A special simplex in the state space for entangled qudits

A special simplex in the state space for entangled qudits

Bernhard Baumgartner, Beatrix Hiesmayr and Heide Narnhofer

Institut für Theoretische Physik, Universität Wien, Boltzmanngasse 5, A-1090 Vienna, Austria

E-mail: Bernhard.Baumgartner@univie.ac.at, Beatrix.Hiesmayr@univie.ac.at and Heide.Narnhofer@univie.ac.at

Abstract

The focus is on two parties with Hilbert spaces of dimension d, i.e. 'qudits'. In the state space of these two possibly entangled qudits an analogue to the well-known tetrahedron with the four qubit Bell states at the vertices is presented. The simplex analogue to this magic tetrahedron includes mixed states. Each of these states appears to each of the two parties as the maximally mixed state. Some studies on these states are performed, and special elements of this set are identified. A large number of them are included in the chosen simplex which fits exactly into conditions needed for teleportation and other applications. Its rich symmetry—related to that of a classical phase space—helps to study entanglement, to construct witnesses and perform partial transpositions. This simplex has been explored in detail for $d = 3$. In this paper, the mathematical background and extensions to arbitrary dimensions are analysed.

PACS numbers: 03.67.Mn, 03.67.Hk

1. Introduction

Entanglement, a non-classical essential feature of quantum theory, was first recognized in 1935 in connection with paradoxes. Studying it with mathematical accuracy began in 1964, introducing the Bell states. With the new era of proposed applications in teleportation, quantum computing and quantum communication [BW92, B93], it became necessary to use the Bell basis of four 'magic Bell states' describing the qubit. Now, in the process of extending the concepts to systems with Hilbert spaces of dimension greater than 2, one faces the practical task of defining analogous sets of states. The presentation of all possible ideal schemes in [W01] reveals a large field of structures that we can choose from.

One item that fits into those schemes is presented in this paper. We were motivated to study it mainly out of curiosity on the theoretical side. It has a rich structure of symmetries

which enable deep concrete investigations on the location of the border between entangled and separable states. (Compare [VW00].) It would be no surprise if its mathematical beauty was reflected in practical application.

In this paper, we focus on two parties with Hilbert spaces of dimension d, i.e. 'qudits'. For these two possibly entangled qudits we construct an analogue to the well-known tetrahedron with four mutually orthogonal Bell states at the vertices [HH96]. This magic tetrahedron includes mixed states, inside lies an octahedron of separable states. Each of these states appears to each of the two parties as the maximally mixed state of its qubit. Considering the duality between maps and states [ZB04] these states are related to bistochastic maps [AU82] (but only for bipartite systems). We make some remarks on this duality in the concluding section 9. Now, also for the qudits one might prefer states with this property. We call it *locally maximally mixed*. For qubits, any such LMM state can be considered as an element of the tetrahedron [BNT02], but for $d \geqslant 3$ the analogue statement is no longer true. So we perform some studies on LMM states in section 2 and identify special elements of this set. In the following sections we then recognize a large number of these special states as included in our chosen subspace of LMM.

For the qudit pair we define and study a special simplex ('generalized tetrahedron') $\mathcal{W}$. It has d^2 pure states at the vertices, with specified relations between them. Its rich symmetry helps us to study entanglement, and it fits exactly into the conditions needed for teleportation and dense coding as stated in [W01]. We explored this magic simplex for $d = 3$ [BHN06]. In this paper, we bring a detailed analysis of the mathematical background. This enables us to extend the study to higher dimensions.

Choose some basis $\{|s\rangle\}$ in each factor and define a 'Bell state', i.e. a maximally entangled pure state, in the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ with the vector

$$|\Omega_{0,0}\rangle = \frac{1}{\sqrt{d}} \sum_s |s\rangle \otimes |s\rangle. \tag{1}$$

On the first factor in the tensorial product we consider actions of the *Weyl operators* defined as

$$\check{W}_{k,\ell}|s\rangle = w^{k(s-\ell)}|s-\ell\rangle, \tag{2}$$

$$w = e^{2\pi i/d}, \tag{3}$$

with the identity

$$|s - \ell\rangle \equiv |s - \ell + d\rangle. \tag{4}$$

The actions of the Weyl operators produce mutually orthogonal Bell state vectors

$$|\Omega_{k,\ell}\rangle = (\check{W}_{k,\ell} \otimes \mathbb{1})|\Omega_{0,0}\rangle. \tag{5}$$

The set of index pairs (k, ℓ) is a *finite discrete classical phase space*: ℓ denotes the values for the coordinate in 'x-space', k the values of the 'momentum'. Remarks on the relation to the physics of the Heisenberg–Weyl quantization we have made for $d = 3$; details on the mathematics follow in section 4. To each point in this space is associated the density matrix for the Bell state, the projection operator

$$P_{k,\ell} = |\Omega_{k,\ell}\rangle\langle\Omega_{k,\ell}|. \tag{6}$$

The mixtures of these pure states form our object of interest, the *magic simplex*

$$\mathcal{W} = \left\{ \sum c_{k,\ell} P_{k,\ell} \,\middle|\, c_{k,\ell} \geqslant 0, \sum c_{k,\ell} = 1 \right\}. \tag{7}$$

As a geometrical object $\mathcal{W}$ is located in a hyperplane of the d^2-dimensional Euclidean space $\left\{ A = \sum a_{k,\ell} P_{k,\ell} \,\middle|\, a_{k,\ell} \in \mathbb{R} \right\}$ equipped with a distance relation $\sqrt{\text{Tr}(A - B)^2}$. Specifying the origin $A = 0$, it is also equipped with the Hilbert–Schmidt norm $\sqrt{A^2}$, and the inner product $\text{Tr}(AB) = \sum a_{k,\ell} b_{k,\ell}$. All this is embedded in the d^4-dimensional Hilbert–Schmidt space of Hermitian $d^2 \times d^2$ matrices. We use this Euclidean geometry for ease of calculations.

The main goal in this paper is the exploration of the borders of *SEP*, i.e. the set of separable states. We find that the structure of the subset SEP $\cap$ $\mathcal{W}$, the analogue to the octahedron of bipartite qubits, is not quite simple. It is not a polytope; but a rather detailed study is enabled by the rich symmetry of the simplex $\mathcal{W}$. Using part of it, we easily determine first two polytopes giving an inner and an outer fence to the border of SEP. These results, among others, appear in sections 3 and 4.

Symmetry is then studied in detail in section 5. It also simplifies performing the partial transpositions of the states in $\mathcal{W}$. This is discussed in section 7. So we get a closer approximation to SEP $\cap$ $\mathcal{W}$ by studies on *PPT*, that is the set of density matrices remaining positive after partial transposition. Here we refer to the Peres criterion [P96] which implies that SEP is a subset of PPT. Furthermore, the partial transposition maps PPT $\cap$ $\mathcal{W}$ into PPT $\cap$ $\hat{\mathcal{W}}$, where $\hat{\mathcal{W}}$ is another convex subset of LMM, also defined in section 7. The partial transposition maps SEP onto itself, so the cases of bound entanglement detected in $\mathcal{W}$ are also cases for bound entanglement in $\hat{\mathcal{W}}$.

Last, but not least, the symmetry of $\mathcal{W}$ can be exploited as the symmetry of the set of witnesses [T00] needed there. Here, in section 6, we use the mathematics of convex cones and their duals. It helps to exactly determine the borderlines of SEP. This has been done in [BHN06] for $d = 3$. Extensions to studies for higher dimensions will follow (work in progress).

This study follows two aims. In the main task of investigations the special simplex is constructed and its symmetries are stated. Using these symmetries, some details in the structure concerning entanglement are explored. In following the second trail we check not to have overlooked anything: the symmetry group is maximal, the polytopes are optimal. The proofs of having 'best possible' results afford some mathematical subtlety. We present these subtle investigations in section 8.

Various mathematical branches are used: theories of numbers, groups, convex sets, matrices and Hilbert spaces. But only some basic facts are needed, to be found in any introduction or encyclopaedia, as [Sch86, V64, A42, W06]. One side effect, which unfortunately makes some pain, is the frequent switching of the mathematical points of view. Being too strict on the reference to the context would make notations cumbersome and difficult to follow. We try to avoid an overburdening with symbols. We refer, for example, to the states with the same letters as we use for the density matrices representing them. But we are strict on not confusing Hilbert space *vectors* with states. Big Greek letters denote elements of the total Hilbert space, small letters, mostly in the environment $|\,\rangle$, are used for elements of $\mathbb{C}^d$.

Moreover, we simplify the notations, omitting the sign for the tensor product concerning the two parties, and write, e.g., $|\varphi, s\rangle$ for an element of $\mathbb{C}^d \otimes \mathbb{C}^d$ instead of $|\varphi\rangle \otimes |s\rangle$. Our unitary operators U, V, W that occur in this work acting on the global Hilbert space are all of product form. They act locally as $\check{U}, \check{V}, \check{W}$ on the first factor, and as $\tilde{U}, \tilde{V}, \tilde{W}$ on the second factor. $U|\varphi, \psi\rangle = |\check{U}\varphi, \tilde{U}\psi\rangle$. Mostly $\tilde{U} = \mathbb{1}$, with exceptions in section 5.

2. LMM states

Elements of LMM are the states ρ on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^d \otimes \mathbb{C}^d$ which appear locally to each of the single parties as maximally mixed[1]. The partial trace in one factor gives the maximally mixed state ω on the other side:

$$\rho_A := \text{Tr}_B \rho = \omega_A := \frac{1}{d} \mathbb{1}_A, \qquad \rho_B := \text{Tr}_A \rho = \omega_B := \frac{1}{d} \mathbb{1}_B. \tag{8}$$

We identify special types of LMM states: its pure states, isotropic states, Werner states and maximally exposed elements of SEP $\cap$ LMM.

