International Journal of Theoretical Physics, Vol. 40, No. 6, 2001

Theory of a Pair of Quantum Bits

Hans J. Kummer[1]

Received September 28, 2000

In this paper we present a thorough study of the theory of a pair of qubits, whose Hilbert space can be identified with $\mathbb{C}^2 \otimes \mathbb{C}^2$. Given an hermitian operator ρ of trace 1 in $\mathbb{C}^2 \otimes \mathbb{C}^2$ we focus on the following Problems: *Problem 1*: Find conditions that guarantee that ρ is a state, that is, positive semidefinite. *Problem 2*: Find conditions that guarantee that a given state ρ is separable, or that ρ is a convex combination of products of one-particle states. The language we develop for our investigation makes use of the observation that $\mathbb{C}^2 \otimes \mathbb{C}^2$ carries representations of the special unitary group $SU(2)$ in two dimensions and of the direct product of this group by itself. We introduce a new type of observable called *Bell observable* (section 5) and a new measure of entanglement called *concurrence*, which is closely related to the concurrence introduced by Wootters (Physical Review Letters (1998) **80**, 2245–2248) (section 8). The work has been inspired by the works of Wootters (Physical Review Letters (1997) **78**, 5022–5025; Physical Review Letters (1998) **80**, 2245–2248) and members of the Horodecki family (cf Horodecki and Horodecki, Physical Review A (1996) **54**, 1838–1843; Horodecki *et al.*, Physics Letters A (1996a) **223**, 1–8; Physics Letters A (1996b) **222**, 21–25) and reproduces some of their results.

1. INTRODUCTION

A *quantum bit* or *qubit* is a quantum mechanical system whose pure states are in one-to-one correspondence with the rays in a two-dimensional Hilbert space endowed with a distinguished *orthonormal* basis $(|0\rangle, |1\rangle)$ (called the *computational basis*). The situation can be mimicked by choosing for the Hilbert space simply $\mathbb{C}^2$ and for the members of the distinguished basis the standard basis $|0\rangle = (1, 0)$ and $|1\rangle = (0, 1)$. Typically a qubit is a spin-1/2 particle, a two-level atom or a polarized photon.

In recent years a great deal of interest has been focused on the theory of a *pair* of qubits. The mathematical structure underlying the physics of this simplest of all *composite* quantum mechanical systems is far from being trivial. This is by no means surprising, considering that such counterintuitive phenomena as the EPR paradox must be describable with the help of the mathematical language associated

[1] Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada.

with such a system. However, owing to the effort of many mathematically sophisticated researchers such as the members of the Horodecki family (Horodecki and Horodecki, 1996; Horodecki *et al.*, 1996a,b) and W. K. Wootters (1997, 1998), considerable progress has been made in uncovering the salient features of the mathematical structure underlying the system consisting of a pair of qubits. In this paper we present in a unified fashion some mathematical results that have been unearthed by these researchers and add some of our own.

Inspired by the pioneering work of Horodecki and Horodecki (1996) and Horodecki *et al.* (1996a,b) we investigated in an earlier paper (Kummer, 1999) the state space of a pair of qubits (spin-1/2 particles). In the present paper we widen and deepen our investigation.

The Hilbert space of a pair of qubits can be identified with $\mathbb{C}^2 \otimes \mathbb{C}^2$. The two major questions that we pursue in this paper are

Question 1: What conditions guarantee that a given hermitian operator (of trace 1) in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is a state, that is, positive semidefinite?

Question 2: What conditions guarantee that a given state is *separable*, that is, it can be represented as a convex combination of products of one-particle states.

In order to tackle these questions it is useful to observe that $\mathbb{C}^2 \otimes \mathbb{C}^2$ carries a representation of the direct product $U_1 \times U_1$ of the special unitary group $U_1 = SU(2)$ with itself.

In section 2 we introduce those fundamentals of the theory of the group U_1 that are needed for the arguments in this paper. We also describe an interesting connection between a modified version of the so-called *Bell basis* in $\mathbb{C}^2 \otimes \mathbb{C}^2$ and that basis of the space $\mathcal{M}_2$ of all complex 2×2 matrices that consists of the identity matrix and the three Pauli matrices.

The answer to both of the above questions can be given in terms of the invariants of an hermitian operator in $\mathbb{C}^2 \otimes \mathbb{C}^2$ with respect to the group $U_1 \times U_1$. These invariants are encapsulated in the *canonical form*, which we introduce in section 3 (Definition 3.1).

In section 4 we construct positive semidefinite hermitian operators by squaring a general hermitian operator. This method immediately reveals a number of symmetries of the two-particle state space (Corollary 4.4). In addition we describe in this section the structure of a general pure state. The orbits of pure states under the group $U_1 \times U_1$ can be labeled by a single parameter ξ that varies over the interval [0, 1]. ξ is called the *concurrence* and measures the degree to which the two qubits are entangled after they have been prepared into the pure state.

Section 5 presents some results on separable states. Horodecki *et al.* (1996a) proved that a state of a pair of qubits is separable iff its partial transposition is still positive semidefinite. We express this condition in a form that is different and better adapted to the way we represent the hermitian operators in $\mathbb{C}^2 \otimes \mathbb{C}^2$ (Theorem 5.2). Another characterization of a separable state that makes use of the concept of a *Bell observable* (Definition 5.5) is given by Theorem 5.6.

Section 6 is devoted to the so-called states with *maximal disorder of the subsystems or mds states* (also called T states or generalized Bell states) introduced by Horodecki *et al.* (1996a). They can be alternatively described as states whose reduced density operators are given by $\frac{1}{2}\mathbf{1}$ or as states that are *invariant with respect to time reversal*. These states are particularly well-adapted to the group $U_1 \times U_1$, because they can be brought to diagonal form by conjugation with an element of that group. Some results of this section can be found in a different form in Horodecki *et al.* (1996b).

In section 7 we investigate the matrices of a hermitian operator h relative to two bases: the Bell basis and an eigenbasis of its mds component (cf. Definition 4.3). It turns out that time reversal of h is represented by *complex conjugation* (or *transposition*) of its matrix relative to the *Bell basis* (Theorem 7.1). Denoting the matrix of an operator ρ of trace 1 relative to an eigenbasis of its mds component by $[\rho]_\psi$ the condition for ρ to be a state now takes the form of the principal subdeterminants of $[\rho]_\psi$ having to be nonnegative (Theorem 7.3). We also give a necessary condition for a state to be nonseparable (Theorem 7.4).

In section 8 we propose a new measure of entanglement for mixed states that generalizes the *concurrence* defined for pure states in section 4. Our extension of the concurrence function (Definition 8.3) to mixed states slightly differs from the one defined by Wootters (1998), although the two functions agree on all mds states.

Section 9 exhibits some examples that are partially adapted from Horodecki *et al.* (1996a).

In section 10, we use the mathematical language developed in the bulk of the paper to express the answers to some questions concerning a pair of spin-1/2 particles.

2. PRELIMINARIES ON THE SPECIAL UNITARY GROUP: THE PAULI MATRICES AND THE (MODIFIED) BELL-BASIS

The Hilbert space of one qubit is $\mathbb{C}^2$ and the set of all linear operators in $\mathbb{C}^2$ can be identified with the algebra $\mathcal{M}_2$ of all complex 2×2 matrices. $\mathcal{M}_2$ can be made into a Hilbert space by introducing the sesquilinear form:

$$\langle a, b\rangle = \mathrm{trace}(a^* b) \quad a, b \in \mathcal{M}_2 \tag{2.1}$$

$\mathcal{M}_2$ carries an irreducible representation of the direct product $U_1 \times U_1$ of the special unitary group $U_1 = SU(2)$ by itself. U_1 is defined as the group of all 2×2 matrices of the form

$$u = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. The complex conjugation

$$u \mapsto \bar{u} \quad u \in U_1$$

is an automorphism of U_1. In fact it is an *inner* automorphism implemented by conjugation with the element

$$u_0 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{2.2}$$

Indeed, one easily verifies that

$$u_0 \cdot u \cdot u_0^* = \bar{u} \quad u \in U_1$$

$U_1 \times U_1$ acts on $\mathcal{M}_2$ by the following rule

$$(u_1, u_2)(a) = u_1 \cdot a \cdot u_2^* \quad a \in \mathcal{M}_2 \;\; (u_1, u_2) \in U_1 \times U_1$$

The Hilbert space of a *pair* of qubits, $\mathbb{C}^2 \otimes \mathbb{C}^2$, is also the carrier space of a representation of the direct product $U_1 \times U_1$, defined by

$$(u_1, u_2) \mapsto u_1 \otimes u_2 \quad (u_1, u_2) \in U_1 \times U_1 \tag{2.3}$$

It turns out that the two representations of $U_1 \times U_1$ are *equivalent*, that is, there exists an isomorphism of $U_1 \times U_1$ modules between $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{M}_2$.

Proposition 2.1. *The linear map $\varphi : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathcal{M}_2$ defined on decomposable vectors by*

$$\varphi(x \otimes y) = x \cdot (u_0 \cdot y)^t \quad x, y \in \mathbb{C}^2$$

is an isomorphism of U_1 modules and an isometry. Here we think of the elements of $\mathbb{C}^2$ as 2×1 matrices and the superscript t symbolizes the transpose.

Proof: First of all $(x, y) \mapsto x \cdot (u_0 \cdot y)^t$ is clearly bilinear and therefore φ can be extended as a linear map to all of $\mathbb{C}^2 \otimes \mathbb{C}^2$. Identifying the *computational basis* of a qub*it* $(|0\rangle, |1\rangle)$ *with* the standard basis in $\mathbb{C}^2$ we have for $j, k = 0, 1$

$$\varphi(|j\rangle \otimes u_0^* |k\rangle) = |j\rangle\langle k|,$$

which shows that all four matrix units are in the range of φ, making it evident that φ is surjective. Furthermore we have for all $(u_1, u_2) \in U_1 \times U_1$ and for all $x, y \in \mathbb{C}^2$

$$\begin{aligned} \varphi((u_1, u_2)(x \otimes y)) &= u_1 \cdot x \cdot (u_0 \cdot u_2 \cdot y)^t = u_1 \cdot x \cdot (\overline{u_2} \cdot u_0 \cdot y)^t \\ &= u_1 \cdot x \cdot (u_0 \cdot y)^t \cdot u_2^* = u_1 \cdot \varphi(x \otimes y) \cdot u_2^* \\ &= (u_1, u_2)(\varphi(x \otimes y)) \end{aligned}$$

and thus φ is an isomorphism of $U_1 \times U_1$ modules. Finally, we have for all x, $y \in \mathbb{C}^2$

$$\|\varphi(x \otimes y)\|^2 = \|x\|^2 \operatorname{trace}\big(u_0 y y^* u_0^*\big) = \|x\|^2 \|y\|^2 = \|x \otimes y\|^2$$

proving that φ is an isometry. □

There is a natural injection of U_1 into the direct product $U_1 \times U_1$ given by $u \mapsto (u, u)$, $u \in U_1$.

Composing this injection with the respective (irreducible) representations of $U_1 \times U_1$ on $\mathcal{M}_2$ and on $\mathbb{C}^2 \otimes \mathbb{C}^2$ we obtain a representation of U_1 that is the direct sum of the identity representation and a representation by rotation matrices. A distinguished basis in $\mathcal{M}_2$ adapted to this decomposition of $\mathcal{M}_2$ into irreducible subspaces consists of the identity matrix $\mathbf{1} = \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ supplemented by the three Pauli matrices:

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.4}$$

1 spans an invariant subspace carrying the identity representation, whereas the three Pauli matrices span a subspace that carries the representation of U_1 by rotation matrices $R(u)$. Accordingly $R(u)$ is defined via the equation

$$u\sigma_k u^* = \sum_{j=1}^{3} R(u)_{jk} \sigma_j, \quad k = 1, 2, 3 \;\; u \in U_1 \tag{2.5}$$

Using the inner product on $\mathcal{M}_2$ we can isolate the (j, k)-th matrix entry:

$$R(u)_{jk} = \frac{1}{2} \langle \sigma_j, u\sigma_k u^* \rangle = \frac{1}{2} \operatorname{trace}(\sigma_j u \sigma_k u^*), \quad j, k = 1, 2, 3 \tag{2.6}$$

Explicitly $R(u)$ is given by

$$R(u) = \begin{bmatrix} Re(\alpha^2 - \beta^2) & Im(\alpha^2 + \beta^2) & -2Re(\alpha\beta) \\ -Im(\alpha^2 - \underline{\ }\beta^2) & Re(\alpha^2 + \underline{\beta}^2) & 2Im(\alpha\beta) \\ 2Re(\alpha\beta) & 2Im(\alpha\beta) & (|\alpha|^2 - |\beta|^2) \end{bmatrix}$$

Since φ is an isometric isomorphism of U_1 modules, the image of the the orthonormal basis

$$\left(\frac{1}{\sqrt{2}} \mathbf{1}, \frac{1}{\sqrt{2}} \sigma_1, \frac{1}{\sqrt{2}} \sigma_2, \frac{1}{\sqrt{2}} \sigma_3 \right) \tag{2.7}$$

in $\mathcal{M}_2$ under φ^{-1} will be an orthonormal basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$ that is adapted to the decomposition of $\mathbb{C}^2 \otimes \mathbb{C}^2$ into irreducibleU_1 submodules. What is this basis? The answer is as follows: It is constituted by the following set of orthonormal vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\begin{aligned}\phi_0 &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\\ \phi_1 &= \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle)\\ \phi_2 &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\ \phi_3 &= \frac{-i}{\sqrt{2}}(|01\rangle + |10\rangle)\end{aligned} \tag{2.8}$$

(Here we use the customary abbreviation $|jk\rangle := |j\rangle \otimes |k\rangle$, $(j, k = 0, 1)$ for the members of the *computational basis* of a pair of qubits.)

Thus our basis agrees up to phase factors with the well-known *Bell basis* and we shall refer to it using this name. Our Bell basis is closely related to what Wootters (1997) calls the “magic basis.” The precise relationship between the distinguished basis in $\mathcal{M}_2$ and the Bell basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$ (as defined by us) is given by the following equations:

$$\begin{aligned}\varphi(\sqrt{2}\phi_0) &= \varphi(|\,01\rangle) - \varphi(|10\rangle) = |\,0\rangle\langle 0\,| + |1\rangle\langle 1| = \mathbf{1}\\ \varphi(\sqrt{2}i\phi_1) &= (\varphi(|11\rangle) - \varphi(|\,00\rangle) = |1\rangle\langle 0\,| + |\,0\rangle\langle 1| = \sigma_1\\ \varphi(\sqrt{2}i\phi_2) &= i(\varphi(|11\rangle) + \varphi(|\,00\rangle)) = i(|1\rangle\langle 0\,| - |\,0\rangle\langle 1|) = \sigma_2\\ \varphi(\sqrt{2}i\phi_3) &= (\varphi(|\,01\rangle) + \varphi(|10\rangle)) = |\,0\rangle\langle 0\,| - |1\rangle\langle 1| = \sigma_3\end{aligned}$$

Therefore

$$\varphi^{-1}\left(\frac{1}{\sqrt{2}}\mathbf{1}, \frac{1}{\sqrt{2}}\sigma_1, \frac{1}{\sqrt{2}}\sigma_2, \frac{1}{\sqrt{2}}\sigma_3\right) = (\phi_0, i\phi_1, i\phi_2, i\phi_3) \tag{2.9}$$

We now deduce from Proposition 2.1 that

$$(u \otimes u)\phi_0 = \phi_0$$

and

$$(u \otimes u)\phi_k = \sum_{j=1}^{3} R(u)_{jk}\phi_j, \quad k = 1, 2, 3$$

where the $R(u)_{jk}$ values are given by formula (2.6).

