnhofer. In this paper we show how the support of such densities can be expressed in terms of lines in a finite geometry and how that same structure lends itself to checking the necessary PPT condition and to a novel sufficient condition for separability.

1 Introduction

Interest in quantum information theory has dramatically increased as the effectiveness of using quantum entanglement as a resource for storing and manipulating information has become more apparent. Early ideas for applications include Shor's and Grover's algorithms (see [1] for example) as well as quantum key distribution [2], and those insights have motivated the surge in theoretical and experimental work during the last fifteen years. Since much of quantum information theory is modelled in the context of finite dimensional composite systems, a subject of particular interest is determining the presence or absence of entanglement in terms of the structure of the density matrix modelling the system.

If one is dealing with two d–level particles, the bipartite context, one can model the state of the composite system as a positive semi-definite trace one matrix ρ on the tensor product product space $C_d \otimes C_d$, where C_d denotes a d–dimensional Hilbert space over the complex numbers. The system is said to be *separable* if it is in the convex hull of densities of the form $\tau_1 \otimes \tau_2$, where each τ_k is a d–dimensional density on its respective space. An early observation by Peres [3] was that such separable states have the positive partial transpose PPT property: they remain separable under the partial transpose defined, for example, by $\tau_1 \otimes \tau_2 \rightarrow \tau_1 \otimes \tau_2^t$, where the superscript denotes the transpose operation.

Since separable systems can be modelled classically, the two particles are not entangled. Thus the PPT condition is a necessary condition for separability, and it has been shown that it is also sufficient in the tensor dimensions $2 \otimes 2$ and $2 \otimes 3$ [4]. In higher dimensions, the condition is not sufficient, as illustrated by a number of examples such as those in [5] and [6] among others. Nonetheless it has proved to be a surprisingly useful criterion, and there are a variety of examples of densities illustrating that fact. In [7] (see also [8]) the authors observed that many of these examples have a common property that facilitates checking the PPT property. That same structure was also defined in [9], [10], and [11], where the goal was to investigate the geometry of a particular subset of densities using "discrete phase space" as a tool. That discrete structure has been used extensively in other contexts – [12], [13], and [14] are just a few of many examples – and the first part of this paper relates the structure of this class of densities to the finite geometry of phase space and to checking the PPT condition.

In the second part of the paper we show how the structure of these densities permits the development of a useful sufficient condition for separability. This condition is an offspring of a sufficient condition for separability that appears in [6], for example, and that serves as a counterpoint to the necessary PPT condition, since there are separable densities that don't satisfy it. The third part of the paper consists of a number of examples, including some of those in [7, 8], [9] and [10], and illustrates the use of this structural criterion

We should note in passing that the investigation of separability and entanglement is an active area of research and there and too many papers to cite. Two survey papers on separability and on entanglement are [15] and [16]. The interested reader is referred to those surveys for an overview of the subject and also to [6] for the derivation of the sufficient condition that motivates our main result.

2 Circulant densities and the PPT condition

Motivated by the examples in [7], we establish notation that expresses the support of circulant densities in terms of lines in the context of finite geometry. The densities ρ to be considered are $d^2 \times d^2$ positive semidefinite, trace one matrices with a particular pattern of support, and we begin by distinguishing between the positions where non-zero entries can appear and the entries themselves. Let M be a $d^2 \times d^2$ matrix with entries equal to zero or one and let *support*(M) denote the set of positions of M with entry equal to one.

Let $\{B\,(j,k) : 0 \leq j,k < d\}$ denote the constituent $d \times d$ submatrices, so that when $d = 3$, for example,

$$M = \begin{pmatrix} B\,(0,0) & B\,(0,1) & B\,(0,2) \\ B\,(1,0) & B\,(1,1) & B\,(1,2) \\ B\,(2,0) & B\,(2,1) & B\,(2,2) \end{pmatrix} . \tag{2.1}$$

For M to provide the locations for the non-zero entries of a density, we obviously need symmetry, $M = M^t$, and that is equivalent to $B^t\,(j,k) = B\,(k,j)$ for all j, k. Entries of M can be indexed as $M(r,s)$, $0 \leq r,s < d^2$ or in tensor product notation as $M_{j_1 j_2, k_1 k_2}$, $0 \leq j_1, j_2, k_1, k_2 < d$. The relationship between the two is

$$(r,s) \leftrightarrow (dj_1 + j_2, dk_1 + k_2) \ . \tag{2.2}$$

In particular, we routinely use the fact that such an entry corresponds to the (j_2, k_2) entry of $B\,(j_1, k_1)$.

As the authors noted implicitly or explicitly in [7] and [10], the support of M can be interpreted as lines in a two dimensional *module*; that is, they are lines in

$$V_2(d) = \{(x,y) : x, y \in Z_d\} \ , \tag{2.3}$$

where Z_d denotes the integers modulo d. (If d is prime, $V_2(d)$ is a *vector space.*) A typical example is the class of lines of the form

$$L_p = \{(x,y) : y = x + p, x \in Z_d\} \ , \tag{2.4}$$

where the addition is mod d, and one connects such lines with the matrix examples in [7] by orienting the y-axis down. For example, when $d = 3$ and $p = 1$, L_1 can be represented by the ones in

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

We can also include "vertical" and "horizontal" sets of lines using L_p to denote $\{(x,y) : x = p\}$ or $\{(x,y) : y = p\}$.