The pure LMM states for qubits are known as the 'Bell states'. We extend this naming to each one of the pure LMM states of qudits. The single Bell states for fixed d are all unitarily equivalent, involving local unitary transformations: Consider the pair Ω, Φ of Bell state vectors. For Schmidt decomposition, we choose a preferred basis $\{|s\rangle\}$ in $\mathcal{H}_B$. Then there are two different bases $|\psi_s\rangle$ and $|\varphi_s\rangle$ in $\mathcal{H}_A$, such that

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_s |\psi_s, s\rangle, \qquad |\Phi\rangle = \frac{1}{\sqrt{d}} \sum_s |\varphi_s, s\rangle. \tag{9}$$

$|\Omega\rangle$ is mapped to $|\Phi\rangle$ by extension of the local unitary operator

$$\check{U} = \sum_s |\varphi_s\rangle\langle\psi_s|. \tag{10}$$

Mixtures of a Bell state Ω with the global maximally mixed state

$$\omega = \frac{1}{d^2} \mathbb{1} \tag{11}$$

define the *isotropic states* $(1 - \alpha)\omega + \alpha|\Omega\rangle\langle\Omega|$. Again all the isotropic states with the same α are unitarily equivalent.

Other special LMM states are the lines of *Werner states*, related to the lines of isotropic states by *PT*, that is *Partial Transposition*. See [VW00] for the appropriate ranges of the parameters α and other details. They are also all equivalent. We need no special check of their belonging to LMM. There is the general fact:

Lemma 1. *The LMM property (8) is preserved under partial transposition.*

Proof. Equation (8) is equivalent to the statement that for each $\varphi \in \mathbb{C}^d$ and each basis $\{\psi_t\}$

$$\sum_t \langle\varphi, \psi_t|\rho|\varphi, \psi_t\rangle = \|\varphi\|^2/d. \tag{12}$$

We write this as $\text{Tr}\,\rho Q = \|\varphi\|^2/d$ with $Q := \sum_t |\varphi, \psi_t\rangle\langle\varphi, \psi_t|$. The PT operator in the Hilbert–Schmidt space is symmetric, i.e. $\text{Tr}(\text{PT}(\rho) \cdot Q) = \text{Tr}(\rho \cdot \text{PT}(Q))$. Calculation of PT is done in the preferred basis $|s\rangle$; the expansion $|\varphi\rangle = \sum_s \varphi_s |s\rangle$ gives

$$\text{PT}(Q) = \sum_{s,r,t} \varphi_s \varphi_r^* \text{PT}(|s, \psi_t\rangle\langle r, \psi_t|)$$
$$= \sum_{s,r,t} \varphi_s \varphi_r^* |r, \psi_t\rangle\langle s, \psi_t| = \sum_t |\hat{\varphi}, \psi_t\rangle\langle\hat{\varphi}, \psi_t|, \tag{13}$$

with $|\hat{\varphi}\rangle = \sum_r \varphi_r^* |r\rangle$. The complex conjugation does not change the norm and (12) holds for $\text{PT}(\rho)$. $\square$

---

[1] In the community working with operator algebras, such a maximally mixed state is known as tracial state.

The Werner states do not only have special symmetries, they have the property of attaining the minimal possible distance (see [GB02]) to the maximally mixed state ω when they are at the border between SEP and the entangled states. We conjecture that they are the only LMM states with this property. What we can show easily is the

Lemma 2. *If an LMM state at the border between PPT and non-PPT states has the minimal border distance to ω, which is $1/d\sqrt{d^2-1}$, then it is a Werner state.*

Proof. Performing PT on the density matrix ρ of this state we get a density matrix σ at the border of PPT $\cap$ LMM to non-positive matrices. The matrices with minimal distance at that border have the form $\sigma = (\mathbb{1} - P)/(d^2 - 1)$, with P being a projector belonging to a pure state. Pure LMM states are Bell states, so σ is isotropic and $\rho = \mathrm{PT}(\sigma)$ is a Werner state. The Euclidean distance squared is easily calculated as

$$\mathrm{Tr}(\rho - \omega)^2 = \mathrm{Tr}(\sigma - \omega)^2 = \mathrm{Tr}\,\sigma^2 - \frac{1}{d^2} = \frac{1}{d^2(d^2-1)}. \tag{14}$$

$\square$

$\mathcal{W}$ does not contain Werner states if $d \geqslant 3$, but $\hat{\mathcal{W}}$ does, see section 7.

A third kind of special LMM states appears in both $\mathcal{W}$ and $\hat{\mathcal{W}}$: the separable states with the largest possible distance between ω and SEP $\cap$ LMM.

Theorem 3. *The maximal distance of a $\sigma \in$ SEP $\cap$ LMM to ω is $\sqrt{d-1}/d$. It is attained if and only if the density matrix σ has the form*

$$\sigma = \frac{1}{d} \sum_s |\varphi_s, \psi_s\rangle\langle\varphi_s, \psi_s|, \tag{15}$$

where both φ_s and ψ_s are bases for $\mathbb{C}^d$.

Proof. The first condition, $\sigma \in$ SEP, is fulfilled iff σ can be represented as

$$\sum_\alpha \lambda_\alpha |\varphi_\alpha, \psi_\alpha\rangle\langle\varphi_\alpha, \psi_\alpha| \tag{16}$$

with $\lambda_\alpha > 0$, $\sum_\alpha \lambda_\alpha = 1$ and normed vectors $\varphi_\alpha, \psi_\alpha$.

The second condition, $\sigma \in$ LMM, implies that $\forall\varphi, \forall\psi$ with norm one

$$\langle\varphi, \psi|\sigma|\varphi, \psi\rangle \leqslant \sum_j \langle\varphi, \psi_j|\sigma|\varphi, \psi_j\rangle = \langle\varphi|\sigma_A|\varphi\rangle = \frac{1}{d}, \tag{17}$$

where we considered some basis ψ_j containing the given ψ. Applying (17) to the vectors appearing in (16) gives

$$\mathrm{Tr}\,\sigma^2 = \sum_\alpha \lambda_\alpha \langle\varphi_\alpha, \psi_\alpha|\sigma|\varphi_\alpha, \psi_\alpha\rangle \leqslant \sum_\alpha \lambda_\alpha \frac{1}{d} = \frac{1}{d}. \tag{18}$$

This proves the first statement about the maximal distance, since $\|\sigma - \omega\|^2 = \mathrm{Tr}\,\sigma^2 - 1/d^2$. To prove the second statement observe that the inequality (17) turns to an equality iff $\forall\psi^\perp$ with $\langle\psi^\perp|\psi\rangle = 0$ the equality $\langle\varphi, \psi^\perp|\sigma|\varphi, \psi^\perp\rangle = 0$ holds. The same is true with the roles of the two sides interchanged, that is $\forall\varphi^\perp$ with $\langle\varphi^\perp|\varphi\rangle = 0$ one has $\langle\varphi^\perp, \psi|\sigma|\varphi^\perp, \psi\rangle = 0$. So one can start diagonalizing the matrix σ. One begins with one pair of vectors appearing in (16), say $\alpha = 0$:

$$\sigma = \frac{1}{d}|\varphi_0, \psi_0\rangle\langle\varphi_0, \psi_0| + \frac{d-1}{d}\sigma_{d-1}. \tag{19}$$

The matrix σ_{d-1} is a normalized density matrix in the LMM $\cap$ SEP with *lower dimension*, acting on $\mathbb{C}^{d-1} \otimes \mathbb{C}^{d-1}$. This can easily be seen by $(d-1)\mathrm{Tr}_B\sigma_{d-1} = d\mathrm{Tr}_B\sigma - |\varphi_0\rangle\langle\varphi_0| = \mathbb{1}_A - |\varphi_0\rangle\langle\varphi_0| = (d-1)\mathbb{1}_{A,d-1}$ and $\langle\varphi^\perp, \psi^\perp|\sigma_{d-1}|\varphi^\perp, \psi^\perp\rangle = d/(d-1)\langle\varphi^\perp, \psi^\perp|\sigma|\varphi^\perp, \psi^\perp\rangle$. Now one may proceed inductively, expanding σ_{d-1} in the form (16)—generally with new vectors—diagonalizing $(d-1)\sigma_{d-1} = |\varphi_1, \psi_1\rangle\langle\varphi_1, \psi_1| + (d-2)\sigma_{d-2}$ and so on. $\qquad\square$

Each one of these maximally exposed SEP $\cap$ LMM states is in unique correspondence to a pair of bases in the Hilbert spaces of the parties and a one-to-one mapping between them. Each one can be represented as a mixture of d Bell states appearing in some $\mathcal{W}$. For example, one may use the bases characterizing σ as stated in theorem 3, to construct a simplex $\mathcal{W}$: put them into definition (1), $|\Omega_{0,0}\rangle = \frac{1}{\sqrt{d}} \sum_s |\varphi_s, \psi_s\rangle$, construct the $P_{k,0}$ and represent $\sigma = \sum_k P_{k,0}/d$. But this representation is not unique. More about this is presented in section 4. PT maps this set of maximally exposed states onto itself, so these states appear in $\hat{\mathcal{W}}$ also.