3. HERMITIAN OPERATORS, CANONICAL FORM

The *real* subspace of $\mathcal{M}_2$ spanned by the Pauli matrices and $\mathbf{1}$ coincides with the subspace $\mathcal{H}_2$ of all hermitian 2×2 matrices. Identifying an hermitian operator with its matrix with respect to the computational basis we shall think of the elements of $\mathcal{H}_2$ as (hermitian) operators in $\mathbb{C}^2$. Accordingly an hermitian operator $h \in \mathcal{H}_2$ can be written as

$$h(\gamma, \mathbf{r}) = \frac{1}{2}(\gamma \mathbf{1} + \mathbf{r} \cdot \sigma), \tag{3.1}$$

where $\gamma = \operatorname{trace}(h)$ is a real number, $\mathbf{r} = (r_1, r_2, r_3)$ is a real 3-vector, and $\mathbf{r} \cdot \sigma$ is defined by $\mathbf{r} \cdot \sigma = \sum_{j=1}^{3} r_j \sigma_j$. From (2.5) we deduce that $h(\gamma, \mathbf{r})$ transforms under conjugation by elements of the group U_1 according to the formula

$$uh(\gamma, \mathbf{r})u^* = h(\gamma, R(u)\mathbf{r}), \quad u \in U_1 \tag{3.2}$$

The spectrum of $h(\alpha, \mathbf{r})$ is given by

$$\operatorname{sp}(h(\gamma, \mathbf{r})) = \left\{ \frac{1}{2}(\gamma - \|\mathbf{r}\|), \frac{1}{2}(\gamma + \|\mathbf{r}\|) \right\}$$

Therefore the positive cone $\mathcal{H}_2^+$ of $\mathcal{H}_2$ can be described as

$$\mathcal{H}_2^+ = \{h(\gamma, \mathbf{r}) \mid \gamma \geq 0 \;\&\; \|\mathbf{r}\| \leq \gamma\}$$

Denoting by $\mathcal{H}_2^1$ the set of all hermitian operators of trace 1 a state of a qubit is described by an element $\rho(\mathbf{r}) = h(1, \mathbf{r})$ of the *state space*

$$\mathcal{H}_2^1 \cap \mathcal{H}_2^+ = \{\rho(\mathbf{r}) \mid \mathbf{r} \in B^3\}$$

where B^3 denotes the unit ball in $\mathbb{R}^3$. In fact the map $\mathbf{r} \mapsto \rho(\mathbf{r})$ is an affine bijection of B^3 onto $\mathcal{H}_2^1 \cap \mathcal{H}_2^+$. This implies that $\rho(\mathbf{r})$ is precisely a *pure state* of the 1-qubit system (i.e., a projection) if $\mathbf{r}$ belongs to the unit sphere S^2. Indeed, one easily checks that $\rho(\mathbf{r})^2 = \rho(\mathbf{r})$ iff $\|\mathbf{r}\| = 1$.

The representation (2.3) of the group $U_1 \times U_1$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ induces a representation of $U_1 \times U_1$ in the real vector space $\mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$ of all hermitian 2-qubit operators by conjugation. Accordingly we have an analogous decomposition of an element $h \in \mathcal{H}_4$ into irreducible components:

$$h(\gamma, \mathbf{r}, \mathbf{s}, T) := 1/4\left(\gamma(\mathbf{1} \otimes \mathbf{1}) + \mathbf{r} \cdot \sigma \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{s} \cdot \sigma + \sum_{j,k=1}^{3} t_{jk}\sigma_j \otimes \sigma_k\right) \tag{3.3}$$

Here $T = (t_{jk})$ is a real 3×3 matrix, $\mathbf{r}$ and $\mathbf{s}$ are real 3-vectors and $\gamma = \operatorname{trace}(h)$ again. $h(\gamma, \mathbf{r}, \mathbf{s}, T)$ transforms under conjugation by elements of the group $U_1 \times U_1$ via the formula

$$(u_1 \otimes u_2)h(\gamma, \mathbf{r}, \mathbf{s}, T)\big(u_1^* \otimes u_2^*\big) = h(\gamma, R(u_1)\mathbf{r}, R(u_2)\mathbf{s}, R(u_1)TR(u_2)^*)$$

We write $h(\gamma_2, \mathbf{r}_2, \mathbf{s}_2, T_2) \sim h(\gamma_1, \mathbf{r}_1, \mathbf{s}_1, T_1)$, provided the two hermitian operators are conjugate under the group $U_1 \times U_1$ and we say that the two operators are *equivalent* or *belong to the same orbit*. By a judicious choice of $(u_1 \otimes u_2) \in U_1 \times U_1$ we can achieve $R(u_1)TR(u_2)^* = \pm D$ where $D = \mathrm{diag}(\mu_1, \mu_2, \mu_3)$ and $\mu_1 \geq \mu_2 \geq \mu_3 \geq 0$ are the three singular values of T, that is, the eigenvalues of the matrix $[T] = (T^*T)^{\frac{1}{2}}$.

Definition 3.1. A *canonical form* for the hermitian operator $h(\gamma, \mathbf{r}, \mathbf{s}, T)$ is any hermitian operator $h(\gamma, \mathbf{r}', \mathbf{s}', \pm D) \sim h(\gamma, \mathbf{r}, \mathbf{s}, T)$ where $D = \mathrm{diag}(\mu_1, \mu_2, \mu_3)$ is the diagonal matrix whose diagonal entries are the three singular values of T in descending order.

Proposition 3.2 *(Existence of a canonical form). Given any hermitian operator $h(\gamma, \mathbf{r}, \mathbf{s}, T)$, there exists a canonical form $h(\gamma, \mathbf{r}', \mathbf{s}', \varepsilon D)$ with $\varepsilon \in \{+1, -1\}$.*

If $\det T > 0$ then $\varepsilon = +1$ and if $\det T < 0$ then $\varepsilon = -1$.

If $\det T = 0$ then ε can be chosen to be $+1$ or -1, whereby the vectors $\mathbf{r}'$ and $\mathbf{s}'$ in general will depend on the choice of ε. More precisely, if $h(\gamma, \mathbf{r}', \mathbf{s}', \varepsilon D)$ is a canonical form of $h(\gamma, \mathbf{r}, \mathbf{s}, T)$ then so is $h(\gamma, F_3\mathbf{r}', \mathbf{s}', -\varepsilon D)$, where $F_3 = \mathrm{diag}(-1, -1, 1)$ denotes the 180° flip about the third coordinate axis.

Proof: (i) $\det T > 0$. By the singular decomposition theorem (cf. Horn and Johnson, 1985) there exist rotation matrices (R_1, R_2) such that $R_1TR_2^* = D$. Let $u_k \in U_1 (k = 1, 2)$ be such that $R(u_k) = R_k$, $k = 1, 2$. Then putting $\mathbf{r}' = R_1\mathbf{r}$ and $\mathbf{s}' = R_2\mathbf{s}$, we have

$$(u_1 \otimes u_2)h(\gamma, \mathbf{r}, \mathbf{s}, T)(u_1^* \otimes u_2^*) = h(\gamma, R_1\mathbf{r}, R_2\mathbf{s}, D) = h(\gamma, \mathbf{r}', \mathbf{s}', D)$$

and thus $h(\gamma, \mathbf{r}, \mathbf{s}, T) \sim h(\gamma, \mathbf{r}', \mathbf{s}', D)$.

(ii) $\det T < 0$. In this case the singular decomposition theorem yields a pair of rotation matrices (R_1, R_2) such that $R_1TR_2^* = -D$. The remainder of the argument is the same.

(iii) $\det T = 0$. In this case the singular decomposition theorem gives us again a pair of rotation matrices (R_1, R_2) such that $R_1TR_2^* = D$ and therefore $F_3R_1TR_2^* = -D$. Putting $\mathbf{r}' = R_1\mathbf{r}$ and $\mathbf{s}' = R_2\mathbf{s}$ we get

$$h(\gamma, \mathbf{r}, \mathbf{s}, T) \sim h(\gamma, \mathbf{r}', \mathbf{s}', D) \sim h(\gamma, F_3\mathbf{r}', \mathbf{s}', -D)$$

On the other hand if we put $\mathbf{r}' = F_3R_1\mathbf{r}$ and $\mathbf{s}' = R_2\mathbf{s}$ we obtain

$$h(\gamma, \mathbf{r}, \mathbf{s}, T) \sim h(\gamma, \mathbf{r}', \mathbf{s}', -D) \sim h(\gamma, F_3\mathbf{r}', \mathbf{s}', D) \quad \square$$

The question arises to what extent the vectors $\mathbf{r}'$ and $\mathbf{s}'$ that occur in a canonical form are *unique*. To answer this question we introduce the *stabilizer*

$$H_D := \{(R_1, R_2) \in SO(3) \times SO(3) \mid R_1 D R_2^* = D\}$$

of D. The following proposition is immediate.

Proposition 3.3. *Let $h = h(\gamma, \mathbf{r}, \mathbf{s}, T)$ be an hermitian operator and let $h(\gamma, \mathbf{r}', \mathbf{s}', \varepsilon D)$ be a canonical form. Then the most general canonical form of h (with the same value of ε) is given by $h' = h(\gamma, R_1\mathbf{r}', R_2\mathbf{s}', \varepsilon D)$, where (R_1, R_2) varies over the stabilizer H_D.*

The stabilizer H_D is actually a subgroup of the group $G \times G$ where G is the *commutant group*, namely the group of all rotations that commute with D:

$$G := \{R \in SO(3) \mid RD = DR\}$$

Indeed, it follows from Proposition A.2 (of Appendix A) that

$$H_D = \{(R_1, R_2) \in G \times G \mid R_1 \equiv R_2 \mod G'\} \tag{3.4}$$

where G' denotes the *invariance group*, namely the group of all rotations that leave D fixed by multiplication from the left:

$$G' := \{R \in SO(3) \mid RD = D\}$$

Note that G' is a normal subgroup of G (cf. Proposition A.2). The invariance group G' depends on the rank of D, which of course coincides with the rank of T. In case T has rank 2 or 3, G' is the trivial group that in view of (3.4) implies that $H_D = \Delta(G) := \{(R, R) \mid R \in G\}$. In case T has rank 1, G' coincides with the group $SO_1(2)$ of all rotations about the first coordinate axis. (More generally we shall use the symbol $SO_k(2)$, $k = 1, 2, 3$, to denote the group of all rotations about the kth coordinate axis). Finally if $T = 0$ then $G' = G = SO(3)$.

The commutant group G depends on the degeneracy of the singular values. If all three singular values are different then

$$G = \{F_0, F_1, F_2, F_3)$$

where

$$F_1 = \mathrm{diag}(1, -1, -1)$$

$$F_2 = \mathrm{diag}(-1, 1 - 1)$$

$$F_3 = \mathrm{diag}(-1, -1, 1)$$

are the 180° flips about the three coordinate axes and $F_0 = I$ is the identity matrix. Clearly in this special case G is an instance of the *four-group* $\mathcal{V}$. The following table summarizes the situation:

Rank of T	Possible commutant group G	Invariance group G'
3	$\mathcal{V}, \widetilde{SO}_3(2), \widetilde{SO}_1(2), SO(3)$	$\{I\}$
2	$\mathcal{V}$ or $\widetilde{SO}_3(2)$	$\{I\}$
1	$\widetilde{SO}_1(2)$	$SO_1(2)$
0	$SO(3)$	$SO(3)$

Here $\widetilde{SO}_k(2)$, $k = 1, 3$ stands for the subgroup of the rotation group $SO(3)$ generated by $SO_k(2)$ and F_2.

As we shall see the canonical form turns out to be useful for the characterization of the positive cone $\mathcal{H}_4^+ \subset \mathcal{H}_4$. $\mathcal{H}_4^+$ is a self-dual cone relative to the trace inner product:

$$\langle h, h'\rangle = \mathrm{trace}(hh'), \quad h, h' \in \mathcal{H}_4 \tag{3.5}$$

For the hermitian operators of trace 1 we use the symbol ρ:

$$\rho = \rho(\mathbf{r}, \mathbf{s}, T) = h(1, \mathbf{r}, \mathbf{s}, T)$$

The set $\mathcal{H}_4^1$ of all hermitian operators of trace 1 constitutes a hyperplane in $\mathcal{H}_4$. A hermitian operator that belongs to the intersection $\mathcal{H}_4^+ \cap \mathcal{H}_4^1$ is a *state* of the 2-qubit system. The *state space* $\mathcal{S} = \mathcal{H}_4^+ \cap \mathcal{H}_4^1$ is a compact convex set whose extreme points are the one-dimensional projections, the *pure states*. A state is called *separable* provided it belongs to the convex hull of all pure states of the form $\rho(\mathbf{r}) \otimes \rho(\mathbf{s})$, where $\rho(\mathbf{r})$ and $\rho(\mathbf{s})\,(\mathbf{r}, \mathbf{s} \in S^2)$ are 1-qubit pure states, that is, projections in one-particle space $\mathbb{C}^2$. In the usual formulation of Quantum Mechanics there corresponds to each state a *state in the physical sense*, which can be thought of as a catalogue containing the total information about the system. We ascribe to the system a pure state provided we possess maximal information about it. We ascribe to the system a separable state provided the two qubits are *classically correlated*.

We can now reformulate the two central problems that we address in this paper as follows:

Problem 1: Describe conditions that guarantee that a given hermitian operator $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ of trace 1 is a state.

Problem 2: Describe conditions that guarantee that a given state $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a separable state.

Definition 3.4. Suppose $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a state of a pair of qubits. The 3-vectors $\mathbf{r}$ and $\mathbf{s}$ are called the *one-particle vectors* and the 3×3 matrix $T = T_\rho$ is called the *correlation matrix* of ρ. The singular values $\mu_1 \geq \mu_2 \geq \mu_3$ of T_ρ are called the *correlation values* of the state ρ.

The physical significance of the one-particle vectors becomes clear if we compute the *reduced states*

$$\rho_1 = \text{trace}_2 \rho(\mathbf{r}, \mathbf{s}, T) = \frac{1}{2}(\mathbf{1} + \mathbf{r} \cdot \sigma) = \rho(\mathbf{r}) \tag{3.6}$$

and

$$\rho_2 = \text{trace}_1 \rho(\mathbf{r}, \mathbf{s}, T) = \frac{1}{2}(\mathbf{1} + \mathbf{s} \cdot \sigma) = \rho(\mathbf{s}) \tag{3.7}$$

Since $\rho(\mathbf{r})$ and $\rho(\mathbf{s})$ are one particle *states* we immediately obtain the following:

Proposition 3.5. *If* $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ *is a state then* $\mathbf{r}, \mathbf{s} \in B^3$.

In a subsequent section we shall sharpen this result by imposing a condition on the correlation matrix T also (cf. Corollary 6.4).

The one-particle vectors $\mathbf{r}$ and $\mathbf{s}$ encapsulate the information we possess about the two individual constituent qubits after the system has been prepared into the state ρ. This information is minimal if $\mathbf{r} = \mathbf{s} = \mathbf{0}$. Following Horodecki and Horodecki (1996) we call a state of the form $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ a *state of maximal disorder of the subsystems* or an *mds state*. Likewise we call a general operator of the form $h = h(\gamma, \mathbf{0}, \mathbf{0}, T)$ an *mds operator*. Note that the mds states can also be characterized as those states of the pair of qubits that are *invariant with respect to time reversal*.

What about the physical significance of the correlation matrix T? It is related to the measurement of observables of type $\mathbf{a} \cdot \sigma \otimes \mathbf{b} \cdot \sigma$ where $\mathbf{a}, \mathbf{b} \in \mathbb{R}^3$ are *unit vectors*. In the case of a pair of spin-1/2 particles, measuring the observable $\mathbf{a} \cdot \sigma \otimes \mathbf{b} \cdot \sigma$ means the simultaneous measurement of the spin component of Particle 1 in direction $\mathbf{a}$ and the spin component of Particle 2 in direction $\mathbf{b}$. The expectation value of this observable in the state $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is

$$\langle \rho, \mathbf{a} \cdot \sigma \otimes \mathbf{b} \cdot \sigma \rangle = \mathbf{a} \cdot T\, \mathbf{b} \tag{3.8}$$

In particular the (j, k)-th entry of T is given by

$$t_{jk} = \langle \rho, \sigma_j \otimes \sigma_k \rangle \tag{3.9}$$

Since the eigenvalues of $\mathbf{a}\cdot\sigma\otimes\mathbf{b}\cdot\sigma$ are ± 1 we can conclude that the entries of a correlation matrix must lie in the interval $[-1, 1]$. Substituting in (3.9) for the state ρ its canonical form ρ', we obtain the following.

Proposition 3.6. *The correlation values of a state lie in the interval* $[0, 1]$.

Later we shall sharpen this result considerably (cf. Theorem 6.2 (2)).

Finally before leaving this section we should mention that both problems described above have been completely solved for mds operators (Horodecki and Horodecki, 1996; Horodecki *et al.*, 1996a,b).

4. THE SQUARING OF AN OPERATOR AND PURE STATES

In this section we turn toward the question of how to construct hermitian operators that are states. As is well-known, by squaring any hermitian operators we obtain a positive semidefinite operator and every positive semidefinite operator is obtained this way. Let us look first at the case of one qubit.

We get an arbitrary state by squaring an hermitian operator of the Form (3.1) and making sure that the result has trace 1. In the case of one qubit we obtain

$$h(\gamma, \mathbf{r})^2 = h\left(\frac{1}{2}(\gamma^2 + \|\mathbf{r}\|^2), \gamma\mathbf{r}\right) \tag{4.1}$$

Theorem 4.1. *Let* $\mathbf{r}$ *be a 3-vector with* $\|\mathbf{r}\| \leq \sqrt{2}$. *Let* $\gamma_0 = \sqrt{2 - \|\mathbf{r}\|^2}$. *Then* $\rho(\gamma_0\mathbf{r})$ *is a state and every state can be obtained in this way.*

Since the assignment $\mathbf{r} \mapsto \gamma_0\mathbf{r}$ maps the ball of radius $\sqrt{2}$ into the unit ball (leaving the unit sphere pointwise fixed) this theorem expresses in an indirect way the familiar result that $\rho(\mathbf{r})$ is a state iff $\|\mathbf{r}\| \leq 1$. Using Formula (4.1) we also can rederive the result that $\rho(\mathbf{r})^2 = \rho(\mathbf{r})$ iff $\|\mathbf{r}\| = 1$. *Thus in the case of one qubit the method of squaring yields nothing new*. However, in the case of a pair qubits the same method yields some nontrivial results.

