

Entangled qubit pairs

Dissertation an der Fakultät für Physik der
Ludwig-Maximilians-Universität München, vorgelegt von

Nasser Metwally Aly Mohamed

Aswan, Ägypten

February 28, 2002

Entangled qubit pairs

Dissertation an der Fakultät für Physik der
Ludwig-Maximilians-Universität München, vorgelegt von

Nasser Metwally Aly Mohamed

Aswan, Ägypten

February 28, 2002

Betreuung und Erstgutachten:
Priv.-Doz. Dr. B.-G. Englert

Zweitgutachten:
Prof. Dr. A. Schenzle

Tag der mündlichen Prüfung: 27.6.02

Abstract

In this study, some of the important properties of the states of qubit pairs are reviewed. They are specified by 15 numerical parameters that are naturally regarded as the components of two 3-vectors and 3×3 -dyadic. There are six classes of families of locally equivalent states in a straightforward scheme for classifying all 2-qubit states; four of the classes consist of two subclasses each. Easy-to-use criteria enable one to check whether a given pair of 3-vectors plus 3×3 -dyadic specify a 2-qubit state that is separable or not. The properties of Lewenstein-Sanpera decompositions are employed to split a given state into its optimal separable and pure parts. A number of examples for which the optimal decomposition is known explicitly are reported. A criterion is introduced to decide if a given decomposition is the optimal one or not. Two inequalities are obeyed if the decomposition in question is the optimal one and are violated if it is not. An alternative presentation of the IBM and Oxford purification protocols is obtained. Employing the properties of the characteristic values of the cross dyadic makes the Oxford protocol much faster.

Contents

1	Introduction	3
1.1	Overview of the thesis	5
1.2	Some algebraic notations	6
1.3	Separable and entangled 2-qubit states	11
1.4	Peres-Horodeccy criterion	12
2	Kinematics of qubit pairs	15
2.1	Representation of statistical operators	15
2.2	Invariants under local transformations	16
2.3	Generic form of a pure state	17
2.4	Generic form of a 2-qubit state	19
2.5	Families of 2-qubit states	20
2.5.1	Classes of families of locally equivalent states	21
3	Positivity and separability	25
3.1	A separability criterion	25
3.2	Separability and the cross dyadic	28
3.3	Examples	29
4	Lewenstein-Sanpera Decompositions	31
4.1	Basic properties of optimal LSDs	33
4.2	Optimal LSDs of truly positive states	35
4.2.1	The separable part has full rank	36
4.2.2	The separable part has reduced rank	39
4.2.3	Summary	40
4.3	Examples	41
4.3.1	Self-transposed states	41
4.3.2	Generalized Werner states	43
4.3.3	States of rank 2	47
4.3.4	States of rank “2+2”	57
4.3.5	States of rank 3	58
4.3.6	States of rank 4	63

5	Optimality of decompositions	67
5.1	Infinitesimal changes and optimality	67
5.1.1	Infinitesimal unitary transformations	67
5.1.2	Checking the optimality of a decomposition	69
5.1.3	Examples	71
6	Purification and degree of separability	75
6.1	Introduction	75
6.2	Local unitary transformation	76
6.3	IBM protocol	77
6.4	Oxford Protocol	78
6.4.1	Separability and purification	80
6.4.2	Discussion	82
7	Summary	85
A	Some separability criteria	89
A.1	Bell inequalities	89
A.2	Rení inequalities	90
A.3	The reduction criterion	90
A.4	Positive partial transpose	91
A.5	Volume of separable states	91
B	Some entanglement measures	93
B.1	Measures for pure states	93
B.2	Measures for mixed states	93
B.2.1	Entanglement of formation	94
B.2.2	Entanglement of distillation:	94
C	Infinitesimal changes	97
C.1	Werner state	97
C.2	2-qubit state	98

Chapter 1

Introduction

In the past few years, we have seen the beginnings of a new field in physics and information theory, *the physics of quantum information*, as a result of discovering the phenomenon of *quantum entanglement*, the origin of nonclassical correlations between the outcomes of local measurements performed on two particles. The great importance of quantum entanglement is known since 1935, when Einstein, Podolsky, and Rosen (EPR) considered a quantum system consisting of two particles which interacted with each other at some initial time and then moved off in opposite directions. Finally, the particles enter a measurement device to determine some classical properties of each of them independently. EPR insisted that a measurement on the first particle cannot have any actual influence on the second particle (*the locality condition*), thus the properties of the second particle must be independent of the measurements performed on the first one. The presence of nonclassical correlations – a well established experimental fact as tests of Bell’s inequality demonstrated that it is violated – is incomprehensible from this point of view.