3. Subsets of LMM

Let us proceed and look at *subspaces* of LMM. Most important are the Bell states appearing in the chosen subspace. *Any* set of d^2 mutually orthogonal Bell states P_α—orthogonality of the Hilbert space vectors $\langle\Omega_\alpha|\Omega_\beta\rangle = \delta_{\alpha,\beta}$ is in this case equivalent to the orthogonality of the density matrices in the Euclidean space $\mathrm{Tr}\,P_\alpha P_\beta = \delta_{\alpha,\beta}$—spans a maximal simplex. Each Bell state comes with an optimal witness, a hyperplane B_α defined as $B_\alpha := \{\rho : \mathrm{Tr}\,\rho(P_\alpha - \mathbb{1}/d) = 0\}$. These d^2 hyperplanes B_α, together with the d^2 hyperplanes $A_\alpha := \{\rho : \mathrm{Tr}\,\rho P_\alpha = 0\}$ containing the faces of the simplex, define an *enclosure polytope*. Outside of it are only entangled states. The projectors P_α generate a maximal Abelian subalgebra of operators acting on $\mathcal{H}$. So these conditions alone bring already some insight, but they still allow for many different choices of an LMM subspace. They are not all equivalent. The geometric symmetry of the enclosure polytope, the same symmetry as that of the simplex, is deceptive: SEP must be inside, but the relations of its detailed geometry to the set of pure states in the chosen subspace depend on their algebraic relations. The single Bell states are equivalent, but already *pairs* of orthogonal Bell states fall into different classes of pairs if $d \geqslant 4$. Enter spectral theory: each class is characterized by the spectrum of the local unitary operators identified in (10) connecting the pair. Orthogonality of the Bell state vectors implies $\mathrm{Tr}\,U = 0$. Being interested only in the *intertwining relation*

$$U|\Omega\rangle\langle\Omega|U^\dagger = |\Phi\rangle\langle\Phi| \tag{20}$$

we are free to choose a phase factor for U such that one of its eigenvalues is equal to 1. The condition $\mathrm{Tr}\,U = 0$ specifies the rest of the spectrum only for qubits and qutrits. For $d \geqslant 4$ there are various possibilities, defining different classes of equivalent pairs: unitary or antiunitary local mappings of one pair onto the other can be applied to the interwiners U. So their spectra are either unchanged or complex conjugated and rotated. This characterizes the classes.

To choose *special sets* of Bell states an extra criterion which a theoretician likes to pose is that the intertwining operators form a unitary group, allowing for multiplication of any two of them. This gives a strong restriction on their spectra. Enter number theory:

Theorem 4. *If $\{U^n\}$ is a group of intertwiners between mutually orthogonal Bell states, then, with an appropriately chosen overall phase factor, U has eigenvalues $\mathrm{e}^{2\pi\mathrm{i}m/b}$, where $0 \leqslant m \leqslant b - 1$, and b is either a divisor of d or equal to d. Considering intertwiners acting as $U = \check{U} \otimes \mathbb{1}$ on $\mathcal{H}_A$ only, the multiplicity of each eigenvalue of $\check{U}$ is d/b.*

Proof. The Euclidean space of density matrices has finite dimension, the set of orthogonal projectors onto $U^n|\Omega\rangle$ is finite, less than d^2, and there exists some smallest natural number b, such that $U^b = \mathbb{1} \cdot$ phase factor. We choose the phase factor for U in such a way that we have $U^b = \mathbb{1}$. In the following, we consider U acting on $\mathcal{H}_A$ only. Since $\operatorname{Tr} U^b = d \operatorname{Tr} \check{U}^b$, the orthogonality of the Bell states implies, as stated before (20),

$$\operatorname{Tr} \check{U}^n = d\delta_{n,0} \qquad \text{for} \quad 0 \leqslant n \leqslant b - 1. \tag{21}$$

$\check{U}^b = \mathbb{1}$ implies that the eigenvalues of $\check{U}$ are elements of $\{e^{2\pi im/b}, 0 \leqslant m \leqslant b - 1\}$. Denote the multiplicities as $f(m)$. Then equation (21) can be read as a formula for the Fourier transform of $f(m)$. The inverse transform gives

$$f(m) = \frac{1}{b} \sum_{n=0}^{b-1} e^{2\pi imn/b} \operatorname{Tr} \check{U}^n = \frac{d}{b}. \tag{22}$$

This number has to be an integer. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Corollary 5. *Any group of unitary intertwiners between mutually orthogonal Bell states contains finite cyclic subgroups. Each one is of some order b, where either b = d or b is a divisor of d.*

It follows that there are not many different possibilities for structures of such groups. Our choice is possible for all d, whether prime or not.

4. Groups and the classical phase space for the magic simplex

Letters of the set $\{j, \ldots, t\}$ denote numbers $0, 1, \ldots, d - 1$. They are considered as elements of $\mathbb{Z}_d := \mathbb{Z}/d\mathbb{Z}$. Calculations with them are to be understood as 'modulo d'.

Intertwiners are the Weyl operators $W_{k,\ell} = \check{W}_{k,\ell} \otimes \mathbb{1}$ presented in section 1:

$$W_{k,\ell} P_{p,q} W_{k,\ell}^\dagger = P_{p+k,q+\ell}. \tag{23}$$

The Weyl operators obey the *Weyl relations*

$$W_{j,\ell} W_{k,m} = w^{k\ell} W_{j+k,\ell+m}, \tag{24}$$

$$W_{k,\ell}^\dagger = W_{k,\ell}^{-1} = w^{k\ell} W_{-k,-\ell}, \tag{25}$$

$$W_{0,0} = \mathbb{1}. \tag{26}$$

They form the Heisenberg–Weyl group $\mathbb{W}$. More precisely, $\mathbb{W}$ is a finite discrete subgroup of the doubly infinite continuous Heisenberg group, compare [W06]. Group elements are $w^m W_{k,\ell}$. The phase factors $\{w^m \mathbb{1}\}$ form an Abelian normalizer; the factor group is $\mathbb{W}/\mathbb{Z}_d \cong \mathbb{Z}_d \times Z_d$. This can be considered in the sense originally meant by Weyl [W31] as the quantization of classical kinematics. The kinematics of the Galilei group is represented in the discrete classical phase space as $\mathbb{Z}_d \times \mathbb{Z}_d$, generated by the global boost $(p, q) \mapsto (p + 1, q)$ and the global space translation $(p, q) \mapsto (p, q + 1)$.

The classical phase space $\mathbb{T} := \{(p, q)\}$ is a lattice on a two-dimensional torus. It has a 'linear' structure—multiplication by constants and addition is always done in the ring $\mathbb{Z}_d$— and it is a symmetric space for the Heisenberg–Weyl group: we define the action of $\mathbb{W}$ on $\mathbb{T}$ by identifying each phase space point (p, q) with the projector $P_{p,q}$ and use equation (23). Moreover, we identify non-negative normalized densities $\{c_{p,q} \geqslant 0, \sum c_{p,q} = 1\}$ with the

elements $\sum c_{p,q} P_{p,q}$ of $\mathcal{W}$. Special use is made of equidistributions over subsets $Q \subset \mathbb{T}$ and the corresponding density matrices

$$\rho_Q := \sum_{(p,q) \in Q} P_{p,q}/|Q|. \tag{27}$$

Now the group structure of $\mathbb{W}$ gives a first insight into the structure of $\text{SEP} \cap \mathcal{W}$. Each cyclic subgroup $\left\{ W_{k,\ell}^n \right\}$ acting on a point (p,q) of $\mathbb{T}$ generates a *line* $\{(p + nk, q + n\ell)\}$.[2] These lines, for d prime, have been identified in [N06] as corresponding to separable states. If there are non-cyclic Abelian subgroups—which may be the case if d is not prime—they generate sublattices, each one with at most two independent basis vectors.

Proposition 6. *Each line or sublattice with d points is generated by an Abelian subgroup of $\mathbb{W}$ and corresponds to a maximally exposed state in* $\text{SEP} \cap \mathcal{W}$.

Proof. Consider a sublattice Q with d points. A lattice in two dimensions can be represented with two basis vectors. So we can represent

$$Q = \{(b + j\mu + k\nu, q + \ell\mu + m\nu), 0 \leqslant \mu \leqslant b - 1, 0 \leqslant \nu \leqslant c - 1, b \cdot c = d\}. \tag{28}$$

We include the cases $b = d, c = 1$ representing lines. For the matrices the representation is

$$\rho_Q = \frac{1}{d} \sum_\mu \sum_\nu U^\mu V^\nu |\Omega_{p,q}\rangle\langle\Omega_{p,q}| U^{-\mu} V^{-\nu} \tag{29}$$

where $U = \mathrm{e}^{\mathrm{i}\gamma} W_{j,\ell}$, $V = \mathrm{e}^{\mathrm{i}\delta} W_{k,m}$, with the phase factors chosen, if necessary, such that $U^b = V^c = \mathbb{1}$. Each one of the smaller exponents gives other elements of $\mathbb{W}$; so

$$\text{Tr}_A U^\mu V^\nu = \delta_{\mu,0}\delta_{\nu,0} \cdot d. \tag{30}$$

For the sublattice the Weyl relations (24) imply

$$U \cdot V \cdot U^\dagger \cdot V^\dagger = w^{k\ell - jm}\mathbb{1}, \tag{31}$$

and the exponent $k\ell - jm$ is the oriented area of a unit cell of Q. The union of all d cells spans all of $\mathbb{T}$, which has area d^2, once or several times; so $(k\ell - jm) \cdot d = z \cdot d^2$, with some $z \in \mathbb{Z}$. It follows that $k\ell - jm \equiv 0$, the rhs of (31) is $\mathbb{1}$, so U and V commute. This allows for a common spectral decomposition

$$\begin{aligned}
\check{U} &= \sum_{s=0}^{d/b-1} \sum_{t=0}^{d/c-1} f(s,t)\, \mathrm{e}^{2\pi\mathrm{i}s/b} |\varphi_{s,t}\rangle\langle\varphi_{s,t}|, \\
\check{V} &= \sum_{s=0}^{d/b-1} \sum_{t=0}^{d/c-1} f(s,t)\, \mathrm{e}^{2\pi\mathrm{i}t/c} |\varphi_{s,t}\rangle\langle\varphi_{s,t}|.
\end{aligned} \tag{32}$$