By analogy with the Euclidean plane, two lines are called *parallel* if they do not intersect. For two lines in the same class, $L_p \cap L_q = \phi$ if $p \neq q$, and it is easy to confirm the following result.

Lemma 1 *$\{L_p : 0 \leq p < d\}$ is a partition of $V_2(d)$ by a set of d mutually parallel lines.*

Note that we haven't defined lines using the more general formula $ax + by + c = 0$. This is because we are not assuming that d is a prime, and thus we cannot use the properties of an algebraic field which guarantee multiplicative inverses of non-zero elements.

With this notation in hand, we can describe the pattern of non-zero entries in a generalized *circulant* density as developed in [7]. Let p denote a permutation of Z_d, with the proviso that $p(0) = 0$. Define the non-zero entries of $B_p(j,k)$ by the line

$$L_p(j,k) = \{(x + p(j), x + p(k)) : x \in Z_d\} \ , \tag{2.5}$$

and note that $B_p^t(j,k) = B_p(k,j)$ (When p is the identity permutation, we suppress the subscript.) Then M_p itself is defined in terms of Dirac notation and the $L_p(j,k)$ as

$$M_p = \sum_{j,k} \left[\sum_{x=0}^{d-1} |j\rangle \langle k| \otimes |p(j) + x\rangle \langle p(k) + x| \right] = \sum_x I_p(x) \ , \tag{2.6}$$

where $I_p(x) = \sum_{j,k} |j\rangle \langle k| \otimes |p(j) + x\rangle \langle p(k) + x|$.

As an example, let $d = 3$ and let p denote the identity permutation. Using x_k to denote an entry of one when $x = k$ and dots for entries of zero, the resulting M matrix is

$$\begin{pmatrix}
x_0 & \cdot & \cdot & \cdot & x_0 & \cdot & \cdot & \cdot & x_0 \\
\cdot & x_1 & \cdot & \cdot & \cdot & x_1 & x_1 & \cdot & \cdot \\
\cdot & \cdot & x_2 & x_2 & \cdot & \cdot & \cdot & x_2 & \cdot \\
\cdot & \cdot & x_2 & x_2 & \cdot & \cdot & \cdot & x_2 & \cdot \\
x_0 & \cdot & \cdot & \cdot & x_0 & \cdot & \cdot & \cdot & x_0 \\
\cdot & x_1 & \cdot & \cdot & \cdot & x_1 & x_1 & \cdot & \cdot \\
\cdot & x_1 & \cdot & \cdot & \cdot & x_1 & x_1 & \cdot & \cdot \\
\cdot & \cdot & x_2 & x_2 & \cdot & \cdot & \cdot & x_2 & \cdot \\
x_0 & \cdot & \cdot & \cdot & x_0 & \cdot & \cdot & \cdot & x_0
\end{pmatrix} .$$

Notice in particular the arrangement of the non-zero entries in the different 3×3 blocks: in each $B(j, k)$ there is precisely one point of support associated with each x_k.

In confirming the properties of a putative density ρ, it is easy to check the trace one and the Hermitian conditions. What is harder is checking that ρ is positive semidefinite. One of the points of the present discussion is that if ρ has support in support(M_p), then that difficulty is reduced by the following observation. Representing a d^2 vector v in Dirac notation as $\sum_{j,k} v_{jk} |j\rangle |k\rangle$, it is easy to confirm that the entries of ρ are partitioned into disjoint sets indexed by x in the expression:

$$\langle v| \rho |v\rangle = \sum_x \sum_{j,k} \overline{v}_{j(x+p(j))} \rho_{j(x+p(j)),k(x+p(k))} v_{k(x+p(k))} \ . \tag{2.7}$$

It is also easy to check that the components of v are partitioned into classes indexed by x, and thus one can check that ρ is positive semidefinite by checking that ρ restricted to each of the $I_p(x)$ is positive semidefinite. This means one is checking d $d \times d$ matrices rather than one $d^2 \times d^2$ matrix.

That same feature simplifies checking the PPT property, as was established in [7] and [10].

Theorem 1 *Let p denote a permutation of Z_d with $p(0) = 0$. Let M_p be defined as in (2.6). Then M_p is the sum of the disjoint matrices $\{I_p(x) : x \in Z_d\}$ and for each (j, k) and each x there is exactly one index in support($B_p(j, k) \cap I_p(x)$). If ρ is a density with support(ρ) $\subset$ support(M_p), then ρ is* PPT *if and only if ρ restricted to $I_{-p}(y)$ is positive semidefinite for each y.*

Proof: The third sentence follows from the definitions. For the last assertion, let ρ^τ denote the partial transposition of ρ so that

$$\rho^\tau = \sum_{j,k} \sum_x |j\rangle |x + p(k)\rangle \rho_{j(x+p(j)),k(x+p(k))} \langle k| \langle x + p(j)| \ .$$

Substitute $x = y - p(j) - p(k)$ and reorder the summations:

$$\rho^\tau = \sum_y \sum_{j,k} |j\rangle |y - p(j)\rangle \rho_{j(y-p(k)),k(y-p(j))} \langle k| \langle x - p(k)| \ .$$