Theorem 4.2. *Given any triple* $(\mathbf{r}, \mathbf{s}, T)$, *where* $\mathbf{r}$ *and* $\mathbf{s}$ *are 3-vectors and* T *is a* 3×3 *matrix such that*

$$\|\mathbf{r}\|^2 + \|\mathbf{s}\|^2 + \mathrm{trace}(T^*T) \leq 4$$

(This is a ball of radius 2 *in* 15*-dimensional space), the operator*

$$\rho = \rho\left(\frac{1}{2}(\gamma_0\mathbf{r} + T\mathbf{s}), \frac{1}{2}(\gamma_0\mathbf{s} + T^*\mathbf{r}), \frac{1}{2}(\gamma_0 T - \mathrm{cofac}(T) + |\,\mathbf{r} >< \mathbf{s}\,|)\right)$$

where γ_0 is defined by

$$\gamma_0 = \sqrt{4 - \|\mathbf{r}\|^2 - \|\mathbf{s}\|^2 - \mathrm{trace}(T^*T)}$$

is a state and every state is obtained this way. Here cofac(T) stands for the matrix whose (j, k)-th entry is the cofactor of the (j, k)-th entry of T.

Proof: For the proof we observe that squaring an operator of the form (3.3) yields

$$h^2 = h\left(\frac{1}{4}(\gamma^2 + \|\mathbf{r}\|^2 + \|\mathbf{s}\|^2 + \mathrm{trace}(T^*T)),\ \frac{1}{2}(\gamma\mathbf{r} + T\mathbf{s}),\ \frac{1}{2}(\gamma\mathbf{s} + T^*\mathbf{r}),\ \frac{1}{2}C\right), \tag{4.2}$$

where $C = (c_{jk})$ and

$$c_{jk} = \gamma t_{jk} - (\mathrm{cofac}T)_{jk} + r_j s_k \quad \square$$

Equation (4.2) implies that

$$\mathrm{trace}(h^2) = \frac{1}{4}(\gamma^2 + \|\mathbf{r}\|^2 + \|\mathbf{s}\|^2 + \mathrm{trace}(T^*T)) \tag{4.3}$$

By polarization of this equation we obtain

$$\mathrm{trace}(hh') = \frac{1}{4}(\gamma\gamma' + \mathbf{r}\cdot\mathbf{r}' + \mathbf{s}\cdot\mathbf{s}' + \mathrm{trace}(T^*T')) \tag{4.4}$$

It is useful to introduce the following linear involutions into $\mathcal{H}_4$

$$h \mapsto h^{\#} = h(\gamma, -\mathbf{r}, -\mathbf{s}, T) \quad \text{and} \quad h \mapsto h^{(p)} = h(\gamma, \mathbf{s}, \mathbf{r}, T^*), \qquad h \in \mathcal{H}_4$$

Physically (if h designates an observable or a state) the map $h \mapsto h^{\#}$ is nothing but the *time reversal operation.*

Definition 4.3. If $h = h(\gamma, \mathbf{r}, \mathbf{s}, T) \in \mathcal{H}_4$ we shall refer to $h^{\#}$ as the *time-reversed operator* and to $h^{(p)}$ as the *particle-transposed* or *p-transposed operator*. h is called an *mds operator* provided $h^{\#} = h$ and if h is any hermitian operator its time reversal invariant part $h^{mds} = \frac{1}{2}(h + h^{\#}) = h(\gamma, \mathbf{0}, \mathbf{0}, T)$ is called the *mds component of* h. Finally h is said to be *particle symmetric* or *p symmetric* if $h^{(p)} = h$.

Remark. Note that our choice of the word “p transposed” and “p symmetric,” clumsy as it seems at first, is necessary, since by our identification of an hermitian operator h in $\mathbb{C}^2 \otimes \mathbb{C}^2$ with its matrix relative to the computational basis, the concepts “transposed” and “symmetric” already have a meaning different from “p transposed” and “p symmetric.”

Observe that it follows from (4.4) that the involutions $h \mapsto h^{\#}$ and $h \mapsto h^{(p)}$ are self-adjoint relative to the inner product defined by Eq. (3.5), that is, we have

$$\langle h^{\#}, h' \rangle = \langle h, h'^{\#} \rangle, \quad h, h' \in \mathcal{H}_4 \tag{4.5}$$

and

$$\langle h^{(p)}, h' \rangle = \langle h, h'^{(p)} \rangle, \quad h, h' \in \mathcal{H}_4 \tag{4.6}$$

The following corollary is an immediate consequence of Theorem 4.2:

Corollary 4.4. *If $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a state then so is $\rho^{\#}$ (called the* time reversed *state) and $\rho^{(p)}$ (called the* p-transposed *state). Moreover the mds component $\rho^{mds} = \rho(\mathbf{0}, \mathbf{0}, T)$ of ρ is a state.*

Proof: To show that $\rho^{(p)}$ is a state just interchange $\mathbf{r}$ and $\mathbf{s}$ and replace T by T^* in Theorem 4.2, observing that $\text{cofac}(T^*) = (\text{cofac}T)^*$. To show that $p^{\#}$ is a state replace $\mathbf{r}$ and $\mathbf{s}$ by $-\mathbf{r}$ and $-\mathbf{s}$ respectively. Finally it is clear that the mds component of ρ, being a weighted mean of two states, is a state. □

The following theorem characterizes the idempotent operators of the form $\rho(\mathbf{r}, \mathbf{s}, T)$ (pure states of the 2-qubit system):

Theorem 4.5. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be an hermitian operator of trace* 1. *Then ρ is a pure state ($i.e.,\ \rho^2 = \rho$) iff for some vector* s *with $\|\mathbf{s}\| \leq 1$ and some rotation matrix R*

$$\mathbf{r} = -R\mathbf{s}$$

$$T = -R\big((\sqrt{1 - \|\mathbf{s}\|^2})(I - E_{\mathbf{s}}) + E_{\mathbf{s}}\big) \tag{4.7}$$

where for $\mathbf{s} \neq \mathbf{0}$ $E_{\mathbf{s}}$ denotes the projection in $\mathbb{R}^3$ onto the one-dimensional subspace generated by s. *In other words, the map*

$$(\mathbf{s}, R) \mapsto P_{\mathbf{s},R} := \rho\big(-Rs, \mathbf{s}, -R\big(\sqrt{1 - \|\mathbf{s}\|^2}(I - E_{\mathbf{s}}) + E_{\mathbf{s}}\big)\big)$$

is a parameterization of the set of pure states of the pair of qubits by the points of $B^3 \times SO(3)$ where B^3 denotes the unit ball in $\mathbb{R}^3$. Furthermore $P_{\mathbf{s},R}$ and $P_{\mathbf{s}',R'}$ belong to the same orbit iff $\|\mathbf{s}'\| = \|\mathbf{s}\|$.

Proof: Using Eq. (4.2) the condition $\rho^2 = \rho$ yields

$$\|\mathbf{r}\|^2 + \|\mathbf{s}\|^2 + \text{trace}(T^*T) = 3$$

$$\mathbf{r} = T\mathbf{s} \qquad \mathbf{s} = T^*\mathbf{r} \tag{4.8}$$

$$T^* = |\,\mathbf{s}\rangle\langle\mathbf{r}\,| - (\mathrm{cofac}(T))^*$$

Multiplying the last equation from the right by T^* and making use of the second equation gives

$$T^*T = |\mathbf{s}\rangle\langle\mathbf{s}| - T(\mathrm{cofac}(T))^* = |\mathbf{s}\rangle\langle\mathbf{s}| - (\det T)I$$

Hence

$$T^*T + (\det T)I = |\mathbf{s}\rangle\langle\mathbf{s}| \tag{4.9}$$

Similarly,

$$TT^* + (\det T)I = |\mathbf{r}\rangle\langle\mathbf{r}| \tag{4.10}$$

Now from the second of the Eq. (4.8) we deduce that

$$\|\mathbf{r}\|^2 = \mathbf{r}\cdot T\mathbf{s} = \mathbf{s}\cdot T^*\mathbf{r} = \|\mathbf{s}\|^2 \tag{4.11}$$

Inserting this into the first equation of (4.8) and combining it with the equation obtained from taking the trace in (4.9) we obtain

$$\det T = \|\mathbf{s}\|^2 - 1 \tag{4.12}$$

From Eq. (4.9) or (4.10) we conclude that det $T \leq 0$, which implies the already familiar result $\|\mathbf{s}\| \leq 1$. Equation (4.9) can now be rewritten as

$$[T]^2 = \|\mathbf{s}\|^2 E_{\mathbf{s}} + \big(1 - \|\mathbf{s}\|^2\big)I = \big(1 - \|\mathbf{s}\|^2\big)(I - E_{\mathbf{s}}) + E_{\mathbf{s}}$$

It follows that

$$[T] = \sqrt{1 - \|\mathbf{s}\|^2}(I - E_{\mathbf{s}}) + E_{\mathbf{s}} \tag{4.13}$$

Now by the polar decomposition theorem there exists $R \in SO(3)$ such that $T = -R[T]$. Finally $\mathbf{r} = T\mathbf{s} = -R\mathbf{s}$. The condition $\|\mathbf{s}\| = \|\mathbf{s}'\|$ is clearly necessary for $P_{\mathbf{s},R}$ and $P_{\mathbf{s}',R}$ to be equivalent. Since a canonical form of $P_{\mathbf{s},R}$ is given by

$$P' = P_{\|\mathbf{s}\|\mathbf{e}_1, I} = \rho(-\|\mathbf{s}\|\mathbf{e}_1, \|\mathbf{s}\|\mathbf{e}_1, -\mathrm{diag}\big(1, \sqrt{1 - \|\mathbf{s}\|^2}, \sqrt{1 - \|\mathbf{s}\|^2}\big) \tag{4.14}$$

the condition is also sufficient. □

Following Wootters (1997) we call the number $\xi = \sqrt{1 - \|\mathbf{s}\|^2}$ the *concurrence* of the pure state $P_{\mathbf{s},R}$. The number ξ varies over the interval [0, 1] and measures the degree of entanglement between the two qubits. For fixed $0 \leq \xi \leq 1$ let $\mathcal{P}_\xi$ denote the orbit of all pure states with concurrence ξ and let $\mathcal{S}_\xi$ denote convex hull of $\mathcal{P}_\xi$: $\mathcal{S}_\xi = \mathrm{conv}\mathcal{P}_\xi$.

Note that $\mathcal{P}_\xi$ coincides with the set of all extreme points of $\mathcal{S}_\xi$. (Proof: Theorem A.3)

Theorem 4.6. *(1) The orbit $\mathcal{P}_\xi$ is invariant under the involutions $\rho \mapsto \rho^\#$ and $\rho \mapsto \rho^{(p)}$: If P is a pure state of concurrence ξ then so is the time reversed state $P^\#$ and the p transposed state $P^{(p)}$.*

(2) The convex set $\mathcal{S}_\xi$ is invariant under the involutions $\rho \mapsto \rho^\#$ and $\rho \mapsto \rho^{(p)}$: If the state ρ is a mixture of pure states of concurrence ξ then so is the time reversed state $p^\#$ and the p-transposed state $p^{(p)}$.

Proof: (1) Suppose $P = P_{\mathbf{s},R}$. Then $P^\# = P_{-\mathbf{s},R}$ and $P^{(p)} = P_{\mathbf{v},R^*}$ where $\mathbf{v} = -R\mathbf{s}$.

(2) The assertion is an immediate consequence of Part (1) and the affine character of the involutions $\rho \mapsto \rho^\#$ and $\rho \mapsto \rho^{(p)}$. □

There are two interesting special cases: The set $\mathcal{P}_1$ of pure states corresponding to the points of $SO(3)$ and the set $\mathcal{P}_0$ of the pure states corresponding to the points of $S^2 \times SO(3)$. $\mathcal{P}_0$ comprises the set of all pure states of the product type $\rho = \rho(\mathbf{r}) \otimes \rho(\mathbf{s})$, (where $\mathbf{r}$ and $\mathbf{s}$ are unit vectors) and therefore $\mathcal{S}_0$ coincides with the set of all *separable* states. On the other hand $\mathcal{P}_1$ comprises the set of pure states of the form $\rho = \rho(\mathbf{0}, \mathbf{0}, -R) = P_{\mathbf{0},R}$, and we shall call such a pure state a *pure state of mds type*. It follows that $\mathcal{S}_1$ consists of mds states; as a matter of fact $\mathcal{S}_1$ exhausts the set of all mds states. This follows from the following proposition:

Proposition 4.7. *Let $\mathcal{T}$ denote the set of all correlation matrices. Then*

$$\mathcal{T} = \mathrm{conv}(-SO(3))$$

Proof: Clearly $\mathrm{conv}(-SO(3)) \subset \mathcal{T}$ since for all $R \in SO(3) - R \in \mathcal{T}$ and $\mathcal{T}$ is convex. Conversely, using Eqs. (4.7) and (4.13) we see that every correlation matrix of a *pure state* belongs to $\mathrm{conv}(-SO(3))$. Indeed since for $\mathbf{s} \neq \mathbf{0}$ $E_\mathbf{s} = \frac{1}{2}(I + F_\mathbf{s})$ where $F_\mathbf{s}$ stands for the flip by π about the axis spanned by the vector $\mathbf{s}$ we have for $\xi \in [0, 1]$

$$\xi(I - E_\mathbf{s}) + E_\mathbf{s} = \frac{1}{2}(1 + \xi)I + \frac{1}{2}(1 - \xi)F_\mathbf{s}$$

Now it follows from Eq. (4.13) that $[T]$ is a weighted mean of the identity matrix I and the flip $F_\mathbf{s}$. Therefore $T(= -R[T])$ itself is a weighted mean of $-R$ and $-RF_\mathbf{s}$.

Finally since the correlation matrix T_ρ of an arbitrary state ρ can be written as a weighted mean of the correlation matrices of at most four orthogonal pure states (apply the spectral theorem to ρ) the assertion follows. □

Now let $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ be an arbitrary mds state. Then by the proposition $T_\rho = T \in \mathrm{conv}(-SO(3))$ and therefore $\rho \in \mathcal{S}_1$.

Remark 4.8. If T is any correlation matrix the mds operator $\rho(\mathbf{0}, \mathbf{0}, T)$ is a state. (Indeed if T is a correlation matrix then by definition, for some vectors $\mathbf{r}, \mathbf{s} \in B^3$, $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a state; but then $p^{mds} = p(\mathbf{0}, \mathbf{0}, T)$ is also a state, by Corollary 4.4). Moreover the map $T \mapsto \rho(\mathbf{0}, \mathbf{0}, T)$ is an affine injection of $\mathcal{T}$ into the state space $\mathcal{S}$, whose inverse map is the restriction to $\mathcal{S}_1$ of the map $\rho \mapsto T_\rho$ that associates with each state ρ the corresponding correlation matrix.

Which condition ensures that the two pure states $P_1 = \rho_{0,R_1}$ and $P_2 = \rho_{\mathbf{0},R_2}$ of mds type are orthogonal to each other?

Lemma 4.9. *The pure states $P_1 = P_{0,R_1}$ and $P_2 = P_{0,R_2}$ are orthogonal iff $R_1 R_2^* = F$ where F is a flip, that is, a rotation by π.*

Proof: Clearly P_1 and P_2 are orthogonal iff trace$(P_1 P_2) = 0$. (Indeed let χ_1 and χ_2 be unit vectors in the ranges of P_1 and P_2 respectively. Then trace $(P_1 P_2) = |\langle \chi_1, \chi_2 \rangle|^2$). Now by (4.4), trace$(P_1 P_2) = \frac{1}{4}(1 + \text{trace}(R_1 R_2^*))$. Thus P_1 and P_2 are orthogonal iff trace$(F) = 1 + 2\cos\varphi = -1$, where $F = R_1 R_2^*$ and φ is the angle of rotation of F. Hence $\varphi = \pi$. □

Lemma 4.10. *For $k = 0, 1, 2, 3$, define*

$$P_k = P_{0,F_k}$$

where the F_ks are the elements of the four-group $\mathcal{V}$ defined in the paragraph preceding Proposition 3.3. Then (P_0, P_1, P_2, P_3) is a complete orthogonal set of pure states.