We get the multiplicity function f, in a way analogous to the proof of theorem 4. Here we use the Fourier transform in two variables and equation (30):

$$f(s,t) = \frac{1}{b \cdot c} \sum_{\mu,\nu} \exp(2\pi\mathrm{i}(\mu s/b + \nu t/c))\, \text{Tr}\, \check{U}^\mu \check{V}^\nu = 1. \tag{33}$$

The diagonalizing basis $\varphi_{s,t}$ in $\mathcal{H}_A$ is now used for a Schmidt decomposition of the Bell state vector:

$$|\Omega_{p,q}\rangle = \frac{1}{\sqrt{d}} \sum_{s,t} |\varphi_{s,t}, \psi_{s,t}\rangle, \tag{34}$$

---

[2] Warning: these lines do not for each d fulfil the conditions for a 'line' in the sense of affine geometry. See also [B04].

with $\psi_{s,t}$ as the appropriate basis in $\mathcal{H}_B$. Inserting (32)–(34) into (29), the summation over the phase factors brings some δ factors, reducing the summations. The result is

$$\rho_Q = \frac{1}{d} \sum_{s,t} |\varphi_{s,t}, \psi_{s,t}\rangle \langle \varphi_{s,t}, \psi_{s,t}|. \tag{35}$$

This expression for ρ_Q is exactly as it is used for the matrices in theorem 3. □

SEP is a convex set and the separable states ρ_Q identified in proposition 6 can be considered as the extreme points of a *kernel polytope* which is a subset of SEP ∩ LMM. These ρ_Q appear also as extreme points of the enclosure polytope, but do not cover all of them if $d \geqslant 3$. For the vertices of the enclosure polytope the set Q can be any subset with d elements of $\mathbb{T}$; for the kernel polytope this set Q has to be a line or a sublattice. That all the other sets Q correspond *in fact* to entangled states is proven in theorem 14.

Theorem 7. *The number of lines and sublattices with d points in $\mathbb{T}$ is*

$$N(d) = d \cdot \left[1 + d + \sum b \right],$$

where the sum runs over all b which are proper divisors of d.

Proof. The number in square brackets must be the number of lines and lattices Q of order d, each containing the point $(0, 0) \in \mathbb{T}$. All the others can be found by translations; and doing all d^2 translations gives each line and each lattice of order d in d-fold multiplicity.

We give a list of these Q containing $(0, 0)$:

(a) $\{(s, 0)|0 \leqslant s \leqslant d - 1\}$, one line.
(b) $\{(k \cdot s, s)|0 \leqslant s \leqslant d - 1\}$, d lines, one for each $k \in [0, \ldots, d - 1]$.
(c) $\{(\mu \cdot b + \nu \cdot b, \nu \cdot d/b)|0 \leqslant \mu \leqslant d/b - 1, 0 \leqslant \nu \leqslant b - 1\}$, b sublattices, one for each $\nu \in [0, b - 1]$, with b a proper divisor of d. □

We remark that some of the sublattices listed in (c) can also be considered as lines. But not all of them, if d is not a simple product of prime numbers but also contains their squares or higher powers. One example is $d = 4, b = 2, \nu = 0$.

5. Symmetries of $\mathcal{W}$

We are looking for symmetries compatible with the entanglement, just to make the investigations simpler. We do not pose detailed restrictions, no measure for entanglement is needed. Just the following, physically motivated characterization is sufficient:

Definition 8. *A mapping $L : \mathcal{W} \rightarrow \mathcal{W}$ is E-compatible (i.e. compatible with entanglement), iff*

(a) *Bell states are mapped to Bell states,*
(b) *L is mixture preserving*

$$L(\alpha\rho + (1 - \alpha)\sigma) = \alpha L(\rho) + (1 - \alpha)L(\sigma),$$

(c) *SEP ∩ $\mathcal{W}$ is mapped onto itself.*

Now if we have a *local* unitary transformation $\rho \to U\rho U^\dagger$, the separability is preserved. Also conditions (a) and (b) are fulfilled. So we know already about a subgroup of symmetry transformations: the translations of phase space; they are implemented as local unitary transformations in the Heisenberg–Weyl group $\mathbb{W}$.

For general L the fulfilling of (b) implies the possibility of linearly extending L. It gives then, due to (a), an invertible norm preserving linear map of the Euclidean space, spanned by the $P_{k,\ell}$, onto itself. It affects a permutation of the Euclidean basis elements $P_{k,\ell}$, hence a map $\mathbb{T} \to \mathbb{T}$. In contrast, any permutation of this kind extends via mixing preserving to a map $\mathcal{W} \to \mathcal{W}$. Now, after any permutation of $\mathbb{T}$ a certain translation can bring the origin $(0,0)$ back to its place. So each of the symmetry operations can be formed as a product of a phase space translation with a certain point transformation M, which leaves the point $(0,0)$ at its place.

The *tool box* of these point transformations of phase space contains the following:

- **The 'horizontal' shear of phase space,** $\mathcal{H}$: $\binom{p}{q} \mapsto \binom{p}{p+q}$. Its powers form a cyclic subgroup. The elements are represented by the matrices $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$. (In discrete classical mechanics this is a free time evolution.)

- **The 'vertical' shear of phase space,** $\mathcal{V}$: $\binom{p}{q} \mapsto \binom{p+q}{q}$. The elements of the generated cyclic subgroup are represented by the matrices $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. (It may be considered as a local boost.)

- **A quarter rotation of phase space,** $\mathcal{R}$: $\binom{p}{q} \mapsto \binom{q}{-p}$. It is represented by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. $\mathcal{R}^2 = -\mathbb{1}$ is a point reflection.

- **Squeezing,** a scale transformation $\binom{p}{q} \mapsto \binom{r \cdot p}{s \cdot q}$, for $r \cdot s \equiv d+1$, possible for each r relative prime to d.

- **Reflections:**
  - inversion of momentum, $\mathcal{S} : p \mapsto -p$,
  - space reflection, $q \mapsto -q$,
  - diagonal reflection, $p \mapsto q, q \mapsto p$.

Proposition 9. *Consider a linear mapping $\mathbb{T} \to \mathbb{T}$, defined as the application of a 2×2 matrix M with elements $\in \mathbb{Z}_d$ and with $\det M = \pm 1$. By extending it to a mapping $\mathcal{W} \to \mathcal{W}$, it is E-compatible.*

These matrices form the extended symplectic group $Sp(2, \mathbb{Z}_d)$.

Proof. Addition and multiplication of the matrix elements is according to the rules of the ring $\mathbb{Z}_d$. This defines the matrix multiplication. The unit matrix has $\det \mathbb{1} = 1$ and is also in this set. Inverting a general element M is achieved with the mapping

$$M = \begin{pmatrix} k & m \\ \ell & n \end{pmatrix} \quad \mapsto \quad M^{-1} = \pm \begin{pmatrix} n & -m \\ -\ell & k \end{pmatrix}, \tag{36}$$

with the sign equal to the sign of $\det M$. So the matrices which are either *symplectic*, $\det M = 1$, or *mirror symplectic*, $\det M = -1$, form a group. We establish now the three transformations $\mathcal{V}, \mathcal{R}, \mathcal{S}$ as generating elements.

First, they generate $\mathcal{H} = \mathcal{R}^{-1}\mathcal{V}\mathcal{R}$ and all the powers $\mathcal{V}^t, \mathcal{H}^t$. The space reflection is $\mathcal{R}^{-1}\mathcal{S}\mathcal{R}$, diagonal reflection $\mathcal{R}\mathcal{S} = -\mathcal{R}^{-1}\mathcal{S}$ and squeezing is $\mathcal{R}\mathcal{V}^{-s}\mathcal{H}^r\mathcal{V}^s$. Multiplication

by $\mathcal{S}$ maps symplectic to mirror symplectic matrices and vice versa. Consider a general symplectic M. The condition $\det M = 1$ can only then be true if k and m are relative prime. Also k and ℓ have no common divisor. (Letters denoting the matrix elements are placed as in (36).) So there exist a t and an s, such that $m + kt \equiv 0$ and $\ell + ks \equiv 0$. One calculates

$$M\mathcal{H}^t = \begin{pmatrix} k & 0 \\ \ell & n+t\ell \end{pmatrix}, \qquad \mathcal{H}^s M \mathcal{H}^t = \begin{pmatrix} k & 0 \\ 0 & n+t\ell \end{pmatrix}.$$

This matrix performs a squeezing. It can be represented as stated above. Multiplication by $\mathcal{H}^{-s}$ from the left and $\mathcal{H}^{-t}$ from the right gives us back the matrix M.

To realize the E-compatibility we proceed as we did for $d = 3$. A general group element M can be considered as a product of the three generating elements. For these we present the operators $C, U_\mathcal{R}, U_\mathcal{V}$ and use their products as U_M. The E-compatibility of the generating elements so infers the E-compatibility of M.