The recent development of quantum information theory shows that entanglement can have important practical applications. In particular it turned out that entanglement can be used as a resource for communication of quantum states in an astonishing process called quantum teleportation [1,2,3], and also for quantum *coding*, [4] and for *cloning* [5,6]. Quantum entanglement is not only a fundamental resource in quantum communication, but also can be viewed as a resource in quantum *computation* [7], and quantum *cryptography* [8,9].

It is clear that the entanglement is very important for all quantum information tasks, so there arises naturally the question of how it can be quantified and manipulated. Attempts have been made to find meaningful measures of entanglement, such as the entanglement of formation [10,11], negativity [52], and relative entropy of entanglement [12] have been proposed. Moreover, some of the tasks of quantum information require maximally entangled states, so entanglement purification and distillation [13,14,15], namely the process of extracting maximally entangled states from input states, are very important manipulations

for quantum systems. They extract some more strongly entangled states from an ensemble of weakly entangled ones.

A qubit is, in general terms, a binary quantum alternative, for which there are many different physical realizations. Familiar examples include the binary alternatives of a Stern-Gerlach experiment (“spin up” or “spin down”); of a photon’s helicity (“left handed” or “right handed”); of two-level atoms (“in the upper state” or “in the lower one”); of Young’s double-slit set-up (“through this slit” or “through that slit”); of Mach-Zehnder interferometers (“reflected at the entry beam splitter” or “transmitted at it”); and of Ramsey interferometers (“transition in the first zone” or “in the second zone”).

The actual physical nature of the qubits in question is irrelevant, however, for the issues dealt with here. We are remarking on entangled states of two qubits, and as far as the somewhat abstract mathematical properties are concerned, all qubits are equal. In particular, the two qubits under consideration could be of quite different kinds, one the spin- $\frac{1}{2}$ degree of freedom of a silver atom, say, the other a photon’s helicity. It is even possible, and of experimental relevance [16, 17, 18], that both qubits are carried by the same physical object: the which-way alternative of an atom (photon, neutron, . . .) passing through an interferometer could represent one qubit, for instance, while its polarization (or another internal degree of freedom) is the other.

Entangled qubits are exploited in most schemes proposed for quantum communication purposes, for quantum information processing, or for the secure key distribution procedures known as quantum cryptography. The basic units are entangled qubit pairs. Obviously then, a thorough understanding of the properties of 2-qubit states is desirable. Although there has been considerable progress in this matter recently, the situation is still not fully satisfactory.

Whereas the possible states of a single qubit are easily classified with the aid of a 3-vector (the Bloch vector in one physical context, the Poincaré vector in another, and analogs of both in general — we shall speak of Pauli vectors), the classification of the states of entangled qubit pairs has not been fully achieved as yet. The obvious reason is the richness of the state space, which is parameterized by two 3-vectors, one for each qubit, and a 3×3 -dyadic that represents expectation values of joint observables, so that 15 real numbers are necessary to specify an arbitrary 2-qubit state.

The qubit pairs that we are concerning ourselves with are the simplest intertwined quantum systems. As such they are prototypical for more complicated systems, much like the hydrogen atom is the prototype of all atoms and molecules. Of course, constituting the simplest system conceivable, qubit pairs do not exhibit all the features that can be found in larger systems. In fact, the simplicity of a 2-qubit system is due to the fact that it consists of two parts only, and each part is a qubit.

1.1 Overview of the thesis

The aim of this study is to understand the properties of those most basic entangled states that consist of two qubits. In the rest of this chapter some algebraic notations, the separability of 2-qubits, and the Peres-Horodeccy criterion are introduced.