Proof: For the proof observe that

$$\frac{1}{4}\sum_{k=1}^{3} P_k = \rho\left(\mathbf{0}, \mathbf{0}, -\frac{1}{4}\left(I + \sum_{k=1}^{3} F_k\right)\right) = \rho(\mathbf{0}, \mathbf{0}, 0) = \frac{1}{4}(\mathbf{1} \otimes \mathbf{1}) \qquad \square$$

Using the formulas

$$(\sigma_k \otimes \sigma_k)\phi_0 = -\phi_0, \quad k = 1, 2, 3 \tag{4.15}$$

and

$$(\sigma_k \otimes \sigma_k)\phi_j = (-1)^{\delta_{jk}}\phi_j, \quad j, k = 1, 2, 3 \tag{4.16}$$

it is easily verified that the P_ks are the projections corresponding the one-dimensional subspaces generated by the members of the *Bell basis* $(\phi_0, \phi_1, \phi_2, \phi_1)$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ defined by Eq. (2.8), that is, for $k = 0, 1, 2, 3$, $P_k = |\phi_k\rangle\langle\phi_k|$. Accordingly we shall call (P_0, P_1, P_2, P_3) the *Bell set*. (Traditionally P_0 is called the *singlet state*, whereas P_1, P_2, P_3 are called *triplet states*). A *general Bell set* will be for us any set (Q_0, Q_1, Q_2, Q_3) such that for $k = 0, 1, 2, 3$

$$Q_k = (u_1 \otimes u_2) P_k \big(u_1^* \otimes u_2^*\big) = P_{0, R(u_1) F_k R(u_2)^*} \tag{4.17}$$

If $h(\gamma, \mathbf{r}, \mathbf{s}, T)$ is an hermitian operator with canonical form $h(\gamma, \mathbf{r}', \mathbf{s}', \varepsilon D)$ we can compute its lowest eigenvalue λ_1 using the following expression

$$\begin{aligned} \lambda_1 &= \inf_{\|\mathbf{v}\| \leq 1, R \in SO(3)} \operatorname{trace}(h(\gamma, \mathbf{r}', \mathbf{s}', \varepsilon D) P_{\mathbf{v}, R^*}) \\ &= \frac{1}{4} \inf_{\|\mathbf{v}\| \leq 1, R \in SO(3)} \big((\gamma - \mathbf{v} \cdot (R\mathbf{s}' - \mathbf{r}') \\ &\quad - \varepsilon \operatorname{trace}\big(RD\big(\sqrt{1 - \|\mathbf{v}\|^2}(I - E_{\mathbf{v}}) + E_{\mathbf{v}}\big)\big)\big) \end{aligned}$$

The operator is positive semidefinite iff $\lambda_1 \geq 0$. This leads to the following criterion for a given hermitian operator $\rho(\mathbf{r}, \mathbf{s}, T)$ of trace 1 to be a state

Theorem 4.11. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a hermitian operator of trace 1 and let $\rho(\mathbf{r}', \mathbf{s}', \varepsilon D)$ be one of its canonical forms. Then a necessary and sufficient condition for ρ to be a state is that*

$$\sup_{\|\mathbf{v}\| \leq 1, R \in SO(3)} \big(\mathbf{v} \cdot \big(R\mathbf{s}' - \mathbf{r}' + \varepsilon \operatorname{trace}\big(RD\big(\sqrt{1 - \|\mathbf{v}\|^2}(I - E_{\mathbf{v}}) + E_{\mathbf{v}}\big)\big)\big) \leq 1$$

5. SEPARABLE STATES

In this section we deal with the set $\mathcal{S}_0$ of all separable states. The following lemma shows that the set $\mathcal{S}_0$ possesses a symmetry property beyond the general symmetry properties exhibited by $\mathcal{S}_\xi$ for general ξ (which are described in Part (2) of Theorem 4.6):

Lemma 5.1. *If $\rho(\mathbf{r}, \mathbf{s}, T) \in \mathcal{S}_0$ then $\rho(\mathbf{r}, -\mathbf{s}, -T) \in \mathcal{S}_0$.*

Proof: Suppose $\rho(\mathbf{r}, \mathbf{s}, T) = \sum c_k(\rho(\mathbf{r}_k) \otimes \rho(\mathbf{s}_k))$, where the c_k are nonnegative numbers adding up to 1 and $\mathbf{r}_k$ and $\mathbf{s}_k$ are unit vectors. Then $\mathbf{r} = \sum c_k \mathbf{r}_k$, $\mathbf{s} = \sum c_k \mathbf{s}_k$ and $T = \sum c_k |\mathbf{r}_k >< \mathbf{s}_k|$. Therefore

$$\rho(\mathbf{r}, -\mathbf{s}, -T) = \sum c_k(\rho(\mathbf{r}_k) \otimes \rho(-\mathbf{s}_k)) \in \mathcal{S}_0 \quad \square$$

The following theorem, part of whose proof we moved to Appendix B, shows that this symmetry property characterizes the set of all separable states.

Theorem 5.2. *Suppose $\rho(\mathbf{r}, \mathbf{s}, T)$ is a state. Then these are equivalent:*

(1) $\rho(\mathbf{r}, \mathbf{s}, T)$ is separable.
(2) $\rho(\mathbf{r}, -\mathbf{s}, -T)$ is a state.
(3) $\rho(-\mathbf{r}, \mathbf{s}, -T)$ is a state.

Proof: (1) $\Rightarrow$ (2) by Lemma 5.1
(2) $\Leftrightarrow$ (3) by Corollary 4.4
(3) $\Rightarrow$ (1) by Corollary B.5 □

Corollary 5.3. *Suppose $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a state and either $\rho(\mathbf{r}, -\mathbf{s}, -T) \sim \rho$ or $\rho(-\mathbf{r}, \mathbf{s}, -T) \sim \rho$; then ρ is separable.*

Corollary 5.4. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a state with det $T = 0$ and suppose that there is a canonical form $\rho(\mathbf{r}', \mathbf{s}', D)$ of ρ such that either $r'_3 = 0$ or $s'_3 = 0$. Then ρ is separable.*

Proof: Since det $T = 0$ $\rho(F_3\mathbf{r}', \mathbf{s}', -D)$ and $\rho(\mathbf{r}', F_3\mathbf{s}', -D)$ are other canonical forms of $\rho(\mathbf{r}, \mathbf{s}, T)$ (cf. Proposition 3.2). If $r'_3 = 0$ then $F_3\mathbf{r}' = -\mathbf{r}'$ and therefore $\rho(-\mathbf{r}', \mathbf{s}', -D)$ is a canonical form of ρ. Now $\rho(-\mathbf{r}', \mathbf{s}', -D)$ is manifestly a canonical form of $\rho(-\mathbf{r}, \mathbf{s}, -T)$ and therefore $\rho(-\mathbf{r}, \mathbf{s}, -T) \sim \rho$. Similarly if $s'_3 = 0$ then $\rho(\mathbf{r}, -\mathbf{s}, -T) \sim \rho$. The conclusion now follows from the previous Corollary. □

Corollary 5.5. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a state and assume that rank $T \leq 1$. Then ρ is separable.*

Proof: In this case the invariance group G' of $D = \text{diag}(\mu_1, 0, 0)$ contains the subgroup $SO_1(2)$ of all rotations about the first coordinate axis. Thus if $\rho(\mathbf{r}', \mathbf{s}', D)$ is any canonical form of $\rho(\mathbf{r}, \mathbf{s}, T)$ then so is $\rho(R\mathbf{r}', \mathbf{s}', D)$ for any $R \in SO_1(2)$. By a judicious choice of R we can achieve $(R\mathbf{r}')_3 = 0$. □

Theorem 5.2 suggests that we introduce another linear involution $h \mapsto \hat{h}$ into the set $\mathcal{H}_4$, whereby $\hat{h} = (\gamma, \mathbf{r}, -\mathbf{s}, -T)$ if $h = (\gamma, \mathbf{r}, \mathbf{s}, T)$. This involution is again self-adjoint relative to the inner product defined on $\mathcal{H}_4$:

$$\langle \hat{h}, h' \rangle = \langle h, \hat{h}' \rangle, \quad h, h' \in \mathcal{H}_4 \tag{5.1}$$

a result that implies, together with the self-duality of cone $\mathcal{H}_4^+$, that also the cone$\widehat{\mathcal{H}_4^+} = \{h \in \mathcal{H}_4 | \hat{h} \in \mathcal{H}_4^+\}$ is self-dual. Moreover we have

$$h + \hat{h} = h(\gamma, \mathbf{r}) \otimes \mathbf{1} \tag{5.2}$$

Let $\mathcal{K}$ be the (closed) convex cone generated by the set $\mathcal{S}_0$ of all separable states: $\mathcal{K} = \bigcup_{\gamma \geq 0} \gamma \mathcal{S}_0$ and let $\widetilde{\mathcal{K}}$ be its dual cone

$$\widetilde{\mathcal{K}} = \{h \in \mathcal{H}_4 \mid \forall \rho \in \mathcal{S}_0 \colon \langle h, \rho \rangle \geq 0\}$$

By Theorem B.3 (of Appendix B) we have

$$\widetilde{\mathcal{K}} = \mathcal{H}_4^+ + \widehat{\mathcal{H}_4^+} \tag{5.3}$$

Definition 5.6. An hermitian operator h of the form $h = k + \hat{k}'$ with $k, k' \in \mathcal{H}_4^+$ is called a *Bell observable*.

Now the bipolar theorem (cf. Hilgert *et al.* (1989), Proposition I.14) immediately gives

Theorem 5.7. *An hermitian operator ρ of trace* 1 *is a separable state iff $\langle h, \rho \rangle \geq 0$ for every Bell observable. A state ρ is separable iff the expectation value of every Bell observable in the state ρ is nonnegative.*

If ρ is a state then by definition $\hat{\rho}$ is a Bell observable. The eigenvalues of $\hat{\rho}$ are the possible outcomes that a measurement of the observable can yield. By Theorem 5.2, ρ is *separable* iff $\hat{\rho}$ is positive semidefinite. Let $\rho_1 = (\text{trace}\pi_1)^{-1}\pi_1$ be the normalized eigenprojection of $\hat{\rho}$ belonging to the lowest eigenvalue $\hat{\lambda}_1$. Then the expectation value of the Bell observable $\hat{\rho}_1$ in the state ρ is given by $\langle \hat{\rho}_1, \rho \rangle = \langle \rho_1, \hat{\rho} \rangle = \hat{\lambda}_1$. If ρ is nonseparable then $\hat{\lambda}_1 < 0$ and therefore ρ_1 is nonseparable (since $\hat{\rho}_1$ is not positive semidefinite or since the expectation value of the Bell observable $\hat{\rho}$ in the state ρ_1 is negative). Thus we have proved

Corollary 5.8. *Let ρ be a state. Then ρ is nonseparable iff the lowest eigenvalue $\hat{\lambda}_1$ of the Bell observable $\hat{\rho}$ is strictly negative. Let ρ_1 be the normalized eigenprojection of $\hat{\rho}$ belonging to the lowest eigenvalue $\hat{\lambda}_1$. Then $\hat{\lambda}_1$ is the expectation value of the Bell observable $\hat{\rho}_1$ in the state ρ, and if ρ is nonseparable then so is ρ_1.*

Example. Suppose $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ is an mds state. Then it follows from Eq. (5.2) that $\rho + \hat{\rho} = \frac{1}{2}(\mathbf{1} \otimes \mathbf{1})$ and therefore

$$\hat{\rho}\rho = \frac{1}{2}\rho - \rho^2$$

If ρ is also *pure* and therefore is of the form $\rho = \rho(\mathbf{0}, \mathbf{0}, -R) = P_{0,R}$ then

$$\hat{\rho}\rho = -\frac{1}{2}\rho$$

Since $\hat{\rho}$, being equivalent to $\rho(\mathbf{0}, \mathbf{0}, I)$, has the spectrum

$$\text{sp}(\hat{\rho}) = \left\{-\frac{1}{2}, \frac{1}{2}\right\}$$

with $-\frac{1}{2}$ being a *simple* eigenvalue, we conclude that $\rho_1 = \rho$ and $\hat{\lambda}_1 = -\frac{1}{2}$.

6. THE MDS-STATES

In this section we turn our attention to hermitian operators of the form $\rho(\mathbf{0}, \mathbf{0}, T)$ whose canonical form is $\rho(\mathbf{0}, \mathbf{0}, \varepsilon D)$. Thus in case $\det T > 0(\det T < 0)$ the canonical form is uniquely given by $\rho(\mathbf{0}, \mathbf{0}, D)(\rho(\mathbf{0}, \mathbf{0}, -D))$. In the case where $\det T = 0$ there are two canonical forms $\rho(\mathbf{0}, \mathbf{0}, \pm D)$. The spectrum of $\rho(\mathbf{0}, \mathbf{0}, T)$ coincides with the spectrum of its canonical form $\rho(\mathbf{0}, \mathbf{0}, \varepsilon D)$, which in turn can easily be determined since the Bell basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$ consists of eigenvectors for $\rho(\mathbf{0}, \mathbf{0}, \varepsilon D)$. The corresponding eigenvalues are affine functions of the singular values μ_1, μ_2, and μ_3 of T.

More precisely, using Formulas (4.15) and (4.16) we easily verify the following theorem:

Theorem 6.1. *For $k = 0, 1, 2, 3$ we have*

$$\rho(\mathbf{0}, \mathbf{0}, \varepsilon D)\phi_k = w_k(\varepsilon)\phi_k$$

where

$$w_0(\varepsilon) = \frac{1}{4}(1 - \varepsilon(\mu_1 + \mu_2 + \mu_3))$$

$$w_1(\varepsilon) = \frac{1}{4}(1 + \varepsilon(-\mu_1 + \mu_2 + \mu_3))$$

$$w_2(\varepsilon) = \frac{1}{4}(1 + \varepsilon(\mu_1 - \mu_2 + \mu_3))$$

$$w_3(\varepsilon) = \frac{1}{4}(1 + \varepsilon(\mu_1 + \mu_2 - \mu_3))$$

Let $(u_1, u_2) \in U_1 \times U_1$ be such that

$$\rho(\mathbf{0}, \mathbf{0}, T) = (u_1 \otimes u_2)(\rho(\mathbf{0}, \mathbf{0}, \varepsilon D)\big(u_1^* \otimes u_2^*\big) \tag{6.1}$$

Then the vectors defined by

$$\psi_k = (u_1 \otimes u_2)\phi_k, \quad k = 0, 1, 2, 3 \tag{6.2}$$

constitute an *eigenbasis* of $\rho(\mathbf{0}, \mathbf{0}, T)$, that is, an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$ that consists of eigenvectors of $\rho(\mathbf{0}, \mathbf{0}, T)$, whereby $w_k(\varepsilon)$ is the eigenvalue that belongs to the eigenvector ψ_k. Thus the spectral resolution of $\rho(\mathbf{0}, \mathbf{0}, T)$ takes the form

$$\rho(\mathbf{0}, \mathbf{0}, T) = \sum_{k=0}^{3} w_k(\varepsilon) Q_k \tag{6.3}$$

where the Q_ks as defined by Eq. (4.17) are the projections corresponding to the one-dimensional subspaces generated by the ψ_ks.

Theorem 6.2. *Let $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ be an mds operator. Then these are equivalent:*

(1) *ρ is a state*
(2) $\mu_1 + \mu_2 + \varepsilon\mu_3 \leq 1$
(3) $\rho \in \mathcal{S}_1$

Proof: (1)⇔(2). ρ is a state iff the lowest eigenvalue is nonnegative. The lowest eigenvalue is given by $w_0(1)$ if $\varepsilon = 1$ and $w_3(-1)$ if $\varepsilon = -1$. The two conditions can be summarized by Condition (2) of the theorem.

(2)⇒(3). According to Eqs. (6.3) and the particular form of the Q_ks as given by Eq. (4.17) we have

$$\rho = \sum_{k=0}^{3} w_k(\varepsilon) Q_k = \sum_{k=0}^{3} w_k(\varepsilon) P_{\mathbf{0}, R(u_1)F_k R(u_2)^*} \tag{6.4}$$

Since the $w_k(\varepsilon)$s add up to 1 and if (2) is satisfied are nonnegative the above formula makes it evident that ρ belongs to $\mathcal{S}_1$.

(3)⇒(1) obvious □

Remarks.