Now we construct for each generating group element M an operator $\check{U}_M \otimes \tilde{U}_M^{-1}$, either unitary or anti-unitary. Its local action in the factor $\mathbb{C}^d$ on the left-hand side as $\check{U}_M$ transforms the Weyl operators, unaffected by $\tilde{U}_M$, as

$$U_M W_{k,\ell} U_M^{-1} = e^{i\eta(M,k,\ell)} W_{k',\ell'}, \tag{37}$$

when M maps $(k, \ell) \mapsto (k', \ell')$. Some phase factors $e^{i\eta}$ may appear. Then we use operators $\tilde{U}$ acting in $\mathbb{C}^d$ on the right-hand side. They are uniquely defined by the condition that $\check{U} \otimes \tilde{U}^{-1}$ leaves the chosen Bell state vector $\Omega_{0,0}$ invariant. Its matrix elements in our preferred basis are $\langle s|\tilde{U}|t\rangle = \langle t|\check{U}|s\rangle$. The joint action in the space $\mathcal{W}$ can now be calculated to give

$$P_{k,\ell} \quad \mapsto \quad \left(\check{U}_M \otimes \tilde{U}_M^{-1}\right) P_{k,\ell} \left(\check{U}_M^{-1} \otimes \tilde{U}_M\right) = U_M P_{k,\ell} U_M^{-1} = P_{k',\ell'}. \tag{38}$$

Now we look at an implementation of the generating elements as local transformations of the Hilbert space. The reflection $\mathcal{S}$ can be implemented by complex conjugation in the preferred basis

$$\check{C}: \quad \sum_s \varphi_s |s\rangle \mapsto \sum_s \varphi_s^* |s\rangle.$$

This is a local anti-unitary operation. It acts onto the Weyl operators as

$$\check{C} \check{W}_{k,\ell} \check{C} = \check{W}_{-k,\ell}. \tag{39}$$

Its anti-linear extension C is complex conjugation in the global Hilbert space,

$$C W_{k,\ell} C = W_{-k,\ell}, \tag{40}$$

mapping SEP onto SEP. So $\mathcal{S}$ is E-compatible.

The other two generators are implemented by local unitaries, so the E-compatibility is obvious. The quarter rotation $\mathcal{R}$ is implemented as $U_\mathcal{R} = \check{U}_\mathcal{R} \otimes \tilde{U}_\mathcal{R}^{-1}$ by the local Fourier transform:

$$\check{U}_\mathcal{R}: \quad |s\rangle \mapsto \frac{1}{\sqrt{d}} \sum_t w^{-st} |t\rangle.$$

It acts onto the Weyl operators as

$$U_\mathcal{R} W_{k,\ell} U_\mathcal{R}^\dagger = w^{-k\ell} W_{\ell,k}. \tag{41}$$

For implementing the vertical shear of phase space, $\mathcal{V}$, one may choose any integer ν and define

$$\check{U}_\mathcal{V}: \quad |s\rangle \mapsto w^{-s(s+d+2\nu)/2} |s\rangle.$$

For general dimension d we use the ordinary integers $s \in \{0, 1 \ldots, d-1\}$ when calculating the exponents. (In $\mathbb{Z}_d$ dividing by 2 is well defined for odd d only.) For even d the half-integer

powers of w have to be chosen consistently for all the odd s. This choice, e.g. $w^{\mu/2} = e^{i\pi\mu/d}$, appears then also in the action onto the Weyl operators:

$$U_\mathcal{V} W_{k,\ell} U_\mathcal{V}^\dagger = w^{\ell(\ell+d+2\nu)/2} W_{k+\ell,\ell}. \tag{42}$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Now this group of E-compatible point transformations is maximal, other transformations do not have the compatibility property. The proof is given in section 8.

Some remarks on more subtleties: note that the implementations of the matrix group elements M are not unique. There are four different groups of transformations of vectors and operators involved. Transformations of vectors in $\mathbb{C}^d$ by $\check{U}_M$, unitary transformations of the operators as noted in (37).[3] Then there are transformations by $\check{U}_M \otimes \tilde{U}_M$ of vectors in the global Hilbert space, and the related transformations of the operators as noted in (38). Only the last one gives a representation of $Sp(2, \mathbb{Z}_d)$, when restricted to the Euclidean space spanned by $P_{k,\ell}$. The others are 'quantizations', involving phase factors. There is moreover the possibility of multiplying each U_M by some $W_{j,r}$, and this gives a discrete set of different implications.

The total group $\mathbb{E}$ of E-compatible transformations has, by the way, the structure of the semidirect product $Sp(2, \mathbb{Z}_d) \rtimes \mathbb{W}$ of the extended symplectic group and the Heisenberg–Weyl group. That is (see, for example, [W06]): the extended symplectic group gives an automorphism of the normal subgroup $\mathbb{W}$, as noted in (37). The group product in $\mathbb{E}$ is given as

$$(U_M W_{j,m}) * (U_L W_{k,\ell}) = (U_{M \cdot L} e^{i\eta(L,j,m)} W_{j'+k,m'+\ell}) \tag{43}$$

when L maps $(j, m) \mapsto (j', m')$.

6. Witnesses and more symmetry

Entanglement witnesses have been introduced [T00] to detect the entanglement. Detection can be either experimentally or theoretically. To prove theorem 14 we use them in that way, to discern the entangled vertices of the enclosure polytope from the separable ones.

Here we reverse the point of view. 'Witnesses' are used to study the location of SEP, the convex set of separable states. We define the set of *structural* witnesses,

$$\text{SW} := \{K = K^\dagger \neq 0 | \forall \sigma \in \text{SEP} : \text{Tr}(\sigma K) \geqslant 0\}. \tag{44}$$

This set forms a convex cone of operators. $\text{SW} \cup \{0\}$ is the dual convex cone to $\{\alpha\rho, \alpha \geqslant 0, \rho \in \text{SEP}\}$ and thus completely characterizes the location of SEP. Geometrically, every structural witness defines a hyperplane in the Hilbert–Schmidt space of Hermitian matrices ρ, which is a Euclidean space with dimension d^4. The extremal rays of this dual cone are *tangential* witnesses for density matrices ρ on the *surface* of SEP:

$$\text{TW} := \bigcup_{\rho \in \text{surface (SEP)}} \text{TW}_\rho \tag{45}$$

$$\rho \in \text{surface (SEP)}: \qquad \text{TW}_\rho := \{K \in \text{SW} | \text{Tr}(\rho K) = 0\}. \tag{46}$$

Being interested in SEP restricted to a linear subspace of states, we may restrict the study of witnesses onto a dual subspace. If the set of states is defined by invariance under the action of a group $\mathcal{G}$, the dual subspace is a set of witnesses which are also invariant. The details of

---

[3] Some of the unitary transformations of operators appear as 'gates' in quantum computation, see e.g. [G99, GKP01].

this argument have been presented for $d = 3$. There was no use of a special dimension and we may take over the results from [BHN06]:

Theorem 10. *Characterizing* $SEP \cap \mathcal{W}$ *through witnesses is simplified by using the following properties:*

- *SEP* $\cap$ *$\mathcal{W}$ is completely characterized by duality, using witnesses of the form* $K = \sum_{k,\ell} \kappa_{k,\ell} P_{k,\ell}$.
- *Such an operator K is a witness, iff* $\forall \tilde{\psi} \in \mathbb{C}^d$ *the operator*

$$\sum_{k,\ell} \kappa_{k,\ell} W_{k,\ell} |\tilde{\psi}\rangle\langle\tilde{\psi}| W_{k,\ell}^{-1} \tag{47}$$

 is not negative.
- *K is a tangential witness in some TW_ρ iff* $\exists |\varphi, \psi\rangle$ *such that*

$$\sum_{k,\ell} \kappa_{k,\ell} |\langle\varphi| W_{k,\ell} |\tilde{\psi}\rangle|^2 = 0 \tag{48}$$

 with $|\tilde{\psi}\rangle = \sum_s \langle s|\psi\rangle^* |s\rangle$. *The state*

$$\rho = \langle|\varphi, \psi\rangle\langle\varphi, \psi|\rangle_{\mathcal{G}} \tag{49}$$

 is a boundary state of SEP and located in the tangential hyperplane, $\text{Tr}\,\rho K = 0$. *Here $\mathcal{G}$ is the Abelian group of unitaries generated by* $(\mathbb{1} - P_{k,\ell})/2$. $\langle\ \rangle_{\mathcal{G}}$ *denotes symmetrizing by the 'twirl' operation concerning the group $\mathcal{G}$.*

Some states have more symmetry and the tangential witnesses can be found in some even smaller set, showing the same symmetry as the state. Sometimes these extra symmetries are given as subgroups of the inner symmetries of $\mathcal{W}$ which we analysed in section 5. The simplest example concerns the *isotropic* witness, which is the optimal entanglement witness for a Bell state. The elementary calculation may again be performed for general d as it is done for $d = 3$. Sometimes external groups, mapping part of $\mathcal{W}$ to other states, have to be used. We give one example.

Theorem 11. *Concerning the subsection* $\{\rho = \sum_k c_k P_{k,0}\}$ *of density matrices, the search for witnesses can be reduced to* $\{K = \sum_k \kappa_k P_{k,0} + \sum_\ell \gamma_\ell Q_\ell\}$, *with* $Q_\ell = \sum_k P_{k,\ell}/d$ *and* $\gamma_{-\ell} = \gamma_\ell$.