Chapter Two is studying the kinematics of 2-qubit states. The representation of 2-qubit states in a Hilbert space is introduced, where they are specified by 15 real numbers; 6 of them represent the components of the two Pauli vectors, one for each qubit, and a 3×3 dyadic represents the expectation values for the joint observables. A generic form for a 2-qubit pure state is obtained as well as a generic form for a general 2-qubit state. The behavior of a 2-qubit state under some local transformation is studied, where there are 9 independent combinations of the 15 numbers that are invariant under local transformations. There are six classes of families of locally equivalent states which classify all 2-qubit states.

Chapter Three gives a criterion to check if a given 2-qubit state is separable or not. This criterion depends on three numbers which are invariant under local transformations. If these values obey a certain set of three inequalities then the state in question is separable, if one or more of those inequalities are violated, then the state is non-separable. The two largest characteristic values of the 3×3 dyadic are employed as a test if a 2-qubit state obeys or violates the Clauser-Horne-Shimony-Holt (CHSH) inequality. This chapter ends with two examples showing how these procedures work.

For a finer distinction between non-separable states that shall enable us to tell the more useful states from the less useful ones for quantum communications, one asks for the degree of separability as a numerical measure for this usefulness. This is the aim of *Chapter Four*. The degree of separability is a part of the so called optimal Lewenstein-Sanpera decomposition (LSD) of a 2-qubit state. The general properties of this decomposition are studied, and the optimal decompositions are known for a number of relevant types of states. The relation between the degree of separability and what is called *concurrence* is investigated.

It is always possible to obtain a LSD, but it may be very difficult to decide if this decomposition is the optimal one. *Chapter Five* gives a criterion for the optimal decomposition. Two inequalities are obeyed if the decomposition in question is the optimal one and are violated if it is not.

In *Chapter Six*, the dynamical variables are used to describe the IBM and Oxford protocols for purification. An improved version of the Oxford protocol is described, in which local unitary transformations optimize each step. This alternative of the Oxford protocol is applied to an ensemble using imperfect operations. The degree of separability is introduced as a purity parameter, where the purified state has a smaller degree of separability than the initial one.

Finally, provided for reference, in Appendix A, I review some criteria of separability for pure and mixed states. Some popular entanglement measures for pure

and mixed states are given in Appendix B. The optimality criteria is obtained by the infinitesimal changes in the 15 parameters for any 2-qubit state. Appendix C gives these changes for the particular Werner states and also for any two-qubit state.

1.2 Some algebraic notations

Analogous of Pauli's spin operators are, as usual, used for the description of the individual qubits: the hermitian set $\sigma_x, \sigma_y, \sigma_z$ for the first qubit, and τ_x, τ_y, τ_z for the second. Upon introducing corresponding sets of three-dimensional unit vectors — $\vec{e}_x, \vec{e}_y, \vec{e}_z$ and $\vec{n}_x, \vec{n}_y, \vec{n}_z$, respectively, each set orthonormal and right-handed — we form the vector operators

$$\begin{aligned}\vec{\sigma} &= \sum_{\alpha=x,y,z} \sigma_\alpha \vec{e}_\alpha = (\sigma_x, \sigma_y, \sigma_z) \begin{pmatrix} \vec{e}_x \\ \vec{e}_y \\ \vec{e}_z \end{pmatrix}, \\ \vec{\tau} &= \sum_{\beta=x,y,z} \tau_\beta \vec{n}_\beta = (\tau_x, \tau_y, \tau_z) \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}.\end{aligned}\tag{1.1}$$

We emphasize that the two three-dimensional vector spaces thus introduced are unrelated and they may have nothing to do with the physical space. Even if the qubits should consist of the spin- $\frac{1}{2}$ degrees of freedom of two electrons, say, so that an identification with the physical space would be natural, we could still define the x , y , and z directions independently for both qubits.