We see that the entries of ρ are again partitioned into disjoint sets indexed by y, and the earlier discussion applies, using the permutation $-p$, and completing the proof. $\square$

The 9×9 example above illustrates the idea. In tensor indexing, one of the three 3×3 matrices of a density ρ and one of the 3×3 matrices of ρ^τ that one would check for positive semidefiteness are

$$\rho : \begin{pmatrix} \rho_{00,00} & \rho_{00,11} & \rho_{00,22} \\ \rho_{11,00} & \rho_{11,11} & \rho_{11,22} \\ \rho_{22,00} & \rho_{22,11} & \rho_{22,22} \end{pmatrix} \qquad \rho^\tau : \begin{pmatrix} \rho_{00,00} & \rho_{02,10} & \rho_{01,20} \\ \rho_{10,02} & \rho_{12,12} & \rho_{12,20} \\ \rho_{20,01} & \rho_{20,12} & \rho_{21,21} \end{pmatrix} .$$

A useful necessary and sufficient condition to verify ρ is positive semidefinite is that the principal leading minors are non-negative. We leave it to the reader to write out the other submatrices for ρ and its partial transpose.

In the preceding discussion we used addition of indices in the context of Z_d. When d is the power of a prime, we have another alternative, and that is to use the Galois field $GF(p^n)$. For example when $d = 4 = 2^2$ we could have defined the four parallel lines (right-side up) as

$$\begin{pmatrix} \lambda+1 & \lambda & 1 & 0 \\ \lambda & \lambda+1 & 0 & 1 \\ 1 & 0 & \lambda+1 & \lambda \\ 0 & 1 & \lambda & \lambda+1 \end{pmatrix} ,$$

where $GF(2^2)$ is the set $\{0, 1, \lambda, \lambda+1\}$ and the table above actually defines addition. (Multiplication uses $\lambda^2 = \lambda+1$ and the usual properties of a field.). Since our only algebraic requirement so far is that addition be commutative, we could have used this different set of scalars in the prime power case. With the appropriate notation to index rows and columns, this gives an example of a $d = 4$ pattern that generalizes the circulant notation and that is not included in the appendix of [7]. The proof of Theorem (2.1) then goes through unchanged.

3 Generalized spin matrices and separability

The PPT condition is a necessary condition for separability and is expressed in terms of the components of a density in the computational basis. Using a generalization of the Pauli spin matrices, one can obtain a sufficient condition for separability of a density in terms of the coefficients of a particular orthogonal family of unitary matrices. An accessible reference is [18], and since the geometry of the support of the densities considered in this paper make them amenable to this approach, we summarize the salient points here. In [9] and [10] this family of matrices is used to define entangled projections, and the papers analyze the convex hull of those projections.

Let $\widehat{S} = \{S_{j,k} : 0 \leq j, k < d\}$ be defined by

$$S_{j,k} = \sum_{m=0}^{d-1} \eta^{jm} \left|m\right\rangle \left\langle m+k\right| \ , \tag{3.1}$$

where $\eta = e^{2\pi i/d}$. One can interpret these matrices as discrete Fourier transforms of the computational basis matrices $\left|m\right\rangle \left\langle m+k\right|$, a feature that manifests itself in various applications. One always has S_{00} equal to the identity matrix. When $d = 2$, $S_{10} = \sigma_z$, $S_{01} = \sigma_x$, and $S_{11} = i\sigma_y$ in terms of the usual Pauli spin matrices. That accounts for also calling them generalized Pauli matrices, and for historical reasons they are also known as (discrete) Weyl-Heisenberg matrices or, possibly more accurately, as the discrete Weyl matrices [9].

Two useful properties of these matrices are:

$$S_{j,k} S_{u,v} = \eta^{ku} S_{j+u,k+v}, \qquad (S_{j,k})^{\dagger} = \eta^{jk} S_{-j,-k} = S_{j,k}^{-1} \ . \tag{3.2}$$

Using the trace norm as an inner product, $\langle A \, | B \rangle = Tr \left(A^{\dagger} B \right)$, it follows that $\widehat{S}$ is an orthogonal family of unitary matrices. As such, $\widehat{S}$ is a basis for the space of $d \times d$ matrices, and a density can be written in this basis as

$$\rho = \frac{1}{d} \left[\sum_{j,k} s_{j,k} S_{j,k} \right] \ , \tag{3.3}$$

where $s_{0,0} = 1$ and $s_{j,k} = Tr \left[S_{j,k}^{\dagger} \rho \right]$. From earlier work we have the following result.

Theorem 2 *[18] If ρ is a bipartite density and $S_{u,v}$ denotes the tensor product $S_{u_1,v_1} \otimes S_{u_2,v_2}$, then a sufficient condition for ρ to be separable is that $\sum_{u,v} |s_{u,v}| \leq 2$, where $s_{u,v}$ is the coefficient of $S_{u,v}$ in the spin representation of ρ.* □

This is a relatively strong condition, although it is shown in [6] that the condition is sharp for certain families of densities with $d = 2^n$. The relevance here is that we can use the ideas behind the proof of this theorem and obtain sufficient conditions for separability for certain families of PPT circulant densities.