Proof. As a first step we use the $\mathcal{W}$-symmetry of space reflection $\ell \leftrightarrow -\ell$. This is an invariance of the chosen states. Projecting $K = \sum_{k,\ell} \kappa_{k,\ell} P_{k,\ell}$ onto an invariant operator by the 'twirl' operation with this group $\mathcal{G}$ of two elements gives

$$\langle K \rangle_{\mathcal{G}} = \sum_{k,\ell} \kappa'_{k,\ell} P_{k,\ell}, \qquad \kappa'_{k,\ell} = \frac{1}{2}(\kappa_{k,\ell} + \kappa_{k,-\ell}). \tag{50}$$

In the second step we use the group $\mathcal{G}U$ of local unitaries $\check{U} \otimes \tilde{U}$ diagonal in the preferred basis,

$$\check{U} : |s\rangle \mapsto e^{i\alpha(s)}|s\rangle, \quad \tilde{U} : |t\rangle \mapsto e^{-i\alpha(t)}|t\rangle.$$

We use the expansion

$$P_{k,\ell} = \frac{1}{d} \sum_{t,r} w^{k(t-r)} |t-\ell, t\rangle\langle r-\ell, r|, \tag{51}$$

and form the second projection by twirl onto operators invariant under this group,

$$\langle\langle K\rangle_{\mathcal{G}}\rangle_{\mathcal{G}U} = \sum_{k,\ell} \kappa'_{k,\ell} \frac{1}{d} \sum_{t,r} w^{k(t-r)} \langle |t-\ell, t\rangle\langle r-\ell, r|\rangle_{\mathcal{G}U}. \tag{52}$$

The invariant part involves

$$\langle |t-\ell, t\rangle\langle r-\ell, r|\rangle_{\mathcal{G}U} = \langle e^{i(\alpha(t-\ell)-\alpha(t)-\alpha(r-\ell)+\alpha(r))}\rangle_{\mathcal{G}U} |t-\ell, t\rangle\langle r-\ell, r|$$
$$= \delta_{\ell,0}|t, t\rangle\langle r, r| + (1-\delta_{\ell,0})\delta_{t,r}|t-\ell, t\rangle\langle t-\ell, t|.$$

Inserting this equation and also (50) into (52) gives for the first term $\sum_k \kappa_{k,0} P_{k,0}$, for the second term $(1-\delta_{\ell,0})\gamma_\ell Q_\ell$ with $\gamma_\ell = \frac{1}{2}\sum_k(\kappa_{k,\ell}+\kappa_{k,-\ell})$. $\qquad\square$

7. Partial transposition

PT can be used, referring to the Peres criterion, to prove entanglement. On the other hand, it maps LMM ∩ PPT onto itself, see lemma 1. There is a PT-related subset $\hat{\mathcal{W}}$ of LMM with $\hat{\mathcal{W}} \cap \text{PPT} = \mathcal{W} \cap \text{PPT}$: it is defined as the linear extension of PT($\mathcal{W} \cap \text{PPT}$) to the borders of positivity. The dimensions of these related subspaces are equal, $\dim(\mathcal{W}) = \dim(\hat{\mathcal{W}}) = d^2 - 1$. Studies on the structure of $\mathcal{W}$ are automatically studies on the structure of $\hat{\mathcal{W}}$. The two pictures, figures 2 and 3, presented in [BHN06] for $d = 3$ can be seen in that way. The region of PPT-matrices (not necessarily positive) becomes the region of states, i.e. positive matrices, and vice versa. Their intersections are the PPT states—density matrices which are both positive and PPT—in both points of view. The Peres criterion, SEP $\subset$ PPT, implies that also $\mathcal{W} \cap \text{SEP} = \hat{\mathcal{W}} \cap \text{SEP}$. The cases of *bound entanglement* [HHH98] may therefore also be seen in two ways. The regions of bound entanglement in $\mathcal{W}$, e.g. those that we found for $d = 3$, are in one-to-one correspondence to those in $\hat{\mathcal{W}}$.

PT of our simplex $\mathcal{W}$ has nice features, inferring simplification for calculations. We use again the expansion (51) and observe that PT maps

$$|t-\ell, t\rangle\langle r-\ell, r| \mapsto |m-t, t\rangle\langle m-r, r| \qquad \text{with} \quad m = t+r-\ell.$$

Splitting the global Hilbert space into subspaces according to the quantum number m allows for a splitting of partial transposed $\mathcal{W}$-states:

$$\text{PT}: \quad \rho = \sum_{k,\ell} c_{k,\ell} P_{k,\ell} \quad \mapsto \quad \bigoplus_m B_m, \tag{53}$$

with Hermitian $d \times d$ matrices B_m,

$$\langle s|B_m|t\rangle = \frac{1}{d}\sum_k c_{k,s+t-m} w^{k(s-t)} = \langle t|B_m|s\rangle^*. \tag{54}$$

Theorem 12. *Consider the matrices B_m corresponding to some state in $\mathcal{W}$ according to (53):*

- *For odd d all B_m are unitarily equivalent.*
- *For even d there are two classes of mutually equivalent B_m, one for even m and the other for odd m.*
- *If d is even, there is the relation of matrix elements for every B_m*

$$\langle s+d/2|B_m|t+d/2\rangle = \langle s|B_m|t\rangle. \tag{55}$$

Proof. For any d observe

$$\langle s|B_{m-2}|t\rangle = \frac{1}{d}\sum_k c_{k,s+t-m+2}w^{k(s-t)} = \langle s+1|B_m|t+1\rangle.$$

For d odd one shows $\langle s|B_{m-1}|t\rangle = \langle s+(d+1)/2|B_m|t+(d+1)/2\rangle$ by observing $s+t-m+1 \equiv [s+(d+1)/2]+[t+(d+1)/2]-m$ in the second index of c. For even d, the equivalence $s+t \equiv [s+d/2]+[t+d/2]$ implies (55). $\square$

The last point has the consequence that, if d is even, each B_m has the form of a block matrix

$$\begin{pmatrix} C & D \\ D & C \end{pmatrix} \cong C \otimes \mathbb{1}(2) + D \otimes \sigma_x \cong \frac{C+D}{2} \oplus \frac{C-D}{2} \tag{56}$$

with Hermitian blocks C_m and D_m. $\mathbb{1}(\nu)$ is the $\nu \times \nu$ unit matrix.

Consider now the Abelian algebras

$$\mathcal{A}(d) := \left\{ \sum_{k,\ell} a_{k,\ell} P_{k,\ell}, a_{k,\ell} \in \mathbb{C} \right\} \cong M_0(d^2, \mathbb{C}) \tag{57}$$

emerging as a linear span of the special density matrices. Using theorem 12 and (56) the results of mapping by PT are the following subalgebras of $M(d^2, \mathbb{C})$:

- If d is odd—PT: $\mathcal{A}(d) \mapsto M(d, \mathbb{C}) \otimes \mathbb{1}(d)$,
- If d is even—PT: $\mathcal{A}(d) \mapsto M(d/2, \mathbb{C}) \otimes M_0(4, \mathbb{C}) \otimes \mathbb{1}(d/2)$.

A consequence is a simplification for checking whether a state in $\mathcal{W}$ is PPT or not. These states are mapped to linear functionals of $PT(\mathcal{A}(d))$, represented either, if d is odd, by Hermitian matrices in $M(d, \mathbb{C})$ or, if d is even, by four Hermitian matrices in $M(d/2, \mathbb{C})$.

A further consequence is an insight into the structure of the state space $\hat{\mathcal{W}}$:

Theorem 13. *The subset $\hat{\mathcal{W}}$ of LMM is given by the intersection of $PT(\mathcal{A}(d))$ with the set of density matrices.*

Only for $d = 2$ it is again a simplex—the reflected tetrahedron. For odd d it is the state space consisting of Hermitian $d \times d$ density matrices—when the tensorial factor $\mathbb{1}$ is neglected. For even $d \geqslant 4$ there are three-dimensional sections with the form of a tetrahedron through every point in this (d^2-1)-dimensional convex body. In other directions there exist sections of dimension $d^2/4-1$ with the structure of the state space with $(d/2) \times (d/2)$ density matrices. The space of states for $M(\nu, \mathbb{C})$ is the convex set of normalized positive $\nu \times \nu$ matrices. Every maximal face is equivalent to the set of normalized $(\nu-1) \times (\nu-1)$ matrices. So its faces have dimension $\nu(\nu-2)$ at most. It follows that the surface of $\hat{\mathcal{W}}$ is curved in many directions, if $d \geqslant 3$. Part of the border of $\hat{\mathcal{W}}$ is the border of $PPT \cap \mathcal{W}$. This border is therefore also curved in many directions.

Both local unitary transformations and the global complex conjugation map PPT onto itself. So the symmetries established in section 5 are symmetries of $PPT \cap \mathcal{W}$ and of $\hat{\mathcal{W}}$ too. Also the witnesses for $\mathcal{W}$ can be transported to witnesses of $\hat{\mathcal{W}}$ by PT. This follows from the 'self-adjointness' of PT as a transformation in the Hilbert–Schmidt space: $\mathrm{Tr}(PT[\rho]K) = \mathrm{Tr}(\rho PT[K])$.

Finally, look at special LMM states in $\hat{\mathcal{W}}$. No Bell states are in $\hat{\mathcal{W}}$, if $d \geqslant 3$. There is a set of Werner states instead, and $\hat{\mathcal{W}}$ includes as many Werner states with some given mixing as $\mathcal{W}$ contains Bell states: d^2 of them are extremal with a density matrix which is a $(d(d-1)/2)$-dimensional projector. The *set* of maximally exposed LMM $\cap$ SEP states are mapped by PT onto itself. Their number in $\hat{\mathcal{W}}$ is thus again $N(d)$, the same as in $\mathcal{W}$, see theorems 7 and 14.

8. Optimality

We follow the second trail which aims at proving not to have overlooked anything.

Theorem 14. *There is a one-to-one correspondence between the maximally exposed states in* SEP $\cap$ $\mathcal{W}$ *and the lines or sublattices with d points, generated by Abelian subgroups of* $\mathbb{W}$.