(1) Note that since $T_\rho = T_{\rho^{mds}}$ (cf. Remark 4.8) every correlation matrix is derived from an mds state. Thus Eq. (6.4) implies that every correlation matrix can be represented as a weighted mean of *four* improper orthogonal matrices, thereby strengthening Proposition 4.7.
(2) Observe that we can use Condition (2) of the theorem to give a new proof of Proposition 3.6 (which asserts that the correlation values of a state belong to the interval [0, 1]).
(3) We can extract from the theorem the following interesting mathematical result:

Corollary 6.3. *Let T be a real 3×3 matrix and let $\mu_1 \geq \mu_2 \geq \mu_3$ be its singular values in descending order and let $\varepsilon = \operatorname{sign}(\det T)$. Then T belongs to the convex hull of $SO(3)$ iff $\mu_1 + \mu_2 - \varepsilon\mu_3 \leq 1$.*

Proof: If $T \in \operatorname{conv}(SO(3))$ then by Proposition 4.7 $-T$ is a correlation matrix, and therefore $\rho(\mathbf{0}, \mathbf{0}, -T)$ is a state (cf. Remark 4.8), which by the theorem implies $\mu_1 + \mu_2 - \varepsilon\mu_3 \leq 1$. Conversely, if $\mu_1 + \mu_2 - \varepsilon\mu_3 \leq 1$ holds then by the theorem $\rho(\mathbf{0}, \mathbf{0}, -T)$ is a state and therefore by Proposition 4.7 $T \in \operatorname{conv}(SO(3))$. □

The following Corollary sharpens Proposition 3.5:

Corollary 6.4. *If $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a state then $\mathbf{r}, \mathbf{s} \in B^3$ and*

$$T \in \operatorname{conv}(-SO(3))$$

Our next step is to single out those mds states that are also separable, that is, we want to characterize the set $\mathcal{S}_0 \cap \mathcal{S}_1$. An extreme point of $\mathcal{S}_0$ is a pure state of the product form:

$$P = \rho(\mathbf{r}) \otimes \rho(\mathbf{s}) = \rho(\mathbf{r}, \mathbf{s}, |\mathbf{r}\rangle\langle\mathbf{s}|), \quad \|\mathbf{r}\| = \|\mathbf{s}\| = 1$$

Taking the mds component of such a state

$$\rho_{\mathbf{r},\mathbf{s}} := (\rho(\mathbf{r}) \otimes \rho(\mathbf{s}))^{mds} = \rho(\mathbf{0}, \mathbf{0}, |\mathbf{r}\rangle\langle\mathbf{s}|)$$

we obtain a state (of rank 2) that belongs to $\mathcal{S}_1 \cap \mathcal{S}_0$. Let $\mathcal{E}$ denote the set of all these states.

$$\mathcal{E} = \{\rho_{\mathbf{r},\mathbf{s}} \mid \mathbf{r}, \mathbf{s} \in S^2\}$$

Then $\mathcal{E}$ constitutes an orbit under the group $U_1 \times U_1$ and we can state the following proposition:

Proposition 6.5. $\mathcal{S}_0 \cap \mathcal{S}_1 = \operatorname{conv}(\mathcal{E})$ and $\mathcal{E}$ is the set of extreme points of $\mathcal{S}_0 \cap \mathcal{S}_1$.

Proof: Clearly $\mathcal{S}_0 \cap \mathcal{S}_1 \supset \operatorname{conv}(\mathcal{E})$. To prove the opposite inclusion let $\rho \in \mathcal{S}_0 \cap \mathcal{S}_1$. Since $\rho \in \mathcal{S}_0$

$$\rho = \sum_{k=1}^{n} c_k(\rho(\mathbf{r}_k) \otimes \rho(\mathbf{s}_k))$$

where the c_ks are nonnegative numbers adding up to 1 and n is a positive integer not larger than 16 (Caratheodory's Theorem; cf. Bronsted (1982), Corollary 2.4). Now since $\rho \in \mathcal{S}_1$, taking the mds component (cf. Definition 4.3) on both sides leaves the left hand side of the equation unaffected:

$$\rho = \sum_{k=1}^{n} c_k(\rho(\mathbf{r}_k) \otimes \rho(\mathbf{s}_k))^{mds} = \sum_{k=1}^{n} c_k \rho_{\mathbf{r}_k,\mathbf{s}_k}$$

showing that $\rho \in \operatorname{conv}(\mathcal{E})$. That the set of extreme points of $\mathcal{S}_0 \cap \mathcal{S}_1$ coincides with $\mathcal{E}$ now is a consequence of Theorem A.3. □

Theorem 6.6. *Let $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ be a state. Then these are equivalent:*

(1) *ρ is separable*

(2) *$\rho(\mathbf{0}, \mathbf{0}, -T)$ is a state*

(3) trace$(D) = \mu_1 + \mu_2 + \mu_3 \leq 1$
(4) sp$(\rho(\mathbf{0}, \mathbf{0}, T)) \subset [0, \frac{1}{2}]$

Proof: (1)⇒(2) By Lemma 5.1

(2)⇒(3) Since $\rho(\mathbf{0}, \mathbf{0}, \pm T)$ are states it follows from Theorem 5.2 that $\mu_1 + \mu_2 + \mu_3 \leq 1$.

(3)⇒(1) Define $\mu_0 = 1 - \mu_1 - \mu_2 - \mu_3$. Then

$$D = \frac{\mu_0}{2}(-E_1) + \left(\frac{\mu_0}{2} + \mu_1\right)E_1 + \mu_2 E_2 + \mu_3 E_3 \tag{6.5}$$

where for $i = 1, 2, 3$, E_j denotes the projection onto the jth coordinate axis.

Since the operators $\rho(\mathbf{0}, \mathbf{0}, \pm E_j)$ belong to $\mathcal{E}$, it follows from (6.5) that $\rho(\mathbf{0}, \mathbf{0}, \varepsilon D) \in \text{conv}\mathcal{E} = \mathcal{S}_0 \cap \mathcal{S}_1$. Hence by the invariance of $\mathcal{S}_0 \cap \mathcal{S}_1$ under $U_1 \times U_1$, we also have $\rho = \rho(\mathbf{0}, \mathbf{0}, T) \in \mathcal{S}_0 \cap \mathcal{S}_1$.

(3)⇔(4) In case $\varepsilon = 1$ Condition (2) implies $w_0(1) \geq 0$ and $w_3(1) \leq \frac{1}{2}(1 - \mu_1)$. Therefore in this case sp$(\rho(\mathbf{0}, \mathbf{0}, T)) \subset [w_0(1), w_3(1)] \subset [0, \frac{1}{2}]$. In case $\varepsilon = -1$ Condition (2) implies $w_3(-1) \geq \frac{1}{2}\mu_1$ and $w_0(-1) \leq \frac{1}{2}$. Hence in this case sp$(\rho(\mathbf{0}, \mathbf{0}, T)) \subset [w_3(-1), w_0(-1)] \subset [0, \frac{1}{2}]$. Conversely, assume that sp$(\rho(\mathbf{0}, \mathbf{0}, T)) \subset [0, \frac{1}{2}]$. Then Condition (2) is implied in case of $\varepsilon = 1$ by $w_0(1) \geq 0$ and in case $\varepsilon = -1$ by $w_0(-1) \leq \frac{1}{2}$. □

Corollary 6.7. *Suppose* $\det T \geq 0$. *Then if* $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ *is a state then* ρ *is separable.*

Proof: If $\det T \geq 0$ then ε can be chosen to be $+1$ and therefore the eigenvalues of $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$ are $w_j(1),\ j = 0, 1, 2, 3$. Thus if ρ is a state then

$$w_0(1) = \frac{1}{4}(1 - \mu_1 - \mu_2 - \mu_3) \geq 0,$$

a condition which by Theorem 6.6, Part (3), is equivalent to ρ being separable.

□

7. WHEN IS A GENERIC OPERATOR $\rho(\mathbf{r}, \mathbf{s}, T)$ A (SEPARABLE) STATE?

In this section we shall deal with the matrices of a 2-qubit operator $h = h(\gamma, \mathbf{r}, \mathbf{s}, T)$ relative to two distinguished bases: the Bell basis (2.8) $(\phi_0, \phi_1, \phi_2, \phi_3)$ and an eigenbasis (6.2) $(\psi_0, \psi_1, \psi_2, \psi_3)$ of the mds component $h^{mds} = h(\gamma, \mathbf{0}, \mathbf{0}, T)$ of h. To analyze the structure of the matrix $[h]_\phi$ of the operator h relative to the Bell basis, it is useful to write h in the form

$$h = h(\gamma, \mathbf{0}, \mathbf{0}, T) + \Delta(\mathbf{r}, \mathbf{s})$$

where $\Delta(\mathbf{r}, \mathbf{s}) = \frac{1}{4}(\mathbf{r} \cdot \sigma \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{s} \cdot \sigma)$. A straightforward computation shows that the matrices relative to the Bell basis (2.8) of the operators $\sigma_j \otimes \mathbf{1},\ j = 1, 2, 3$ and the operators $\mathbf{1} \otimes \sigma_k,\ k = 1, 2, 3$ respectively have the form

$$[\sigma_j \otimes \mathbf{1}]_\phi = iA_j \quad \text{and} \quad [\mathbf{1} \otimes \sigma_k]_\phi = iB_k$$

where i denotes the imaginary unit and A_j and B_k are *real* 4×4 matrices with $[A_j, B_k] = 0$ for $j, k = 1, 2, 3$. It follows that

$$[h]_\phi = [h(\gamma, \mathbf{0}, \mathbf{0}, T)]_\phi + [\Delta(\mathbf{r}, \mathbf{s})]_\phi = X + iY$$

where

$$X = [h(\gamma, \mathbf{0}, \mathbf{0}, T)]_\phi = \frac{1}{4}\left(\mathbf{1} \otimes \mathbf{1} - \sum_{j,k=1}^{3} t_{jk} A_j B_k\right)$$

and

$$Y = \frac{1}{i}[\Delta(\mathbf{r}, \mathbf{s})]_\phi = \left(\sum_{j=1}^{3} r_j A_j + s_j B_j\right)$$

are *real* 4×4 matrices. Thus we can state

Theorem 7.1. *The time reversal of observables and states of a pair of qubits is represented by the complex conjugation of the corresponding matrix relative to the Bell basis. More precisely let $h = h(\gamma, \mathbf{r}, \mathbf{s}, T)$ is an observable (state) of the qubit system. Then if $[h]_\phi$ denotes its matrix relative to the Bell basis, we have*

$$[h^\#]_\phi = \overline{[h]_\phi}$$

and therefore

$$[h^{mds}]_\phi = Re[h]_\phi.$$

Proof: Taking the matrix relative to the Bell basis in the equation

$$h^\# = h(\gamma, 0, 0, T) + \Delta(-\mathbf{r}, -\mathbf{s})$$

yields

$$[h^\#]_\phi = [h(\gamma, \mathbf{0}, \mathbf{0}, T)]_\phi + [\Delta(-\mathbf{r}, -\mathbf{s})]_\phi = X - iY = \overline{[h]_\phi} \quad \square$$

Corollary 7.2. *The matrix $[h]_\phi$ of an hermitian operator h relative to the Bell basis has* real *entries iff h is an mds operator (cf. Definition 4.3).*

A one-particle hermitian operator $\rho = \rho(\mathbf{r})$ of trace 1 is a state iff $\det \rho \geq 0$. In the case of a pair of qubits we are interested in finding analogous criteria that help us to decide if a given hermitian operator $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ of trace 1 is a (separable) state. For this purpose we are interested in the matrices of ρ (and $\hat{\rho}$) relative to an eigenbasis $(\psi_0, \psi_1, \psi_2, \psi_3)$ of ρ^{mds}. Let $\rho' = \rho(\mathbf{r}', \mathbf{s}', \varepsilon D)$ and $\hat{\rho}' = \rho(\mathbf{r}', -\mathbf{s}', -\varepsilon D)$ be the canonical forms of ρ and $\hat{\rho}$ respectively. Using Eq. (6.1) we find

$$[\rho]_\psi = [\rho']_\phi = \begin{bmatrix} w_0(\varepsilon) & -ia_1 & -ia_2 & -ia_3 \\ ia_1 & w_1(\varepsilon) & -ib_3 & ib_2 \\ ia_2 & ib_3 & w_2(\varepsilon) & -ib_1 \\ ia_3 & -ib_2 & ib_1 & w_3(\varepsilon) \end{bmatrix} \tag{7.1}$$

and

$$[\hat{\rho}]_\psi = [\hat{\rho}']_\phi = \begin{bmatrix} w_0(-\varepsilon) & -ib_1 & -ib_2 & ib_3 \\ ib_1 & w_1(-\varepsilon) & -ia_3 & ia_2 \\ ib_2 & ia_3 & w_2(-\varepsilon) & -ia_1 \\ ib_3 & -ia_2 & ia_1 & w_3(-\varepsilon) \end{bmatrix} \tag{7.2}$$

where $a_k = \frac{1}{4}(\mathrm{r}'_k - \mathrm{s}'_k)$ and $b_k = \frac{1}{4}(\mathrm{r}'_k + \mathrm{s}'_k)$, $k = 0, 1, 2, 3$. ρ is a state if the principal sub-determinants of the matrix (7.1) are nonnegative. If in addition the principal sub-determinants of the matrix (7.2) are nonnegative the state is separable.

Theorem 7.3. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be an hermitian operator of trace* 1. *Let $\rho(\mathbf{r}', \mathbf{s}', \varepsilon D)$ be a canonical form and let $\mathbf{a} = \frac{1}{4}(\mathbf{r}' - \mathbf{s}')$ and $\mathbf{b} = \frac{1}{4}(\mathbf{r}' + \mathbf{s}')$. Then ρ is a state iff $\mu_1 + \mu_2 + \varepsilon\mu_3 \leq 1$ and*

$$\begin{aligned} w_0(\varepsilon)w_1(\varepsilon)w_2(\varepsilon)w_3(\varepsilon) + (\mathbf{a}\cdot\mathbf{b})^2 \geq{} & w_2(\varepsilon)w_3(\varepsilon)a_1^2 + w_1(\varepsilon)w_3(\varepsilon)a_2^2 \\ & + w_1(\varepsilon)w_2(\varepsilon)a_3^2 + w_0(\varepsilon)w_1(\varepsilon)b_1^2 \\ & + w_0(\varepsilon)w_2(\varepsilon)b_2^2 + w_0(\varepsilon)w_3(\varepsilon)b_3^2 \end{aligned} \tag{7.3}$$

$$w_0(\varepsilon)w_1(\varepsilon)w_2(\varepsilon) \geq w_0(\varepsilon)b_3^2 + w_1(\varepsilon)a_2^2 + w_2(\varepsilon)a_1^2 \tag{7.4}$$

$$w_0(\varepsilon)w_1(\varepsilon)w_3(\varepsilon) \geq w_0(\varepsilon)b_2^2 + w_1(\varepsilon)a_3^2 + w_3(\varepsilon)a_1^2 \tag{7.5}$$

$$w_0(\varepsilon)w_2(\varepsilon)w_3(\varepsilon) \geq w_0(\varepsilon)b_1^2 + w_2(\varepsilon)a_3^2 + w_3(\varepsilon)a_2^2 \tag{7.6}$$

$$w_1(\varepsilon)w_2(\varepsilon)w_3(\varepsilon) \geq w_1(\varepsilon)b_1^2 + w_2(\varepsilon)b_2^2 + w_3(\varepsilon)b_3^2 \tag{7.7}$$

$$w_1(\varepsilon)w_2(\varepsilon) \geq b_3^2 \qquad w_1(\varepsilon)w_3(\varepsilon) \geq b_2^2 \qquad w_2(\varepsilon)w_3(\varepsilon) \geq b_1^2 \tag{7.8}$$

$$w_0(\varepsilon)w_k(\varepsilon) \geq a_k^2 \quad k = 1, 2, 3. \tag{7.9}$$

ρ is a separable state iff $\mu_1 + \mu_2 + \mu_3 \leq 1$ and in addition to the inequalities (7.3)–(7.9) the same inequalities are satisfied in which ε is replaced by $-\varepsilon$ and the vectors **a** *and* **b** *are interchanged.*

Remarks

(1) Note that the conditions of Theorem 7.2 are invariant with respect to the substitutions $(\mathbf{a}, \mathbf{b}) \to (\pm\mathbf{a}, \pm\mathbf{b})$. This observation can be used to give another proof of the fact that the state space $\mathcal{S}$ is invariant under the involutions $\rho \mapsto \rho^{\#}$ and $\rho \mapsto \rho^{(p)}$ (cf. Corollary 4.4). (Indeed, $[\rho^{\#}]_{\psi}$ is obtained from $[\rho]_{\psi}$ by the substitution $(\mathbf{a}, \mathbf{b}) \to (-\mathbf{a}, -\mathbf{b})$. Moreover since $\rho(\mathbf{s}', \mathbf{r}', \varepsilon D)$ is a canonical form of $\rho^{(p)}$, it is possible to represent $\rho^{(p)}$ by a matrix that is obtained from $[\rho]_{\psi}$ by the substitution $(\mathbf{a}, \mathbf{b}) \to (-\mathbf{a}, \mathbf{b})$).

A similar argument based on Theorem 7.2 can be used to give a second proof of the fact that the space $\mathcal{S}_0$ of all separable states is invariant under the two involutions $\rho \mapsto \rho^{\#}$ and $\rho \mapsto \rho^{(p)}$ (cf. Theorem 4.6).