To see the connection, let p denote the identity permutation. Then substituting $m = u$, $n = m + t$ and $v = m + k$ we can rewrite M as

$$\begin{aligned} M &= \sum_{u,v} \left[\sum_{t=0}^{d-1} |u\rangle \langle v| \otimes |u+t\rangle \langle v+t| \right] \\ &= \sum_{k} \sum_{m} \sum_{n} |m\rangle \langle m+k| \otimes |n\rangle \langle n+k| \\ &= \sum_{k} S_{0,k} \otimes S_{0,k} \ . \end{aligned}$$

Thus the support of M equals the support of the sum of the tensor products $S_{0,k} \otimes S_{0,k}$. Since the support of $S_{j,k}$ is the same as the support of $S_{0,k}$, it is reasonable to assume that the spin matrix representation for a density with *support*(M) requires only tensor products of the form $S_{j_1,k} \otimes S_{j_2,k}$. That is indeed the case, and we skip the easy verification that the other spin coefficients equal zero.

When the permutation p is not the identity, a similar analysis can be made that requires some additional notation, but no new concepts. We defer that discussion to the Appendix and stay with the assumption that p is the identity permutation.

The next thing to notice is that the main diagonal of M is disjoint from any $S_{j_1,k} \otimes S_{j_2,k}$ with $k \neq 0$. Put another way, if ρ_D denotes the diagonal of a density ρ with support(M), then

$$\rho - \rho_D = \frac{1}{d^2} \sum_{k \neq 0} \sum_{j_1, j_2} s_{j_1 k, j_2 k} S_{j_1,k} \otimes S_{j_2,k} \ . \tag{3.4}$$

Our strategy is to express the spin coefficients in terms of the computational basis entries of ρ and the spin matrices themselves in terms of projections. In certain cases we can then write ρ as a sum of tensor products of projections with non-negative coefficients – and that satisfies the definition of separability. To be effective we require that d be prime power and for computational simplicity we assume that d itself is prime.

We provide the calculations in the Appendix and record here the basic structural result.

Theorem 3 *Suppose d is prime and support(ρ) is contained in support(M) as defined in (2.6). Then if ρ_D denotes the diagonal of ρ, there are rank one projections $P_{a,1}(m)$ such that*

$$\rho - \rho_D = \sum_{a_1,a_2=0}^{d-1} \sum_{m_1,m_2=0}^{d-1} P_{a_1,1}(m_1) \otimes P_{a_2,1}(m_2)\, C(a,m) \ , \tag{3.5}$$

where each $C(a,m)$ is real and $d^2C(a,m)$ equals

$$\sum_{k\neq 0,n_1,n_2} \eta^{-\binom{k}{2}(a_1+a_2)-k(m_1+m_2)-k(a_1n_1+a_2n_2)} \rho_{n_1n_2,(n_1+k)(n_2+k)} \ . \tag{3.6}$$

4 First application of the structural result

Equations (3.5) and (3.6) look a bit daunting, but in special cases they simplify quite nicely. Specifically, assume that $\rho_{n_1n_2,(n_1+k)(n_2+k)}$depends only on $r = n_2 - n_1$:

$$\rho_{n_1(n_1+r),(n_1+k)(n_1+r+k)} = c_r \ . \tag{4.1}$$

Then $d^2C(a,m)$ equals

$$\begin{aligned} & \sum_r c_r \sum_{k\neq 0} \eta^{-\binom{k}{2}(a_1+a_2)-k(m_1+m_2+a_2r)} \sum_{n_1} \eta^{-n_1(k(a_1+a_2))} && (4.2) \\ = \ & d\delta(a_1,-a_2) \sum_r c_r \sum_{k\neq 0} \eta^{-k(m_1+m_2-ra_1)} \\ = \ & d\delta(a_1,-a_2) \sum_r c_r \left[d\delta(m_1+m_2, ra_1) - 1\right] \ . && (4.3) \end{aligned}$$

4.1 A special case

As an example, assume that $c_r = 0$ for $r \neq 0$:

$$\rho_{n_1n_2,(n_1+k)(n_2+k)} = c\delta(n_1,n_2) \ .$$

Then

$$\rho = \rho_D + c \sum_n \sum_{k\neq 0} |n\rangle |n\rangle \langle n+k| \langle n+k| \ ,$$

so the support of ρ is on the diagonal and on $I(0)$, in the notation above. (Recall that we have assumed d is prime.) We find that

$$C(a,m) = \frac{c}{d}\delta(a_1+a_2,0)\left[d\delta(m_1+m_2,0) - 1\right] \ .$$

Substituting this in (3.5) gives

$$\begin{aligned}\rho &= \rho_D - \frac{c}{d}\sum_{a_1=0}^{d-1}\sum_{m_1,m_2}^{d-1} P_{a_1,1}\left(m_1\right)\otimes P_{-a_1,1}\left(m_2\right) \\ &+c\sum_{a_1=0}^{d-1}\sum_{m_1=0}^{d-1} P_{a_1,1}\left(m_1\right)\otimes P_{-a_1,1}\left(-m_1\right)\ .\end{aligned} \tag{4.4}$$

If $c>0$, we can rewrite this using (6.2) to obtain

$$\rho = \rho_D - cI_d\otimes I_d + c\sum_{a_1=0}^{d-1}\sum_{m_1=0}^{d-1} P_{a_1,1}\left(m_1\right)\otimes P_{-a_1,1}\left(-m_1\right)\ . \tag{4.5}$$

Thus the density ρ will be separable provided the smallest entry in ρ_D is at least c.