Proof. One-half of this theorem is proven in proposition 6. On the other hand, SEP $\cap$ LMM is inside the enclosure polytope. In the large space of Hermitian matrices, the extremal points of this polytope lie at the intersections of the witness hyperplanes B_α and the positivity borders A_β, with $\alpha \in Q \subset \mathbb{T}, \beta \in \mathbb{T}\backslash Q$. Restricting the space to the space of normalized matrices gives the condition $|Q| = d$. This is the condition to get those vertices of the enclosure polytope which are inside of $\mathcal{W}$. They all have exactly the same distance to ω as the maximally exposed separable states. But not all of them are separable, only those where Q is a line or a sublattice. For d prime this has been stated in [N06]. For general dimension d we define

$$K = \mathbb{1} - (1 + \varepsilon) \sum_{\alpha \in Q} P_\alpha = \mathbb{1} - (1 + \varepsilon)d \cdot \rho_Q \tag{58}$$

and claim that it is an entanglement witness if ε is small and if Q is *not* a line or a sublattice. To prove this claim we have to show that $\forall |\varphi, \psi\rangle$ the expectation value of (58) is not negative,

$$\langle \varphi, \psi | K | \varphi, \psi \rangle \geqslant 0. \tag{59}$$

With $P_\alpha = W_\alpha |\Omega_{0,0}\rangle\langle\Omega_{0,0}|W_\alpha^\dagger$ one gets

$$\langle \varphi, \psi | K | \varphi, \psi \rangle = \|\varphi\|^2 \|\psi\|^2 - (1 + \varepsilon) \sum_\alpha |\langle \varphi, \psi | W_\alpha | \Omega_{0,0} \rangle|^2. \tag{60}$$

We insert definition (1) of $\Omega_{0,0}$:

$$\langle \varphi, \psi | W_\alpha | \Omega_{0,0} \rangle = \frac{1}{\sqrt{d}} \sum_s \langle \varphi | \check{W}_\alpha | s \rangle \langle \psi | s \rangle = \frac{1}{\sqrt{d}} \langle \varphi | \check{W}_\alpha | \tilde{\psi} \rangle,$$

with $|\tilde{\psi}\rangle := \sum_s \langle s | \psi \rangle^* | s \rangle$. So we have to check the non-negativity of

$$\|\varphi\|^2 \|\tilde{\psi}\|^2 - \frac{1 + \varepsilon}{d} \sum_{\alpha \in Q} |\langle \varphi | \check{W}_\alpha | \tilde{\psi} \rangle|^2. \tag{61}$$

Since Q is not a sublattice, the Weyl operators which appear in the sum do not all commute with each other. That means $\check{W}_\alpha \check{W}_\beta = e^{i\gamma} \check{W}_\beta \check{W}_\alpha$ with $e^{i\gamma} \neq 1$ for some pairs of operators, and there is no common eigenvector. For each pair of vectors there is at least one α such that $|\langle \varphi | \check{W}_\alpha | \tilde{\psi} \rangle| < \|\varphi\| \|\tilde{\psi}\|$. There is only a finite number of operators and a compact set of normalized vectors; one has equicontinuity and uniform boundedness,

$$\exists \varepsilon > 0, \text{ s.t. } \forall \varphi, \tilde{\psi} : \sum_{\alpha \in Q} |\langle \varphi | \check{W}_\alpha | \tilde{\psi} \rangle|^2 < d \cdot (1 - 2\varepsilon) \|\varphi\|^2 \|\tilde{\psi}\|^2.$$

So the claim that K defined in (58) is a witness for some ε is proven:

$$\langle \varphi, \psi | K | \varphi, \psi \rangle > \|\varphi\|^2 \|\psi\|^2 (\varepsilon - 2\varepsilon^2). \tag{62}$$

Since $\text{Tr } K \rho_Q = -\varepsilon$, the state ρ_Q is shown to be entangled. $\qquad\square$

Remark. The procedure connecting the expectations (60) with formula (61) is also used in section 6, theorem 10.

In theorem 14 we have proved that the geometric symmetry of the kernel polytope is smaller than that for the enclosure polytope. One implication is

Lemma 15. *Every E-compatible point transformation M must be a linear invertible mapping* $\mathbb{T} \to \mathbb{T}$.

Proof. The set of kernel vertices has to be mapped onto itself. This set corresponds to the set of lines and sublattices with exactly d points in the phase space $\mathbb{T}$. Every pair of phase space points lies on one line at least, many pairs on not more than one. Since the mappings are one to one, each of these one-line-only pairs has to be mapped onto an equivalent one-line-only pair. There are enough of them, like $[(p, q), (p + k, q + 1)]$, to imply the *linearity*: every line is mapped onto a line. □

We remark that invertibility of M means that the matrix

$$M^{-1} = (\det M)^{-1} \begin{pmatrix} n & -m \\ -\ell & k \end{pmatrix}$$

has to exist. This is only then the case if $\det M$ is coprime with d, excluding e.g. $\det M = 2$ for $d = 4$ and $\det M = \pm 2$ or 3 for $d = 6$.

Next we show that the geometric symmetry of the kernel polytope is still deceptive, if $d = 5$ or $d \geqslant 7$.

Theorem 9. *Consider a linear mapping* $\mathbb{T} \to \mathbb{T}$ *defined by applying a* 2×2 *matrix M with elements* $\in \mathbb{Z}_d$. *Its extension to a mapping* $\mathcal{W} \to \mathcal{W}$ *is E-compatible if and only if* $\det M = \pm 1$.

Proof. The first part is proven constructively in the proof of proposition 9. To prove the other direction we use duality of convex cones. A linear mapping $\mathcal{W} \mapsto \mathcal{W}$ is E-compatible iff the dual transformation maps SW to SW and TW onto TW. The dual transformation, acting onto witnesses, is given by the dual mapping of the set $\{\kappa_{k,\ell}\}$ considered as an element of $\ell^2(\mathbb{T}, \mathbb{R})$:

$$K = \sum \kappa_{k,\ell} P_{k,\ell}, \qquad \rho = \sum c_{k,\ell} P_{k,\ell} \quad \Rightarrow \quad \text{Tr} \, K\rho = \sum \kappa_{k,\ell} c_{k,\ell}.$$

The dual mapping of $\mathbb{T}$ is therefore M^{-1}, which is an element of $Sp(2, \mathbb{Z}_d)$ iff M is such a matrix.

Consider now a line of tangential witnesses

$$K(\varepsilon) = \lambda(\varepsilon)\mathbb{1} + H + \varepsilon P. \tag{63}$$

The parameter λ is fixed through the conditions on K stated in theorem 10. They imply the existence of normed vectors $|\varphi, \psi\rangle$ such that

$$\langle \varphi, \psi | K | \varphi, \psi \rangle = \min_{\chi, \eta} \langle \chi, \eta | K | \chi, \eta \rangle = 0, \tag{64}$$

and therefore

$$-\lambda(\varepsilon) = \min_{\chi, \eta} \langle \chi, \eta | (H + \varepsilon P) | \chi, \eta \rangle. \tag{65}$$

This situation is treated perturbatively. Let $|\varphi(\varepsilon), \psi(\varepsilon)\rangle$ be a differentiable curve of vectors with $|\varphi(0), \psi(0)\rangle = |\varphi, \psi\rangle$, the minimizers at $\varepsilon = 0$, with normalized vectors $\varphi(\varepsilon) = \varphi + \varepsilon\delta\varphi + O(\varepsilon^2)$, $\psi(\varepsilon) = \psi + \varepsilon\delta\psi + O(\varepsilon^2)$. With

$$-\mu(\varepsilon) = \langle \varphi(\varepsilon), \psi(\varepsilon) | (H + \varepsilon P) | \varphi(\varepsilon), \psi(\varepsilon) \rangle$$

one gets

$$-\frac{\mathrm{d}}{\mathrm{d}\varepsilon} \mu(\varepsilon)|_{\varepsilon=0} = \langle \varphi, \psi | P | \varphi, \psi \rangle + [\langle \delta\varphi | \check{H}_\psi | \varphi \rangle + \text{c.c.}] + [\langle \delta\psi | \tilde{H}_\varphi | \psi \rangle + \text{c.c.}], \tag{66}$$

with the operators $\check{H}_\psi$ and $\tilde{H}_\varphi$ defined as quadratic forms in the local Hilbert spaces,

$$\langle\chi|\check{H}_\psi|\eta\rangle := \langle\chi, \psi|H|\eta, \psi\rangle, \qquad \langle\chi|\tilde{H}_\varphi|\eta\rangle := \langle\varphi, \chi|H|\varphi, \eta\rangle.$$

We know from standard perturbation theory that the terms in square brackets in (66) are zero if the ground states of the local $\check{H}_\psi$ and $\tilde{H}_\varphi$ are not degenerate.