(2) Note that the term $(\mathbf{a} \cdot \mathbf{b})^2$ in (7.3) vanishes precisely if $\|\mathbf{r}\| = \|\mathbf{s}\|$ in $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$. Indeed, $\|\mathbf{r}\| = \|\mathbf{s}\|$ is equivalent to $\|\mathbf{r}'\| = \|\mathbf{s}'\|$, which in turn is equivalent to $(\mathbf{a} \cdot \mathbf{b}) = 0$.

As a special case let us consider the case where ρ is *p symmetric*, that is, such that $\rho^{(p)} = \rho$. Then ρ has the form $\rho = \rho(\mathbf{r}, \mathbf{r}, T)$, where T is a symmetric matrix. It is useful to distinguish the cases where T is negative (semi-)definite, indefinite, and positive (semi-)definite. Let us consider the indefinite case where the eigenvalues of T are given by $-\mu_1$, μ_2, and $-\mu_3$. (In the case of a symmetric matrix the eigenvalues agree up to a sign with the singular values). Then there exists a rotation matrix R such that

$$RTR^* = \mathrm{diag}(-\mu_1, \mu_2 - \mu_3)$$

Putting $\mathbf{r}' = R\mathbf{r}$ we see that a canonical form of ρ is given by

$$\rho' = \rho(\mathbf{r}', F_2\mathbf{r}', D)$$

Therefore $\mathbf{a} = (r_1'/2, 0, r_3'/2)$ and $\mathbf{b} = (0, r_2'/2, 0)$. For ρ to be a state it is necessary that $w_0(1) \geq 0$. For simplicity let us further assume that $w_0(1) > 0$, which is equivalent to $\mu_1 + \mu_2 + \mu_3 < 1$.

It follows that under this additional assumption the operator ρ is a state iff the inequality

$$4w_0(1)w_1(1)w_3(1) \geq \left(w_3(1)r_1'^2 + w_0(1)r_2'^2 + w_1(1)r_3'^2\right) \tag{7.10}$$

holds, since under the given hypothesis inequality (7.10) (which is an instant of (7.5)) implies all inequalities (7.4)–(7.9). The state ρ is separable iff, in addition, the inequality

$$4w_0w_1w_2w_3 \geq \left(w_0w_1r_1'^2 + w_1w_3r_2'^2 + w_0w_3r_3'^2\right)$$

with $w_k = w_k(-1),\ k = 0, 1, 2, 3$ is satisfied. All other cases are treated similarly.

We end this section by giving a necessary condition for the nonseparability of a state.

Theorem 7.4. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a state. Then $\mathbf{r} \in S^2$ or $\mathbf{s} \in S^2$ iff ρ is a product state $\rho = \rho(\mathbf{r}) \otimes \rho(\mathbf{s})$ with one factor being a (1-qubit) pure state. In particular if ρ is a nonseparable state then $\|\mathbf{r}\| < 1$ and $\|\mathbf{s}\| < 1$.*

Proof: If $\rho = \rho(\mathbf{r}) \otimes \rho(\mathbf{s})$ with one of the factors being a pure state then clearly $\mathbf{r} \in S^2$ or $\mathbf{s} \in S^2$. To see that also the converse holds we consider the spectral resolution of ρ

$$\rho = \sum_{j=1}^{4} w_j P_{\mathbf{s}_j, R_j} = \sum_{j=1}^{4} w_j \rho(\mathbf{r}_j, \mathbf{s}_j, T_j)$$

where for $j = 1, 2, 3, 4$, $\mathbf{r}_j = -R_j\mathbf{s}_j$ and

$$T_j = -R_j\left(\xi_j\left(I - E_{\mathbf{s}_j}\right) + E_{\mathbf{s}_j}\right)$$

and the w_js are nonnegative numbers adding up to 1. Let us consider the case where $\mathbf{r} = \sum_{j=1}^4 w_j\mathbf{r}_j \in S^2$. Then for $j = 1, 2, 3, 4$, $\mathbf{r}_j = \mathbf{r}$ and therefore $\mathbf{s}_j = -R_j^*\mathbf{r} \in S^2$, which implies that

$$T_j = -R_j|s_j\rangle\langle s_j| = |\mathbf{r}\rangle\langle \mathbf{s}_j|$$

Letting $\mathbf{s} = \sum_{j=1}^4 w_j\mathbf{s}_j$ we obtain that

$$\rho = \rho(\mathbf{r}, \mathbf{s}, |\mathbf{r}\rangle\langle \mathbf{s}|) = \rho(\mathbf{r}) \otimes \rho(\mathbf{s})$$

where $\rho(\mathbf{r})$ is a one-particle pure state. A similar argument can be applied if $\mathbf{s} \in S^2$. □

8. CONCURRENCE AS A MEASURE OF ENTANGLEMENT

In section 4 we introduced the concurrence

$$\xi = \sqrt{1 - \|\mathbf{s}\|^2}$$

as a measure of the entanglement of the two qubits in the pure state $P_{\mathbf{s},R}$. For a member of the Bell set $P_k = |\phi_k\rangle\langle\phi_k|$ we have $\xi(P_k) = 1$. The following theorem shows how to compute the concurrence of a pure state P from the components of a unit vector in the range of P with respect to the Bell basis (2.8).

Theorem 8.1. *Let $P = P_{\mathbf{s},R}$ be a pure state and let χ be a unit vector in the range of P (i.e., $P = |\chi\rangle\langle\chi|$). Let $\alpha_k = \langle\chi, \phi_k\rangle$, $k = 0, 1, 2, 3$ be the four components of χ with respect to the Bell basis (2.8). Then*

$$\xi(P) = \left|\sum_{k=0}^{3} \alpha_k^2\right|.$$

Proof: Probably the most elegant proof of this formula exploits the $U_1 \times U_1$ isometry φ between $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{M}_2$, whose existence we established in Proposition 2.1. Application of φ to the expression $\chi = \sum_{k=0}^{3} \alpha_k\phi_k$ yields, in view of Formula (2.9)

$$\varphi(\chi) = \frac{1}{\sqrt{2}}\left(\alpha_0\mathbf{1} - i\sum_{k=1}^{3}\alpha_k\sigma_k\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} \alpha_0 - i\alpha_3 & i\alpha_1 - \alpha_2 \\ i\alpha_1 + \alpha_2 & \alpha_0 + i\alpha_3 \end{bmatrix}$$

Taking the determinant leads to the formula

$$\left|\sum_{k=0}^{3}\alpha_k^2\right| = 2|\det\varphi(\chi)|$$

Now the determinant of $\varphi(\chi)$ is clearly a $U_1 \times U_1$ invariant. Indeed if $\chi' = (u_1 \otimes u_2)\chi$ for some $(u_1, u_2) \in U_1 \times U_1$ then

$$\det\varphi(\chi') = \det\varphi((u_1 \otimes u_2)\chi) = \det(u_1\varphi(\chi)u_2^*) = \det\varphi(\chi)$$

Next, observe that the unit vector

$$\chi' = \frac{1}{\sqrt{2}}\big((-\sqrt{1+\xi})\phi_0 + \big(i\sqrt{1-\xi}\big)\phi_1\big)$$

with $\xi = \xi(P) = \sqrt{1 - \|\mathbf{s}\|^2}$, belongs to the range of the canonical form (4.14) $P' = P_{\|\mathbf{s}\|\mathbf{e}_1,I}$ of P. Indeed we have

$$[|\chi'\rangle\langle\chi'|]_\phi = \frac{1}{2}\begin{bmatrix} (1+\xi) & i\|\mathbf{s}\| & 0 & 0 \\ -i\|\mathbf{s}\| & (1-\xi) & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \big[P_{\|\mathbf{s}\|\mathbf{e}_1,I}\big]_\phi$$

It follows that χ' must have the form $\chi' = (u_1 \otimes u_2)\chi$ for some $(u_1, u_2) \in U_1 \times U_1$. Finally

$$\left|\sum_{k=0}^{3} \alpha_k^2\right| = 2|\det \varphi(\chi)| = 2|\det \varphi(\chi')|$$

$$= \frac{1}{2}\left|\left(-\sqrt{1+\xi}\right)^2 + \left(i\sqrt{1-\xi}\right)^2\right| = \xi. \quad \square$$

Corollary 8.2. *A pure state $P = P_{\mathbf{s},R}$ is of mds type (belongs to $\mathcal{P}_1$) iff the range of P contains a unit vector χ all of whose four components relative to the Bell basis are real.*

Proof: First suppose that the range of P contains a unit vector χ whose four components $\alpha_k = \langle \chi, \phi_k \rangle$, $k = 0, 1, 2, 3$ are real. Then by the theorem $\xi(P) = \sum_{k=0}^{3} \alpha_k^2 = \sum_{k=0}^{3} |\alpha_k|^2 = 1$. Conversely suppose P is of mds type ($P \in \mathcal{P}_1$). Then by Corollary 7.2 $[P]_\phi$ is a real (symmetric) matrix. Since $[P]_\phi$ is also idempotent and of trace 1, it admits a normalized eigenvector $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^4$ (unique up to a sign) belonging to the eigenvalue 1. Then $\chi = \sum_{k=0}^{3} \alpha_k \phi_k$ has the desired property. $\square$

One of the problems that arises in this context is how to extend the concurrence from the set of all pure states to the set of all states. It seems to us that the lowest eigenvalue $\hat{\lambda}_1$ of $\hat{\rho}$ is a perfect candidate for such an extension.

Definition 8.3. Let ρ be an arbitrary state. By the *concurrence* of a state ρ we mean the number

$$\xi(\rho) = \max(0, -2\hat{\lambda}_1)$$

The following lemma shows that this definition is indeed an extension of the notion of concurrence for pure states.

Lemma 8.4. If $P = P_{\mathbf{s},R}$ *is a pure state then*

$$\hat{\lambda}_1 = -\frac{1}{2}\sqrt{1 - \|\mathbf{s}\|^2} = -\frac{1}{2}\xi(P)$$

Proof: A canonical form of $\hat{P}$ is given by

$$\hat{P}' = \rho\left(\|\mathbf{s}\|\mathbf{e}_1, -\|\mathbf{s}\|\mathbf{e}_1,\ \operatorname{diag}\left(1, \sqrt{1 - \|\mathbf{s}\|^2}, \sqrt{1 - \|\mathbf{s}\|^2}\right)\right)$$

Therefore the matrix of $\hat{P}$ relative to an eigenbasis of P^{mds} has the form

$$[\hat{P}]_{\psi} = [\hat{P}']_{\phi} = \frac{1}{2}\begin{bmatrix} -\sqrt{1-\|\mathbf{s}\|^2} & 0 & 0 & 0 \\ 0 & \sqrt{1-\|\mathbf{s}\|^2} & 0 & 0 \\ 0 & 0 & 1 & i\|\mathbf{s}\| \\ 0 & 0 & -i\|\mathbf{s}\| & 1 \end{bmatrix}$$

an equation which makes it evident that the smallest eigenvalue of $\hat{P}$ is given by $\hat{\lambda}_1 = -\frac{1}{2}\sqrt{1-\|\mathbf{s}\|^2}$. □

Example. What is the concurrence of a general mds state $\rho = \rho(\mathbf{0}, \mathbf{0}, T)$? Since if $\det T \geq 0$ $\rho(\mathbf{0}, \mathbf{0}, T)$ is separable by Corollary 6.7, the concurrence can only be different from 0 if $\det T < 0$, in which case the smallest eigenvalue of $\hat{\rho} = \rho(\mathbf{0}, \mathbf{0}, -T)$ is

$$\hat{\lambda}_1 = \frac{1}{4}(1 - \mu_1 - \mu_2 - \mu_3)$$

Thus the concurrence of the mds state ρ is given by

$$\xi(\rho) = \max\left(0, \frac{1}{2}(\mu_1 + \mu_2 + \mu_3 - 1)\right) \tag{8.1}$$

A special class of mds states are the *Werner states*. A hermitian operator $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is *invariant with respect to the group of rotations* iff it is of the form $\rho = \rho(\mathbf{0}, \mathbf{0}, \zeta I)$. ρ is a state, called a *Werner state*, iff $\zeta \in [-1, \frac{1}{3}]$. If $\zeta \in [0, \frac{1}{3}]$ then $\mu_j = \zeta$, $j = 1, 2, 3$ and therefore $\xi(\rho) = 0$ by (8.1). If $\zeta \in [-1, -\frac{1}{3}]$ then $\mu_j = -\zeta$, $j = 1, 2, 3$ and therefore by (8.1)

$$\xi(\rho) = \max\left(0, -\frac{1}{2}(1 + 3\zeta)\right)$$

which is 0 for $\zeta \in [-\frac{1}{3}, 0]$ and varies between 0 and 1 as ζ varies from $-\frac{1}{3}$ to -1.

Remark 8.5. Wootters (1998) extends the concurrence from pure to arbitrary states in a different way. He defines the concurrence of an arbitrary state ρ via the following formula

$$C(\rho) = \max(0, \kappa_1 - \kappa_2 - \kappa_3 - \kappa_4)$$

where $\kappa_1 \geq \kappa_2 \geq \kappa_3 \geq \kappa_4$ are the eigenvalues in descending order of the positive-semidefinite operator

$$R = \left(\rho^{\frac{1}{2}}\rho^{\#}\rho^{\frac{1}{2}}\right)^{\frac{1}{2}}$$

It is easy to prove that for all mds states ρ, $C(\rho) = \xi(\rho)$, that is, on these special states the two extensions agree.

9. SOME EXAMPLES

(1) Following Horodecki *et al.* (1996) we give an example of a nonseparable state whose mds component is separable. Let

$$\chi_1 = \cos\beta(e_1 \otimes e_1) + \sin\beta(e_2 \otimes e_2)$$

$$\chi_2 = \cos\beta(e_1 \otimes e_2) + \sin\beta(e_2 \otimes e_1)$$

with $0 < \beta < \pi/2$. Then χ_1 and χ_2 are orthogonal and

$$\begin{aligned} P_1 = |\chi_1\rangle\langle\chi_1| &= \frac{1}{4}(\cos^2\beta(\mathbf{1} + \sigma_3) \otimes (\mathbf{1} + \sigma_3) \\ &\quad + 2\cos\beta\sin\beta(\sigma_1 \otimes \sigma_1 - \sigma_2 \otimes \sigma_2) + \sin^2\beta(\mathbf{1} - \sigma_3) \otimes (\mathbf{1} - \sigma_3)) \\ &= \rho\big(-F_2\cos 2\beta\mathbf{e}_3, \cos 2\beta\mathbf{e}_3, -F_2\big(\sin 2\beta\big(I - E_{\mathbf{e}_3}\big) + E_{\mathbf{e}_3}\big)\big) = P_{\cos 2\beta\mathbf{e}_3, F_2} \\ P_2 = |\chi_2\rangle\langle\chi_2| &= \frac{1}{4}(\cos^2\beta(\mathbf{1} + \sigma_3) \otimes (\mathbf{1} - \sigma_3) \\ &\quad + 2\cos\beta\sin\beta(\sigma_1 \otimes \sigma_1 + \sigma_2 \otimes \sigma_2) + \sin^2\beta(\mathbf{1} - \sigma_3) \otimes (\mathbf{1} + \sigma_3)) \\ &= \rho\big(\cos 2\beta\mathbf{e}_3, -\cos 2\beta\mathbf{e}_3,\ \mathrm{diag}(\sin 2\beta, \sin 2\beta, -1)\big) \\ &= \rho\big(-F_3(-\cos 2\beta\mathbf{e}_3), -\cos 2\beta\mathbf{e}_3, -F_3\big(\sin 2\beta\big(I - E_{\mathbf{e}_3}\big) + E_{\mathbf{e}_3}\big)\big) \\ &= P_{-\cos 2\beta\mathbf{e}_3, F_3} \end{aligned}$$

From these formulae we see that $P_1, P_2 \in \mathcal{P}_\xi$, with $\xi = \sin 2\beta$ and thus (for the given range of β) both pure states are nonseparable.