Now suppose that $c<0$. Then we can rework (4.4) to obtain

$$\rho = \rho_D - |c|\left(d-1\right)I_d\otimes I_d + |c|\sum_{a_1}\sum_{m_1\neq -m_2} P_{a_1,1}\left(m_1\right)\otimes P_{-a_1,1}\left(m_2\right)\ , \tag{4.6}$$

and ρ is separable if the smallest entry in ρ_D is larger than $|c|\left(d-1\right)$.

4.1.1 Isotropic state (example 2 from [8])

In this example $c=\lambda/d$ and the diagonal entries are either $\lambda/d+\left(1-\lambda\right)/d^2$ or $\left(1-\lambda\right)/d^2$. Then a sufficient condition for separability is $\lambda\leq 1/\left(1+d\right)$, which also happens to be the PPT condition.

4.1.2 Werner density (example 1 from [8])

Suppose one starts with a density of the form

$$\rho = \sum_{j,k} b_{j,k}\left|jk\right\rangle\left\langle kj\right| + \sum_{j\neq k} c_{jk}\left|jk\right\rangle\left\langle jk\right|\ ,$$

so that the second expression on the right has only entries on the diagonal and the first term on the right includes all of the non-zero off-diagonal entries. For separability, it would suffice to prove either ρ or its partial transpose ρ^τ is separable, and it is convenient to work with the latter. Define

$$x_\pm = \frac{1}{d}\left[\frac{1-p}{d+1}\pm\frac{p}{d-1}\right]\ .$$

The assumption in [8] is that for $j\neq k$, $b_{j,k}=x_-$, and $b_{jj}=x_-+x_+$. The diagonal entries $c_{jk}=x_+$. If $x_-\geq 0$, the sufficient condition trivially holds and the density is separable. If $x_-<0$, the sufficient condition for separability from (4.6) leads to $p\leq 1/2$, which again is the PPT condition.

4.1.3 DiVincenzo et al example [17] (example 3 from [8])

The off-diagonal terms of ρ are $((c-b)/2)\,|jk\rangle\langle kj|$ in this example, while the diagonal terms are either $(b+c)/2$ or $a = 1/d - (b+c)(d-1)/2$. (There is a misprint for the latter value in [8].) Again, the notation suggests working with ρ^{τ} to put it into the notational context of this section. If $b < c$, we find the sufficient conditions for separability are q

$$0 \leq b \qquad \text{and} \qquad cd^2 + bd\,(d-2) \leq 2\ .$$

If $c < b$, one obtains $0 \leq c$ and $bd\,(d-1) \leq 1$. It is easy to check that these conditions are equivalent, so that b and c are non-negative in both cases and both of the other two conditions hold. As shown in [8], those were also the PPT conditions, so the separability analysis gives a stronger result than the PPT condition.

4.1.4 Horodecki example (example 4 from [8])

In this example, $d = 3$ and once again $n_1 = n_2$ in the notation above is a necessary condition for the support of ρ. $c = 2/21$, and the diagonal entries are either $\alpha/21$ or $(5-\alpha)/21$. Then separability is guaranteed by $2 \leq \alpha \leq 3$ while the PPT condition allows $2 \leq \alpha \leq 4$. The theory used here does not resolve the question of separability when $3 < \alpha \leq 4$, and it is known that in this case the state is actually entangled.

4.2 The general case

We assume the c_r's are real and define $s = \sum_r c_r$. If we substitute into (3.5), we can obtain

$$\rho = \rho_D - sI_d \otimes I_d + \sum_c c_r \sum_a \sum_m P_{a,1}(m) \otimes P_{-a,1}(ar - m)\ . \tag{4.7}$$

An easy case is when each of the c_r's is non-negative, since that gives

$$s \leq \min(\rho_{nk,nk})\ ,$$

as a sufficient condition for separability. It is interesting to note that for $d = 3$, if we have $\sqrt{\sum_k c_k^2} \leq \min(\rho_{nk,nk})$, then ρ satisfies the PPT condition and this is a weaker condition than the sufficient condition for separability.

As another special case, suppose that $c_0 < 0 \leq c_r$ for $r \neq 0$ and also that $s = 0$. Then following the usual approach we can write ρ as a sum of separable projections with non-negative weights and a term $\rho_D - d\,|c_0|\,I_d \otimes I_d$, giving the obvious sufficient condition.