For $\varepsilon = 0$ we choose

$$H = \sum_k \gamma_k P_{k,0} \qquad \gamma_k = -(w^k + w^{-k}).$$

Using the expansion (51) and then $\frac{1}{d}\sum_k \gamma_k w^{k(s-t)} = \delta_{s,t-1} + \delta_{s,t+1}$ we get

$$\langle\varphi, \psi|H|\varphi, \psi\rangle = -\sum_{s,t} \varphi_s \psi_s \varphi_t^* \psi_t^* (\delta_{s,t-1} + \delta_{s,t+1}) \tag{67}$$

$$= -2\sum_s f(s)f^*(s+1), \tag{68}$$

with $f(s) := \varphi_s \psi_s$. The minimum of (68) is attained if all $f(s)$ are real valued and positive. Also φ_s and ψ_s can be chosen as positive. One step in minimizing (67) with the condition $\|\varphi\| = \|\psi\| = 1$ can be considered as equivalent to the reverse task of keeping $f(s)$ fixed and minimizing $\|\varphi\| \cdot \|\psi\|$. This gives $\varphi_s = \psi_s$ and $\sum_s f(s) = \|\varphi\|^2 = 1$. Using this as a side condition to minimize (68) one gets the minimizers: for $d \geqslant 5$ they are $f(s) = \frac{1}{2}(\delta_{s,t} + \delta_{s,t+1})$ and $f(s) = \frac{1}{2}\delta_{s,t} + \frac{1}{4}(\delta_{s,t-1} + \delta_{s,t+1})$ for any t. Defining $\varphi = \sqrt{f}$ and $\psi = \sqrt{f}$ one sees the non-degeneracy of the ground states of the local operators H_ψ and $\tilde{H}_\varphi$. Using the ground state vectors $\varphi_s(\varepsilon)$ and $\psi_s(\varepsilon)$ gives $\mu(\varepsilon) = \lambda(\varepsilon)$. Applying (66) results therefore in

$$-\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\lambda(\varepsilon)\mid_{\varepsilon=0} = \langle\varphi, \psi|P|\varphi, \psi\rangle. \tag{69}$$

Choose $\varphi_s = \psi_s = \frac{1}{\sqrt{2}}(\delta_{s,0} + \delta_{s,1})$, consider $P = P_{0,1}$ and transformations by

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

$H(0)$ is invariant under this transformation, but the perturbative $P_{0,1}$ changes to $P_{0,n}$. The value of (69) is changed, unless $n = \pm 1$, proving the non-invariance of TW. Using transformations by symplectic matrices, every matrix M can be transformed to this diagonal form without changing its determinant. So $\det M = \pm 1$ is a necessary condition. $\square$

9. Summary and outlook

The paper extends on previous work [BHN06] for qutrits, but here the results are stated in a more mathematical context and are generalized to arbitrary Hilbert space dimensions d. We consider the state space of two qudits and analyse a certain subset, the simplex (generalized tetrahedron) $\mathcal{W}$ as the main object of our investigations. It is obtained starting from a certain maximally entangled pure state, a Bell-type state. By applying on one side the Weyl operators other orthogonal Bell-type states are formed, and the set of mixtures, the complex hull, is the simplex $\mathcal{W}$. The Weyl operators are related to a discrete classical phase space, representing in turn the algebraic relations of the Weyl operators. This analogy enables us to describe the local transformations of the quantum state space of interest and is very useful for several proofs in this paper: transformations of $\mathcal{W}$ onto itself can be considered as transformations of the discrete classical phase space. Thus, the symmetries and equivalences can be studied by this means.

The simplex $\mathcal{W}$ is embedded in a d^2-dimensional Euclidean space equipped with a norm (the Hilbert–Schmidt norm) and an inner product. We analyse in detail the properties how it

is embedded in the whole state space of two qudits and discuss symmetries and equivalences inside the simplex $\mathcal{W}$, its facets and witnesses. This is obtained via the Weyl group which is a kind of 'quantization' of classical phase space.

Then we investigate the question of the geometry of separability. We start with the construction of two polytopes, an inner (kernel polytope) and an outer (enclosure polytope) fence for separability. They define entanglement witnesses but are in general not optimal. The outer fence, the enclosure polytope, has the same geometric symmetry as $\mathcal{W}$. Because we are able to construct *optimal* entanglement witnesses explicitly we obtain in principle the border between separable and entangled states, sometimes even in analytic form.

With our method we also find the set of *bound* entangled states of the parameter subspace under investigation, by applying the partial transposition on one subsystem, which detects entanglement via PPT. The obtained PPT witnesses are sometimes different from the entanglement witnesses for the density matrices under consideration. We stated and explored also a kind of 'duality' where the partial transposition maps PPT $\cap\ \mathcal{W}$ to PPT $\cap\ \hat{\mathcal{W}}$, where $\hat{\mathcal{W}}$ is another convex subset of LMM (the set of locally maximally mixed states), and the cases of bound entanglement detected in $\mathcal{W}$ are also cases for bound entanglement in $\hat{\mathcal{W}}$.

Summarizing, we could present a detailed geometric structure of the subset of bipartite qudits under investigation. We think that this will help to find a good characterization of the whole state space and to investigate measures for entanglement for higher dimensional systems.

In the outlook, we hope the paper advances our knowledge of these structures, of the convex hull of higher dimensional generalizations of the two-qubit Bell states. These two-qubit states have many applications in quantum information theory, and so their characterization for higher dimension is a desirable research goal. The higher dimensional generalizations may also have applications in quantum information and display interesting geometrical features on their own. Since we show how to construct optimal witnesses explicitly and how to determine regions where there is bound entanglement, i.e. entanglement which cannot be distilled by local operation and classical communication (LOCC), these methods might be useful in quantum cryptography. Regarding possible applications of our results and methods in a wider context, we note that the quasiclassical structure also fits exactly into the conditions needed for teleportation and dense coding, see e.g. [BW92, W01].

Furthermore, according to the opinion of one of the referees, due to the Choi-Jamiołkowski isomorphism between a class of bipartite states and maps [ZB04] or channels [HHH98b] one may infer from the results of the present paper further conclusions about the maps, e.g. (bistochastic) superpositive maps, which correspond to separable states: using the isomorphism (for a recent exposition, see e.g. [B06] or [L06]) we see that the states of a $d \times d$ system satisfying one partial trace condition $\mathrm{Tr}_A \rho = \omega_B$ represent stochastic maps (completely positive, trace-preserving linear maps) while states satisfying simultaneously both conditions $\mathrm{Tr}_A \rho = \omega_B$, $\mathrm{Tr}_B \rho = \omega_A$ represent bistochastic maps. Hence, the set LMM for bipartite systems is isomorphic to the set of bistochastic maps. See also [BDS01] for relations to remote state preparation.

Last but not least, exploration of entanglement properties in still more detail, using the high symmetry of the chosen sets of states, seems to be the nearest and next goal.

References

[BW92] Bennett C H and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen state *Phys. Rev. Lett.* **69** 2881–4

[B93] Bennett C H *et al* 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895

[W01] Werner R F 2001 All teleportation and dense coding schemes *J. Phys. A: Math. Gen.* **34** 7081–94

[VW00] Vollbrecht K G H and Werner R F 2001 Entanglement measures under symmetry *Phys. Rev.* A **64** 062307 (*Preprint* quant-ph/0010095)

[HH96] Horodecki R and Horodecki M 1996 Information-theoretic aspects of inseparability of mixed states *Phys. Rev.* A **54** 1838–43

[ZB04] Zyczkowski K and Bengtsson I 2004 On duality between quantum maps and quantum states *Open Syst. Inf. Dyn.* **11** 3–42 (*Preprint* quant-ph/0401119)

[AU82] Alberti P M and Uhlmann A 1982 *Stochasticity and Partial Order. Doubly Stochastic Maps and Unitary Mixing* (Dordrecht: Reidel)

[BNT02] Bertlmann R A, Narnhofer H and Thirring W 2002 Geometric picture of entanglement and bell inequalities *Phys. Rev.* A **66** 032319 (*Preprint* quant-ph/0111116)

[BHN06] Baumgartner B, Hiesmayr B and Narnhofer H 2006 The state space for two qutrits has a phase space structure in its core *Phys. Rev.* A **74** 032327 (*Preprint* quant-ph/0606083)

[P96] Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* **77** 1413 (*Preprint* quant-ph/9604005)

[T00] Terhal B M 2000 Bell inequalities and the separability criterion *Phys. Lett.* A **271** 319–26 (*Preprint* quant-ph/9911057)

[Sch86] Schroeder M R 1986 *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing and Self-Similarity* (*Springer Series in Information Sciences* vol 7) (Berlin: Springer)

[V64] Valentine F A 1964 *Convex Sets* (*McGraw-Hill Series in Higher Mathematics*) (New York: McGraw-Hill)

[A42] Aitken A C 1942 *Determinants and Matrices* (*University Mathematical Texts* vol 1) (Edingburgh: Oliver and Boyd)

[W06] Wikipedia, The Free Encyclopedia http://en.wikipedia.org/wiki

[GB02] Gurvits L and Barnum H 2002 Largest separable balls around the maximally mixed bipartite quantum state *Phys. Rev.* A **66** 062311

[W31] Weyl H 1931 *Gruppentheorie und Quantenmechanik,* zweite Auflage (Leipzig: S Hirzel)

[B04] Bengtsson I 2004 MUBs, polytopes and finite geometries *Preprint* quant-ph/0406174

[N06] Narnhofer H 2006 Entanglement reflected in Wigner functions *J. Phys. A: Math. Gen.* **39** 7051–64

[G99] Gottesman D 1999 Fault–Tolerant quantum computation with higher-dimensional systems *Lect. Notes Comput. Sci.* **1509** 302 (*Preprint* quant-ph/9802007)

[GKP01] Gottesman D, Kitaev A and Preskill J 2001 Encoding a qubit in an oscillator *Phys. Rev.* A **64** 012310

[HHH98] Horodecki M, Horodecki P and Horodecki R 1998 Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? *Phys. Rev. Lett.* **80** 5239–42

[HHH98b] Horodecki M, Horodecki P and Horodecki R 1998 General teleportation channel, singlet fraction and quasi-distillation *Preprint* quant-ph/9807091

[B06] Bengtsson I 2006 *Geometry of Quantum States* (Cambridge: Cambridge University Press)

[L06] Leifer M S 2006 Conditional density operators and the subjectivity of quantum operations *Preprint* quant-ph/0611233

[BDS01] Bennett C H *et al* 2001 Remote state preparation *Phys. Rev. Lett.* **87** 077902