Now for $0 \leq p \leq 1$ consider the state

$$\begin{aligned} \rho &= (pP_1 + (1-p)P_2) \\ &= \rho(\cos 2\beta\mathbf{e}_3, (2p-1)\cos 2\beta\mathbf{e}_3,\ \mathrm{diag}(\sin 2\beta, (1-2p)\sin 2\beta, 2p-1) \end{aligned}$$

whose spectrum is given by $\mathrm{sp}\,\rho = (0, p, 1-p)$. Note that

$$\det T = -(1-2p)^2\sin^2 2\beta$$

which is negative for the given range of β except for $p = \frac{1}{2}$. Thus we may put $\varepsilon = -1$. To write down a canonical form for ρ we have to distinguish four cases;

Case 1: $0 \leq p \leq \frac{1}{2}(1 - \sin 2\beta)$

$$\rho^{(1)} = \rho(\cos 2\beta\mathbf{e}_1, -(1-2p)\cos 2\beta\mathbf{e}_1, -D_1)$$

where $D_1 =$ diag$((1-2p), \sin 2\beta, (1-2p)\sin 2\beta)$

Case 2: $\frac{1}{2}(1-\sin 2\beta) \leq p \leq \frac{1}{2}$

$$\rho^{(2)} = \rho(\cos 2\beta \mathbf{e}_2, -(1-2p)\cos 2\beta \mathbf{e}_2, -D_2)$$

where $D_2 =$ diag$(\sin 2\beta, (1-2p), (1-2p)\sin 2\beta)$

Case 3:

$$\rho^{(3)} = \rho(\cos 2\beta \mathbf{e}_2, -(2p-1)\cos 2\beta \mathbf{e}_2, -D_3)$$

where $D_3 =$ diag$(\sin 2\beta, (2p-1), (2p-1)\sin 2\beta)\rho$

Case 4:

$$\rho^{(4)} = \rho(-\cos 2\beta \mathbf{e}_1, (2p-1)\cos 2\beta \mathbf{e}_1, -D_4)$$

where $D_4 =$ diag$((2p-1), \sin 2\beta, (2p-1)\sin 2\beta)$.

To investigate if ρ^{mds} or ρ is separable it suffices to consider the matrix of

$$\widehat{\rho^{(1)}} = \rho(\cos 2\beta \mathbf{e}_1, (1-2p)\text{cos}2\beta \mathbf{e}_1, D_1)$$

relative to the Bell basis. It is easily computed as $[\widehat{\rho^{(1)}}]_\phi =$

$$\begin{bmatrix} \frac{1}{2}(p-(1-p)\sin 2\beta) & i\frac{p}{2}\cos 2\beta & 0 & 0 \\ -i\frac{p}{2}\cos 2\beta & \frac{1}{2}(p+(1-p)\sin 2\beta) & 0 & 0 \\ 0 & 0 & \frac{1}{2}((1-p)-p\sin 2\beta) & -i\frac{1-p}{2}\cos 2\beta \\ 0 & 0 & i\frac{1-p}{2}\cos 2\beta & \frac{1}{2}((1-p)+p\sin 2\beta \end{bmatrix}$$

The eigenvalues of $\widehat{\rho^{mds}}$ are the diagonal entries of this matrix. ρ^{mds} is separable iff they are all nonnegative, that is, iff $\frac{\sin 2\beta}{1+\sin 2\beta} \leq p \leq \frac{1}{1+\sin 2\beta}$. For example if $\beta = \pi/12$ ρ^{mds} is separable for any value of $p \in [\frac{1}{3}, \frac{2}{3}]$. What about ρ itself? For the separability of ρ it is necessary and sufficient that the smallest eigenvalue $\hat{\lambda}_1$ of $\hat{\rho}$ is nonnegative. $\hat{\lambda}_1$ is given by the formula

$$2\hat{\lambda}_1 = \begin{cases} p - \sqrt{p^2 + (1-2p)\sin^2 2\beta} & \text{if } 0 \leq p \leq \dfrac{1}{2} \\ 1 - p - \sqrt{(1-p)^2 + (2p-1)\sin^2 2\beta} & \text{if } \dfrac{1}{2} \leq p \leq 1 \end{cases}$$

an expression that is nonnegative iff $p = \frac{1}{2}$. Thus unless $p = 1/2$, ρ is *not* separable and introducing the auxiliary function

$$h(p, \beta) = \sqrt{p^2 + (1-2p)\sin^2 2\beta} - p$$

the *concurrence* of ρ is given by

$$\xi(\rho) = \begin{cases} h(p, \beta) & \text{if } 0 \leq p \leq \dfrac{1}{2} \\ h(1-p, \beta) & \text{if } \dfrac{1}{2} \leq p \leq 1 \end{cases}$$

For $p = \frac{1}{2}\xi(\rho) = h(\frac{1}{2}, \beta) = 0$ and thus ρ becomes separable. The same conclusion can be reached by looking at the explicit formula for ρ in this special case: $\rho = \rho(\cos 2\beta \mathbf{e}_3, \mathbf{0}, \operatorname{diag}(\sin 2\beta, 0, 0))$ and by invoking Corollary 5.3 or by directly noticing that

$$\rho \sim \rho(\cos 2\beta F_3 \mathbf{e}_3, \mathbf{0}, F_3 \operatorname{diag}(\sin 2\beta, 0, 0)) = \rho(\cos 2\beta \mathbf{e}_3, \mathbf{0}, \\ -\operatorname{diag}(\sin 2\beta, 0, 0)) = \hat{\rho}$$

To summarize, *ρ is separable iff $p = \frac{1}{2}$; if $\beta \neq \frac{\pi}{4}$ then $\rho^{mds} \neq \rho$ and ρ^{mds} is separable for all $p \in [\frac{\sin 2\beta}{1+\sin 2\beta}, \frac{1}{1+\sin 2\beta}]$*.

For $\beta = \pi/12$ and for $\beta = \frac{\pi}{4}$ ρ is separable iff $p = \frac{1}{2}$. For $\beta = \frac{\pi}{4}$ $\rho^{mds} = \rho$ whereas for $\beta = \pi/12$ $\rho^{mds} \neq \rho$ and ρ^{mds} is separable for $p \in \left[\frac{1}{3}, \frac{2}{3}\right]$.

(2) Let $\rho = \rho(\mathbf{r}, \mathbf{s}, 0)$. Then ρ is already in canonical form and the commutant group G and the invariance group G' of ρ both coincide with the full rotation group $SO(3)$. Therefore $\rho \sim \rho' = \rho(\|\mathbf{r}\|\mathbf{e}_3, \|\mathbf{s}\|\mathbf{e}_3, 0)$. The matrix of ρ' relative to the standard basis is diagonal and the spectrum of ρ is given by

$$\operatorname{sp} \rho = \{1 + \|\mathbf{r}\| + \|\mathbf{s}\|, 1 + \|\mathbf{r}\| - \|\mathbf{s}\|, 1 - \|\mathbf{r}\| + \|\mathbf{s}\|, 1 - \|\mathbf{r}\| - \|\mathbf{s}\|\}$$

Hence ρ is a state iff $\|\mathbf{r}\| + \|\mathbf{s}\| \leq 1$.

The state is separable, which can be seen directly, since $\rho' \sim \rho(\|\mathbf{r}\|\mathbf{e}_3, -\|\mathbf{s}\|\mathbf{e}_3, 0)$ or by invoking Corollary 5.5 (See Fig. 1).

10. SOME APPLICATION TO PHYSICS

In this last section we assume that the qubits are realized by spin-1/2 particles. We start with certain properties of physical significance that a nonseparable state of a pair of qubits necessarily possesses.

Theorem 10.1. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a state of a pair of qubits that is not a product of two one-particle states in which one or both factors are pure states. Then the maps f and g defined on the unit sphere S^2 by*

$$f(\mathbf{x}) = \frac{\mathbf{r} + T\mathbf{x}}{1 + \mathbf{s} \cdot \mathbf{x}}, \quad \mathbf{x} \in S^2 \tag{10.1}$$

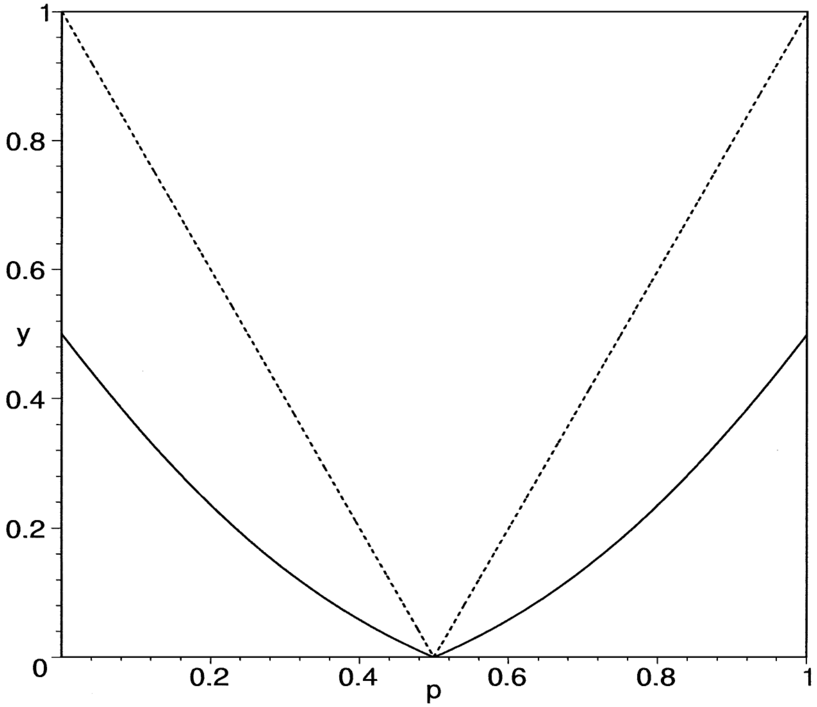

Fig. 1. Concurrence of ρ as as function of p for $\beta = \pi/12$ and $\beta = \pi/4$.

and

$$g(\mathbf{x}) = \frac{\mathbf{s} + T^*\mathbf{x}}{1 + \mathbf{r}\cdot\mathbf{x}}, \quad \mathbf{x} \in S^2 \tag{10.2}$$

are well-defined and they map S^2 into B^3. In the case where ρ is pure f and g map the unit sphere S^2 bijectively onto itself. In fact letting τ denote the antipodal map $\tau(\mathbf{x}) = -\mathbf{x}$, $\mathbf{x} \in S^2$, $\tau \circ g \circ \tau$ is the inverse of f and $\tau \circ f \circ \tau$ is the inverse of g.

Proof: By Theorem 7.2 the hypothesis of the theorem is equivalent to $\|\mathbf{r}\| < 1$ & $\|\mathbf{s}\| < 1$, which implies that for all $\mathbf{x} \in S^2$ $1 + \mathbf{s}\cdot\mathbf{x} \geq 1 - \|\mathbf{s}\| > 0$ and $1 + \mathbf{r}\cdot\mathbf{x} \geq 1 - \|\mathbf{r}\| > 0$, so that f and g are well defined.

Now assume that $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is a pure state and let $\mathbf{x} \in S^2$. Then by Eqs. (4.8), (4.9), (4.11), and (4.12)

$$\begin{aligned}\|\mathbf{r} + T\mathbf{x}\|^2 - (1 + \mathbf{s}\cdot\mathbf{x})^2 &= \|\mathbf{r}\|^2 - 1 + 2(T^*\mathbf{r} - \mathbf{s})\cdot\mathbf{x} + \mathbf{x}^*(T^*T - |\,\mathbf{s} >< \mathbf{s}\,|)\mathbf{x} \\ &= \|\mathbf{s}\|^2 - 1 - \det T\,\|\mathbf{x}\|^2 = (\|\mathbf{s}\|^2 - 1)(1 - \|\mathbf{x}\|^2) = 0\end{aligned}$$

which shows that f maps S^2 into itself. In a similar way, using Eq. (4.10) one proves that g maps S^2 into itself. One easily verifies, using Eqs. (4.8), (4.9), (4.10), and (4.11), that the maps $f \circ \tau$ and $g \circ \tau$ are inverses of each other.

Finally let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be an arbitrary state and let

$$\rho(\mathbf{r}, \mathbf{s}, T) = \sum_{k=1}^{4} w_k \rho(\mathbf{r}_k, \mathbf{s}_k, T_k)$$

be its spectral resolution. Then for $\mathbf{x} \in S^2$

$$\|\mathbf{r} + T\mathbf{x}\| \leq \sum_{k=1}^{4} w_k \|\mathbf{r}_k + T_k\mathbf{x}\| \leq \sum_{k=1}^{4} w_k (1 + \mathbf{s}_k \cdot \mathbf{x}) = (1 + \mathbf{s} \cdot \mathbf{x})$$

which shows that f maps S^2 into B^3. By an analogous argument one shows that g also maps S^2 into B^3. □

Suppose we have a pair of spin-1/2 particles prepared into a state $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$.

Question 1: In what state are the individual constituents of the pair?

Answer: Each constituent particle is in the respective *reduced state* as defined by Eqs. (3.6) and (3.7).

In the special case where ρ has been prepared into a pure state of the mds type ($\mathbf{r} = \mathbf{s} = \mathbf{0}$) we have a well-known paradox: Although the pair is in a state of maximal information the individual constituents are in a state of minimal information (in a state of maximal disorder).

Question 2: What is the probability that a measurement of the observable $1 \otimes \mathbf{a} \cdot \sigma$, where $\mathbf{a}$ is a *unit vector*, yields outcome $+1$? Keeping in mind that we are dealing with a pair of spin-1/2 particles the question can be rephrased. Suppose we measure on particle 2 the component of the spin vector in direction $\mathbf{a}$ by performing a Stern–Gerlach experiment, what is the probability that the particle has its spin (vector) "up," that is, aligned with the direction $\mathbf{a}$?

Answer: The probability is

$$\langle \rho, \mathbf{1} \otimes \rho(\mathbf{a}) \rangle = \langle \rho_2, \rho(\mathbf{a}) \rangle = \langle \rho(\mathbf{s}), \rho(\mathbf{a}) \rangle = \frac{1}{2}(1 + \mathbf{s} \cdot \mathbf{a})$$

Question 3: Suppose the outcome of the measurement is actually $+1$, what state do we now assign to the pair of particles?

Answer: By the von Neumann projection postulate the state after a measurement of $\mathbf{1} \otimes \mathbf{a} \cdot \sigma$ with outcome $+1$ is given by

$$\rho' = \frac{2}{1 + \mathbf{s} \cdot \mathbf{a}} (\mathbf{1} \otimes \rho(\mathbf{a}))\rho(\mathbf{1} \otimes \rho(\mathbf{a})) = \frac{1}{2(1 + \mathbf{s} \cdot \mathbf{a})}$$
$$\times \Bigg(\mathbf{1} \otimes \rho(\mathbf{a}) + \mathbf{r} \cdot \sigma \otimes \rho(\mathbf{a}) + \mathbf{1} \otimes \rho(\mathbf{a})(\mathbf{s} \cdot \sigma)\rho(\mathbf{a})$$
$$+ \sum_{j=1}^{3} \sum_{k=1}^{3} t_{jk}(\sigma_j \otimes \rho(\mathbf{a})\sigma_k \rho(\mathbf{a}) \Bigg)$$
$$= \frac{1}{2}\left(\mathbf{1} + \frac{(\mathbf{r} + T\mathbf{a}) \cdot \sigma}{1 + \mathbf{s} \cdot \mathbf{a}} \right) \otimes \rho(\mathbf{a}) = \rho(f(\mathbf{a})) \otimes \rho(\mathbf{a}),$$

where f is defined by (10.1). Physically this means that the two spin-1/2 particles are now disentangled. The second particle is in the pure state $\rho(\mathbf{a})$ with its spin aligned with the direction $\mathbf{a}$, whereas the first particle is in the state $\rho(f(\mathbf{a}))$, which in general is a *mixed state*. However, in the special case where the original state ρ of the pair was *pure*, it follows from Theorem 10.1 that the first particle too is in a pure state, having its spin vector aligned with the direction $f(\mathbf{a})$. For example, if $\rho = P_{\mathbf{0},R} = \rho(\mathbf{0}, \mathbf{0}, -R)$ was a pure state of the *mds type*, then after a measurement of the observable $\mathbf{1} \otimes \mathbf{a} \cdot \sigma$ yielding outcome $+1$, the first particle will be in the pure state $\rho(-R\mathbf{a})$; in particular if the original state ρ of the pair was the *singlet* state $\rho = P_\mathbf{0} = P_{\mathbf{0},I} = \rho(\mathbf{0}, \mathbf{0}, -I)$, then after the measurement the first particle will have its spin vector aligned with the opposite direction $-\mathbf{a}$.

Similarly if we measure $\mathbf{a} \cdot \sigma \otimes \mathbf{1}$ and find the outcome $+1$, after the measurement the system will be in the product state $\rho(\mathbf{a}) \otimes \rho(g(\mathbf{a}))$ where g is defined by (10.2).

To not unduly interrupt the flow of the argument we relegated a few results and their proofs into two appendices:

APPENDIX A: SOME GROUP-THEORETICAL RESULTS

We start with an elementary group-theoretical result.

Proposition A.1. *Let G be a group and let G' be a normal subgroup. Then the set*

$$H := \{(g_1, g_2) \in G \times G \mid g_1 \equiv g_2 \bmod G'\}$$

is a subgroup of $G \times G$.