4.2.1 Baumgartner, Hiesmayr and Narnhofer: [9], [10]

Define $|\Omega_{j,k}\rangle = S_{j,k} \otimes I_d \sum_u |u\rangle\,|u\rangle$ and the projection $\widetilde{P}_{j,k} = |\Omega_{j,k}\rangle\langle\Omega_{j,k}|$. The class of densities studied in [9] and [10] are defined by

$$\rho = \sum_{j,k} c_{j,k} \widetilde{P}_{j,k}\ , \tag{4.8}$$

where the constants are non-negative and sum to one. One finds that

$$\rho_{n(n+r),(n+k)(n+r+k)} = \frac{1}{d} \sum_j c_{j,r} \eta^{-jk} \ . \tag{4.9}$$

There is no dependence on n, and one calculates

$$C\left(a,m\right) = \frac{1}{d^2} \delta\left(a_1,-a_2\right) \sum_j \sum_r c_{j,r} \left[d\delta\left(a_1 r - j, m_1 + m_2\right) - 1 \right] \ . \tag{4.10}$$

In recent work on discrete Wigner functions, there is a connection between lines in phase space and projections – see for example [13] and [19] among many others. This motivated one of the examples in [9], and the general case is

$$c_{j,r} = \begin{cases} 1/d\,, & \text{if} \quad r = sj + t \\ 0\,, & \text{otherwise} \end{cases} \ ,$$

where s and t are fixed. The geometry is that one is defining a line in the index set, i.e. a discrete phase space. This includes horizontal lines, and vertical lines have to be treated separately. We then have $C\left(a,m\right)$ equals

$$\frac{1}{d^2} \delta\left(a_1,-a_2\right) \sum_j \frac{1}{d} \left[d\delta\left(j\left(a_1 s - 1\right), m_1 + m_2 - a_1 t\right) - 1 \right] \ .$$

When $a_1 s \neq 1$, there is exactly one value of j for which the δ–function equals 1 and thus $C\left(a,m\right) = 0$. If $s = 0$, this is true for all a and m, and ρ is diagonal and therefore separable. In the remaining cases, let $a_1 = a_s \equiv s^{-1}$, so that $C\left(a,m\right)$ equals

$$\frac{1}{d^2} \delta\left(a_1, s^{-1}\right) \delta\left(a_2, -s^{-1}\right) \left[-1 + \sum_j \delta\left(ts^{-1}, m_1 + m_2\right) \right] \ .$$

We find

$$\rho = \rho_D - \frac{1}{d^2} I_d \otimes I_d + \frac{1}{d} \sum_m P_{a_s,1}\left(m\right) \otimes P_{-a_s,1}\left(a_s t - m\right) \ .$$

Since the diagonal entries are $\rho_{n(n+r),n(n+r)} = \frac{1}{d} \sum c_{j,r} = \frac{1}{d^2}$, it follows that these densities are separable. From properties developed in the Appendix, one can also check that they are rank d projections, as noted in [9].

It is known that the normalized identity is contained in an open set of separable densities. We can observe that property in this context by considering parameterized segments of the form

$$\rho\left(t\right) = \frac{1-t}{d^2} I_{d^2} + t\rho \ ,$$

where ρ is defined by (4.8). We will show that if $t \leq t_2 = 1/\left(1+d\right)$ then $\rho\left(t\right)$ is separable. That same bound holds for Werner densities in the bipartite case, and the bound $t_n = 1/\left(1+d^{n-1}\right)$ works for multipartite Werner densities [20]. The obvious conjecture is that t_n works for the multipartite versions of (4.8).

The proof is an easy application of the structure result. Ignoring terms with non-negative coefficients, look at the remaining part of ρ :

$$\rho_D - \frac{1}{d^2} \sum_a \sum_{m_1,m_2} P_{a,1}(m_1) \otimes P_{-a,1}(m_2) \sum_{j,r} c_{j,r} = \rho_D - \frac{1}{d} I_{d^2} \ .$$

The usual requirement takes the form

$$\frac{1-t}{d^2} + \frac{t}{d} \sum_j c_{j,r} \geq \frac{t}{d} \ ,$$

so that for all r

$$t \leq 1/ \left(1 + d - d \sum_j c_{j,r} \right) \ .$$

This verifies the sufficiency of $t \leq t_2$ for separability.

Finally, we illustrate the structural results for one other example from [9] where $d = 3$. α and β are non-negative parameters and in that notation

$$\rho = \frac{1-\alpha-\beta}{9} I_{d^2} + \alpha \widetilde{P}_{1,0} + \beta \widetilde{P}_{2,0} \ .$$

Putting this in the notation above, $t = \alpha + \beta$, $c_{1,0} = \alpha/t$ and $c_{2,0} = \beta/t$. Then the sufficient condition for separability is $t = \alpha + \beta \leq \frac{1}{4}$. Equation(50) in [9] provides a necessary and sufficient condition for ρ to be PPT, and it is easy to confirm the condition for separability satisfies that constraint.

5 A class of circulant densities with product entries

In the examples above, the entries of ρ in (4.1) did not depend on n. In this section they do, but in a very structured manner:

$$\rho_{n(n+r),(n+k)(n+r+k)} = x(n,r) \overline{x}(n+k,r) \ .$$

This seems to be a novel set of examples that is amenable to analysis via the structure results. The key is that

$$\eta^{-\binom{k}{2}(a_1+a_2)-k(m_1+m_2)-kn(a_1+a_2)-kra_2}$$

can be written as

$$\eta^{\binom{n}{2}(a_1+a_2)+n(m_1+m_2+ra_2)} \eta^{-\binom{n+k}{2}(a_1+a_2)-(n+k)(m_1+m_2+ra_2)} \ .$$

This meshes well with $x(n,r)\overline{x}(n+k,r)$ to give $d^2 C(a,m) + \sum_n \sum_r |x(n,r)|^2$ equal to

$$\sum_r \left| \sum_n x(n,r) \eta^{\binom{n}{2}(a_1+a_2)+n(m_1+m_2+ra_2)} \right|^2 \ .$$

Define

$$\widetilde{A}\left(r,b,t\right)=\left|\frac{1}{d}\sum_{n}x\left(n,r\right)\eta^{\binom{n}{2}b+nt}\right|^{2}$$

and

$$Q\left(r,b,t\right)=\sum_{b=a_1+a_2}\ \sum_{t=m_1+m_2+ra_2}P_{a_1,1}\left(m_1\right)\otimes P_{a_2,1}\left(m_2\right)$$

so that up to normalization the $Q's$ are separable. Then the separable representation is

$$\rho=\rho_D-\sum_{n,r}\left|x\left(n,r\right)\right|^2\frac{1}{d^2}\sum_{a_1,a_2}I_d\otimes I_d+\sum_{r,b,t}\widetilde{A}\left(r,b,t\right)Q\left(r,b,t\right)$$

and it follows that a sufficient condition for separability is

$$\min_{m,n}\left(\rho_{mn,mn}\right)\geq\sum_{n,r}\left|x\left(n,r\right)\right|^2\ .$$

Denoting one of these densities as ρ_x we can define the line segment

$$\rho_x\left(t\right)=\frac{1-t}{d^2}I_{d^2}+t\rho_x$$

and obtain a sufficient condition for separability

$$t\left(1+d^2\left(\sum_{n,r}\left|x\left(n,r\right)\right|^2-\min_{m,n}\left(\rho_{mn,mn}\right)\right)\right)\leq 1\ .$$

We omit the details.

6 Appendix: technical details of the proof of Theorem 3.2

To obtain the representation above of $\rho-\rho_D$, we first need to relate projections to the spin matrices, and here is where we restrict the discussion by assuming that d is a prime. Fix an index (j,k) and define

$$P_{j,k}(r)=\frac{1}{d}\sum_{m}\eta^{mr}\left(S_{j,k}\right)^m\ . \tag{6.1}$$

Using the properties above, it is straightforward to check that

$$P_{j,k}(r)P_{j,k}(s)=\delta\left(r,s\right)P_{j,k}(r)\ ,$$

and that the family $\{P_{j,k}\left(r\right):0\leq r<d\}$ is an orthogonal family of rank one projections. (As an aside, for the reader interested in *mutually unbiased bases,* this is one way to construct them when the dimension of the space is a prime power. See [14].) Note that one could interpret (6.1) as another discrete Fourier transform of matrices, so that one should be able to compute the spin matrices from the associated projections. In fact the formula is

$$\left(\eta^r S_{a,1}\right)^t=\sum_{m}\eta^{-mt}P_{a,1}\left(m+r\right)\ , \tag{6.2}$$

and this is nothing more than the spectral decomposition of $(\eta^r S_{a,1})^t$. When $t = 0$ the left side is interpreted as the identity.

Now using (3.2) it is easy to confirm that $(S_{a,1})^k = \eta^{a\binom{k}{2}} S_{ak,k}$, provided we interpret the binomial coefficient as 0 if $k = 0$ or $k = 1$. Since d is prime, for $k \neq 0$ and given j we can define $a = jk^{-1}$ so that

$$S_{j,k} = \eta^{-a\binom{k}{2}} \sum_m \eta^{-mk} P_{a,1}(m) \ , \tag{6.3}$$

and that completes the first step.

For the second step we use the structure of the support of ρ to write

$$\rho - \rho_D = \sum_{m \neq v} \left[\sum_{t=0}^{d-1} \rho_{m(m+t),v(v+t)} \left|m\right\rangle \left\langle v\right| \otimes \left|m+t\right\rangle \left\langle v+t\right| \right]$$

$$= \sum_{k\neq 0} \sum_{n_1} \sum_{n_2} \rho_{n_1 n_2,(n_1+k)(n_2+k)} \left|n_1\right\rangle \left\langle n_1+k\right| \otimes \left|n_2\right\rangle \left\langle n_2+k\right| \ .$$

Comparing this with (3.4) we conclude that the constants $\rho_{n_1 n_2,(n_1+k)(n_2+k)}$ are transforms of the $s_{j_1 k, j_2 k}$,

$$\rho_{n_1 n_2,(n_1+k)(n_2+k)} = \frac{1}{d^2} \sum_{j_1 \cdot j_2} \eta^{j_1 n_1} \eta^{j_2 n_2} s_{j_1 k, j_2 k} \ ,$$

and thus that

$$s_{j_1 k, j_2 k} = \sum_{n_1} \sum_{n_2} \eta^{-n_1 j_1 - n_2 j_2} \rho_{n_1 n_2,(n_1+k)(n_2+k)} \ . \tag{6.4}$$

Substituting (6.4) and (6.2) into (3.4) gives Theorem 3.2, up to the confirmation that $C(a,m)$ is real. That last fact follows readily enough by taking the complex conjugate of $C(a,m)$, substituting $-k$ for k and then making some additional notational changes to obtain $C(a,m)$.