Proof: Let $(g_1, g_2), (h_1, h_2) \in H$. From $g_1 \equiv g_2 \mod G'$ we get $g_1 h_1^{-1} \equiv g_2 h_1^{-1} \mod G'$. But since $h_1 \equiv h_2 \mod G'$ we have

$$g_2 h_1^{-1} = g_2 h_1^{-1} h_2 h_2^{-1} \equiv g_2 h_2^{-1} \quad \mod G'$$

Thus by transitivity $g_1 h_1^{-1} \equiv g_2 h_2^{-1} \mod G'$, which proves that

$$(g_1, g_2) \cdot (h_1, h_2)^{-1} \in H \quad \square$$

The next result pertains to the stabilizer of a positive semidefinite matrix

Proposition A.2. *Let n be a positive integer and let $D = \operatorname{diag}(\mu_1, \mu_2, \ldots, \mu_n)$ be a diagonal matrix with nonnegative entries in descending order $\mu_1 \geq \mu_2 \geq \ldots \mu_n \geq 0$ and let H be the stabilizer of D, that is, the group*

$$H_D = \left\{(R_1, R_2) \in SO(3) \times SO(3) \mid R_1 D R_2^* = D\right\}$$

Let G be the group of all rotations that commute with D:

$$G := \{R \in SO(n) \mid DR = DR\}$$

and let G' be the group of all rotations leaving D fixed by multiplication from the left:

$$G' := \{R \in SO(n) \mid RD = D\}$$

Then

(1) *G' is a normal subgroup of G.*
(2) *$H_D = \{(R_1, R_2) \in G \times G \mid R_1 \equiv R_2 \mod G'\}$*

Proof: (1) Suppose $R' \in G'$. Taking the transpose of the equation $R'D = D$ we obtain $DR'^* = D$ which by multiplication by R' from the right gives $D = DR'$. Thus $R' \in G$ and G' is a subgroup of G. Now for $R \in G$ we have

$$RR'R^* D = RR'DR^* = RDR^* = D$$

and thus $DR'R^* \in G'$, showing that G' is normal in G.

(2) Suppose first that $(R_1, R_2) \in H_D$. Then $R_1 D = DR_2$ holds. Taking the transpose we obtain $DR_1^* = R_2^* D$. Multiplication of this equation from the left by R_2 and from the right by R_1 gives $R_2 D = DR_1$. Multiplication of this equation from left by D gives $DR_2 D = D^2 R_1$. But by the original equation $DR_2 D = R_1 D^2$. Thus $R_1 D^2 = D^2 R_1$, which implies $R_1 \in G$. Similarly $R_2 \in G$. Now the original equation can be rewritten as $R_2^* R_1 D = D$, which means $R_1 \equiv R_2 \mod G'$. Conversely suppose that $R_1, R_2 \in G$ and $R_1 \equiv R_2 \mod G'$. Then $R_1 D R_2^* = R_1 R_2^* D = D$ and therefore $(R_1, R_2) \in H_D$. $\square$

Theorem A.3. *Let V be a finite dimensional real inner product space. Let $GL(V)$ be the group of all invertible linear transformations of V endowed with usual topology (i.e., the topology induced by the operator norm). Let G be a compact subgroup of $GL(V)$ and let*

$$G\mathbf{x} = \{g(\mathbf{x}) \mid g \in G\}$$

be the orbit of G determined by $\mathbf{x} \in V$. Then the set of extreme points of the convex hull $S = \mathrm{conv}G\mathbf{x}$ of $G\mathbf{x}$ coincides with $G\mathbf{x}$.

Proof: As the continuous image of a compact set, $G\mathbf{x}$ is compact. It follows that $S = \mathrm{conv}G\mathbf{x}$ is compact. (Theorem 2.8 in Brønsted, 1982) Hence the set of extreme points of S is contained in $G\mathbf{x}$. (Theorem 5.10 in Brønsted, 1982) But since S is invariant under G the same must be true for the set of extreme points: Every point in $G\mathbf{x}$ is extreme. □

APPENDIX B: SOME APPLICATIONS OF THE THEORY OF CONVEX CONES

We start with the proposition that a state $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ is separable iff $\hat{\rho} = \rho(\mathbf{r}, -\mathbf{s}, -T)$ is also a state. We have seen that the condition is necessary (Lemma 5.1). We want to show that the condition is also sufficient. For this purpose we need to invoke some elementary results from the theory of convex cones. A good source of this material is Hilgert *et al.* (1989). We first introduce the (closed) convex cone

$$\mathcal{K} = \bigcup_{\gamma \geq 0} \gamma \mathcal{S}_0$$

generated by the set $\mathcal{S}_0$ of all separable states within the real vector space $\mathcal{H}_4$ of all hermitian operators and its dual cone:

$$\widetilde{\mathcal{K}} = \{h \in \mathcal{H}_4 \mid \forall h' \in \mathcal{K} \; \langle h, h' \rangle \geq 0\}$$

We have the inclusions $\mathcal{K} \subset \mathcal{H}_4^+ \subset \widetilde{\mathcal{K}}$ and $\mathcal{K}$ is *generating*, that is, $\mathcal{K} - \mathcal{K} = \mathcal{H}_4$, an assertion that follows from (3.3) and the equations

$$\mathbf{1} = \rho(\mathbf{e}_1) + \rho(-\mathbf{e}_1)$$

$$\sigma_k = \rho(\mathbf{e}_k) - \rho(-\mathbf{e}_k), \quad k = 1, 2, 3,$$

where $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ denotes the standard basis in $\mathbb{R}^3$. The statement that $\mathcal{K}$ is generating is equivalent to the statement that $\widetilde{\mathcal{K}}$ is a *proper cone*, that is, it has the property $(-\widetilde{\mathcal{K}}) \cap \widetilde{\mathcal{K}} = \{0\}$ (cf. Hilgert *et al.* (1989), Proposition I.1.7). We first focus our attention on the dual cone $\widetilde{\mathcal{K}}$. Let $\mathcal{L}(\mathcal{H}_2)$ be the space of all linear transformations of $\mathcal{H}_2$. By endowing $\mathcal{L}(\mathcal{H}_2)$ with the trace inner product

$$\langle \Lambda, \Lambda' \rangle = \mathrm{trace}(\Lambda^* \Lambda'), \quad \Lambda, \Lambda' \in \mathcal{L}(\mathcal{H}_2),$$

where Λ^* denotes the adjoint of Λ, $\mathcal{L}(\mathcal{H}_2)$ becomes an *inner product space*. A linear transformation Λ of $\mathcal{L}_2$ is said to be *positive* provided Λ leaves the positive cone $\mathcal{H}_2^+ \subset \mathcal{H}_2$ invariant. The set $\mathcal{L}(\mathcal{H}_2)^+$ of all positive linear transformations constitute a convex cone within $\mathcal{L}(\mathcal{H}_2)$, which can be used to characterize $\widetilde{\mathcal{K}}$. In fact we have

Theorem B.1. *Let $\mathcal{J} : \mathcal{L}(\mathcal{H}_2) \to \mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$ be the linear map defined by*

$$\mathcal{J}(\Lambda) = 2(\mathbf{1} \otimes \Lambda)P_0, \quad \Lambda \in \mathcal{L}(\mathcal{H}_2),$$

where $\mathbf{1}$ *denotes the identity transformation of $\mathcal{H}_2$ and $P_0 = \rho(\mathbf{0}, \mathbf{0}, -I)$ is the singlet state. Then $\mathcal{J}$ is an isometry onto $\mathcal{H}_4$ and*

$$\widetilde{\mathcal{K}} = \mathcal{J}(\mathcal{L}(\mathcal{H}_2)^+).$$

Proof: Throughout this proof we denote the 2×2 identity matrix by σ_0, reserving the symbol $\mathbf{1}$ for the identity transformation of $\mathcal{H}_2$.

(1) Let $\Lambda_{jk} \in \mathcal{L}(\mathcal{H}_2)$, $j, k = 0, 1, 2, 3$ be the transition operators between the members of the orthonormal basis (2.7). Explicitly Λ_{jk} is defined by

$$\Lambda_{jk}(a) = \frac{1}{2}\langle \sigma_k, a \rangle \sigma_j, \quad a \in \mathcal{H}_2, \quad j, k = 0, 1, 2, 3.$$

By linear algebra generalities these transition operators constitute an orthonormal basis in $\mathcal{L}(\mathcal{H}_2)$. It is easily verified that the images $\mathcal{J}(\Lambda_{jk})$ are given by the formulas

$$\mathcal{J}(\Lambda_{j0}) = \frac{1}{2}(\sigma_0 \otimes \sigma_j), \quad j = 0, 1, 2, 3$$
$$\mathcal{J}(\Lambda_{jk}) = -\frac{1}{2}(\sigma_k \otimes \sigma_j), \quad j = 0, 1, 2, 3 \;\; k = 1, 2, 3,$$

and hence they constitute an orthonormal basis in $\mathcal{H}_4$. This proves that $\mathcal{J}$ is an isometry onto $\mathcal{H}_4$.

(2) The remainder of the proof rests on the formula

$$\forall \mathbf{x}\mathbf{y} \in S^2 : \langle \Lambda(\rho(-\mathbf{x})), \rho(\mathbf{y}) \rangle = \langle \rho(\mathbf{x}) \otimes \rho(\mathbf{y}), \mathcal{J}(\Lambda) \rangle \tag{B.1}$$

which holds for any linear transformation Λ of $\mathcal{H}_2$. For the proof of (B.1) we apply Λ to the expression

$$\rho(-\mathbf{x}) = \frac{1}{2}\left(\langle \rho(\mathbf{x}), \sigma_0 \rangle \sigma_0 - \sum_{k=1}^{3} \langle \rho(\mathbf{x}), \sigma_k \rangle \sigma_k \right)$$

and then form the inner product with $\rho(\mathbf{y})$. We obtain

$$\begin{aligned}\langle\Lambda(\rho(-\mathbf{x})),\rho(\mathbf{y})\rangle &= \frac{1}{2}\left(\langle\rho(\mathbf{x}),\sigma_0\rangle\langle\Lambda(\sigma_0),\rho(\mathbf{y})\rangle - \sum_{k=1}^{3}\langle\rho(\mathbf{x}),\sigma_k\rangle\langle\Lambda(\sigma_k),\rho(\mathbf{y})\rangle\right)\\ &= \frac{1}{2}\left\langle\rho(\mathbf{x})\otimes\rho(\mathbf{y}),\sigma_0\otimes\Lambda(\sigma_0) - \sum_{k=1}^{3}\sigma_k\otimes\Lambda(\sigma_k)\right\rangle\\ &= 2\langle\rho(\mathbf{x})\otimes\rho(\mathbf{y}),(\mathbf{1}\otimes\Lambda)P_0\rangle = \langle\rho(\mathbf{x})\otimes\rho(\mathbf{y}),\mathcal{J}(\Lambda)\rangle.\end{aligned}$$

(3) Now suppose that $\Lambda \in \mathcal{L}(\mathcal{H}_2)^+$. Then the left hand side of (B.1) is nonnegative for all $\mathbf{x},\mathbf{y} \in S^2$. Hence the same is true for the right hand side: $\mathcal{J}(\Lambda) \in \tilde{K}$.

Conversely suppose that $h \in \tilde{K}$ and let $\Lambda = \mathcal{J}^{-1}(h)$. Then the right hand side of (B.1) is nonnegative for all $\mathbf{x},\mathbf{y} \in S^2$. Hence the same is true for the left hand side, which implies that $\Lambda \in \mathcal{L}(\mathcal{H}_2)^+$. □

Lemma B.2. *Every positive linear map $\Lambda : \mathcal{H}_2 \to \mathcal{H}_2$ has the form $\Lambda = \lambda + \theta\lambda'$, where λ and λ' are completely positive and θ denotes the positive linear involution of $\mathcal{H}_2$ (time reversal) defined by*

$$\theta(h(\gamma,\mathbf{a})) = h(\gamma,-\mathbf{a}), \quad h \in \mathcal{H}_2.$$

Proof: It is well-known that every positive linear transformation of $\mathcal{H}_2$ has the form

$$\Lambda = \lambda + \tau\lambda'' \tag{B.2}$$

where λ and λ'' are completely positive and $\tau \in \mathcal{L}(\mathcal{H}_2)^+$ is the transposition $\tau(h) = h^t \in \mathcal{H}_2$ (cf. Woronowicz, 1976). In terms of the representation (3.1) of h the transposition can be expressed as

$$\tau(h(\gamma,\mathbf{r})) = h(\gamma,\mathbf{r})^t = h(\gamma,S\mathbf{r}), \quad h \in \mathcal{H}_2$$

where S stands for the reflection at the (1, 3)-coordinate plane. Hence

$$\begin{aligned}\tau(h(\gamma,\mathbf{r})) &= h(\gamma,S\mathbf{r}) = h(\gamma,F_2F_2S\mathbf{r}) = h(\gamma,-F_2\mathbf{r}) = \theta(h(\gamma,F_2\mathbf{r}))\\ &= \theta\big(u_0h(\gamma,\mathbf{r})u_0^*\big)\end{aligned}$$

where $u_0 \in U_1$ is defined by (2.2). In the last part of the equation we use Formula (3.2) in combination with the easily verifiable fact that $R(u_0) = F_2$. It follows that $\tau = \theta\circ\widetilde{u}_0$, where $\widetilde{u}_0$ stands for the conjugation by u_0. Inserting this expression into (B.2) we obtain the desired decomposition with $\lambda' = \widetilde{u}_0\circ\lambda''$. □

Theorem B.3.

$$\widetilde{\mathcal{K}} = \mathcal{H}_4^+ + \widehat{\mathcal{H}_4^+} \tag{B.3}$$

Proof: Since $\mathcal{K} \subset \mathcal{H}_4^+$ and by Lemma 5.1, $\mathcal{K} = \hat{\mathcal{K}} \subset \widehat{\mathcal{H}_4^+}$, and the cones $\mathcal{H}_4^+$ and $\widehat{\mathcal{H}_4^+}$ are self-dual, we obtain $\mathcal{H}_4^+ + \widehat{\mathcal{H}_4^+} \subset \tilde{\mathcal{K}}$. To prove the opposite inclusion suppose that $h \in \widetilde{\mathcal{K}}$. Then by Theorem B.1 h can be written as

$$h = (\mathbf{1} \otimes \Lambda)P_0$$

for some $\Lambda \in \mathcal{L}(\mathcal{H}_2)^+$. Now applying Lemma B.2 we obtain

$$h = (\mathbf{1} \otimes \Lambda)P_0 = (\mathbf{1} \otimes \lambda)P_0 + (\mathbf{1} \otimes \theta\lambda')P_0 = (\mathbf{1} \otimes \lambda)P_0 + (\widehat{\mathbf{1} \otimes \lambda'})P_0$$

where $\lambda, \lambda' : \mathcal{M}_2 \to \mathcal{M}_2$ are completely positive maps. This implies that $(\mathbf{1} \otimes \lambda)$ P_0, $(\mathbf{1} \otimes \lambda')P_0 \in \mathcal{H}_0^+$ and therefore $h \in \mathcal{H}_4^+ + \widehat{\mathcal{H}_4^+}$. □

Taking the dual of Eq. (B.3) and keeping in mind that $\mathcal{H}_4^+$ and $\widehat{\mathcal{H}_4^+}$ are self-dual, we obtain, using the bipolar theorem (cf. Propositions I.1.4 and I.1.6 in Hilgert *et al.*, 1989).

Corollary B.4.

$$\mathcal{K} = \mathcal{H}_4^+ \cap \widehat{\mathcal{H}_4^+}$$

Corollary B.5. *Let $\rho = \rho(\mathbf{r}, \mathbf{s}, T)$ be a state such that also $\hat{\rho} = \rho(\mathbf{r}, -\mathbf{s}, -T)$ is a state. Then ρ is separable.*

REFERENCES

Brønsted, A. (1982). An introduction to convex polytopes. In *Graduate Texts in Mathematics*, Vol. **90**, Springer-Verlag, New York.

Hilgert, J., Hofmann, K. H., and Lawson, J. D. (1989). *Lie Groups*, *Convex Cones and Semigroups*, Chap. I, Clarendon Press, Oxford.

Horodecki, R. and Horodecki, M. (1996). Information-theoretic aspects of inseparability of mixed states. *Physical Review A* **54**, 1838–1843.

Horodecki, M., Horodecki, P., and Horodecki, R. (1996a). Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A* **223**, 1–8.

Horodecki, R., Horodecki, M., and Horodecki, P. (1996b). Teleportation, Bell's inequalities and inseparability. *Physics Letters A* **222**, 21–25.

Horn, R. A. and Johnson, C. A. (1985). *Matrix Analysis*, section 7.3, Cambridge University Press.

Kummer, H. J. (1999). The state space of a pair of spin-1/2 particles. *International Journal of Theoretical Physics* **38**, 1741–1756.

Wootters, W. K. (1997). Entanglement of a pair of quantum bits. *Physical Review Letters* **78**, 5022–5025.

Wootters, W. K. (1998). Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters* **80**, 2245–2248.

Woronowicz, S. L. (1976). Positive maps of low dimensional matrix algebras. *Reports on Mathematical Physics* **10**, 165–183.