Finally, we show that assuming the permutation p is not the identity only complicates the notation without generalizing the discussion. Suppose then that the permutation p defining M_p is not the identity. Let σ denote the inverse permutation p^{-1}. Make the substitutions $p(u) = m$, $n = m + t$, and $p(v) = m + k$ in the expression for M_p to obtain

$$\begin{aligned} M_p &= \sum_t \sum_u \sum_v \left|u\right\rangle \left\langle v\right| \otimes \left|p(u)+t\right\rangle \left\langle p(v)+t\right| \\ &= \sum_k \sum_m \left|\sigma(m)\right\rangle \left\langle \sigma(m+k)\right| \sum_n \left|n\right\rangle \left\langle n+k\right| \\ &= \sum_k S_{0,k}(\sigma) S_{0,k} \end{aligned}$$

where $S_{j,k}(\sigma) = \sum_m \eta^{jm} \left|\sigma(m)\right\rangle \left\langle \sigma(m+k)\right|$. Introducing the permutation σ in the definition of the spin matrices is equivalent to a relabeling of the computational basis in the first space and the class $\widehat{S}(\sigma)$ should have the same properties as $\widehat{S}$. It is easy to check that is indeed the case, and thus the only difference that one has in (3.5) is that the projections $P_{a_1,1}(m_1)$ should have a σ added to the notation. Thus, for all practical purposes in studying classes of examples, we can simply assume that p is the identity.

Acknowledgement

DC research supported in part by the Polish Ministry of Science and Education Grant 3004/B/H03/2007/33. AP research supported in part by NSF Grant 0605069.

References

[1] Michael A. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, (2000).

[2] Artur Ekert, “From quantum code-making to quantum code-breaking”, ArXiv: quant-ph/9703035, (1997).

[3] Asher Peres, “Separability criterion for density matrices”, Phys. Rev. Lett. **77**, 1413–1414, (1966).

[4] Michał Horodecki, Paweł Hordecki, Ryszard Horodecki, ”Separability of Mixed States: Necessary and Sufficient Conditions”, Phys. Lett. A **223**, 1, (1996). See also ArXiv: quant-ph/9605038, (1996).

[5] Paweł Horodecki, ”Separability criterion and inseparable mixed states with positive partial transposition”, Phys. Lett. A **232**, 333 (1997).

[6] Arthur O. Pittenger, Morton H. Rubin, “Complete separability and Fourier representations of n - qubit states,” Phys. Rev. A **62**, 042306, (2000). (ArXiv: quant-ph/9912116).

[7] Dariusz Chruściński, Andrzej Kossakowski, “On circulant states with positive partial transform,” Phys. Rev. A **76**, 032308 (2007).

[8] Dariusz Chruściński, Andrzej Kossakowski, “Class of positive partial transformation states”, Phys. Rev. A **74**, 022308, (2006).

[9] Bernhard Baumgartner, Beatrix C. Hiesmayr, Heide Narnhofer, “The state space for two qutrits has a phase space structure at its core,” Phys. Rev. A **74**, 032327 (2006).

[10] Bernhard Baumgartner, Beatrix C. Hiesmayr, Heide Narnhofer, “A special simplex in the state space for entangled qudits,” J. Phys. A: Math. Theor. **40**, 7919–7938 (2007).

[11] Bernhard Baumgartner, Beatrix C. Hiesmayr, Heide Narnhofer, “The geometry of bipartite qutrits including bound entanglement,” Phys. Lett. A **372**, 2190–2195, (2008) (arXiv:0705.1403).

[12] Daniel I. Fivel, ”Remarkable Phase Oscillations Appearing in the Lattice Dynamics of Einstein-Podolsky-Rosen States”, Phys. Rev. Lett. **74**, 835 (1995).

[13] Kathleen S. Gibbons, Matthew J. Hoffman, William K. Wootters, “Discrete space based on finite fields,” Phys. Rev. A **70**, 062101 (2004).

[14] Arthur O. Pittenger, Morton H. Rubin, “Mutually unbiased bases, generalized spin matrices and separability,” Linear Alg. and Appl. **390**, 255, (2004). (ArXiv: quant-ph/0308142).

[15] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, R. Tarrach, "Separability and distilability is composite quantum systems – a primer," J. Mod. Optics **47**, 2841 (2000).

[16] Ryszard Horodecki, Paweł Hordecki, Michał Horodecki, Karol Horodecki, "Quatum entanglement", ArXiv:0702.225, (2007).

[17] David P. DiVincenzo, Peter Shor, John A. Smolin, Barbara M. Terhal, Ashish V. Thapliyal, "Evidence for bound entangled states with negative partial transpose," Phys. Rev. A **61**, 062312 (2000), (quant-ph/9910026).

[18] Arthur O. Pittenger, Morton H. Rubin, "Convexity and the separability problem of quantum mechanical density matrices," Linear Alg. and Appl. **346**, 47–71, (2002) (ArXiv: quant-ph/0103038).

[19] Arthur O. Pittenger, Morton H. Rubin, "Wigner functions and separability for finite systems," J. Phys. A: Math Gen. **38**, 6005–6036 (2005).

[20] Arthur O. Pittenger, Morton H. Rubin, "Note on separablity of Werner states in arbitrary dimensions," Optics Comm. **179**, 447 (2000).