As in [19, 20], we employ a self-explaining notation that distinguishes row vectors from column vectors, related to each other by transposition, as illustrated by

$$\sigma^\downarrow = \vec{\sigma}^T, \quad \vec{\tau} = \tau^\downarrow T,\tag{1.2}$$

for example. Scalar and vector products — denoted by a dot \cdot and a cross \times , respectively — such as the ones appearing in the basic algebraic relations

$$\begin{aligned}\vec{a}_1 \cdot \sigma^\downarrow \vec{a}_2 \cdot \sigma^\downarrow &= \vec{a}_1 \cdot \vec{a}_2 + i (\vec{a}_1 \times \vec{a}_2) \cdot \sigma^\downarrow, \\ \vec{b}_1 \cdot \tau^\downarrow \vec{b}_2 \cdot \tau^\downarrow &= \vec{b}_1 \cdot \vec{b}_2 + i (\vec{b}_1 \times \vec{b}_2) \cdot \tau^\downarrow, \\ \vec{a} \cdot \sigma^\downarrow \vec{b} \cdot \tau^\downarrow &= \vec{b} \cdot \tau^\downarrow \vec{a} \cdot \sigma^\downarrow,\end{aligned}\tag{1.3}$$

where $\vec{a}_1, \vec{a}_2, \vec{a}$ and $\vec{b}_1, \vec{b}_2, \vec{b}$ are arbitrary numerical vectors, involve rows and columns of the same type, that is: two of e -type or two of n -type. Numerical summands in operator equations, such as $\vec{a}_1 \cdot \vec{a}_2$ in the first statement of (1.3), are to be read as multiples of the identity operator.

Products of the ‘‘column times row’’ kind are dyadics, for which $\sigma^\downarrow \vec{\tau}$ is an important example; it is a column of e -type combined with a row of n -type. The transpose of such a en -dyadic is a ne -dyadic; there are also ee -dyadics and nn -dyadics. Suppose that \overleftarrow{A} and \overleftarrow{B} are two en -dyadics, so that their transposes $\overleftarrow{A}^T, \overleftarrow{B}^T$ are ne -dyadics. Then $\overleftarrow{A}^T \cdot \overleftarrow{B}$, for example, is a nn -dyadic and $\overleftarrow{B} \cdot \overleftarrow{A}^T$ is of ee -type. Yet another product of \overleftarrow{A} and \overleftarrow{B} is the symmetric two-fold vector product $\{\overleftarrow{A}, \overleftarrow{B}\} = \{\overleftarrow{B}, \overleftarrow{A}\}$, which is the en -dyadic defined by¹

$$\begin{aligned} & \frac{1}{2} \left(\vec{\sigma} \cdot \overleftarrow{A} \cdot \tau^\downarrow \vec{\sigma} \cdot \overleftarrow{B} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftarrow{B} \cdot \tau^\downarrow \vec{\sigma} \cdot \overleftarrow{A} \cdot \tau^\downarrow \right) \\ & = \text{Sp} \left\{ \overleftarrow{A}^T \cdot \overleftarrow{B} \right\} + \vec{\sigma} \cdot \left\{ \overleftarrow{A}, \overleftarrow{B} \right\} \cdot \tau^\downarrow . \end{aligned} \quad (1.4)$$

All properties of $\{\overleftarrow{A}, \overleftarrow{B}\}$ follow from its linearity in both \overleftarrow{A} and \overleftarrow{B} in conjunction with

$$\left\{ a_1^\downarrow \vec{b}_1, a_2^\downarrow \vec{b}_2 \right\} = a_1^\downarrow \times a_2^\downarrow \vec{b}_2 \times \vec{b}_1 , \quad (1.5)$$

where $a_1^\downarrow, a_2^\downarrow$ are any two columns of e -type and \vec{b}_1, \vec{b}_2 are any two rows of n -type. In particular, we have

$$\left\{ \overleftarrow{A}, \overleftarrow{A} \right\} = -2 \overleftarrow{A}_{\text{sub}} \quad (1.6)$$

and

$$\overleftarrow{A}^T \cdot \left\{ \overleftarrow{A}, \overleftarrow{A} \right\} = -2 \det \left\{ \overleftarrow{A} \right\} \overleftarrow{\mathbf{1}}_{nn} , \quad (1.7)$$

where the en -dyadic $\overleftarrow{A}_{\text{sub}}$ consists of the signed sub-determinants, the cofactors, of \overleftarrow{A} , and $\overleftarrow{\mathbf{1}}_{nn}$ is the unit dyadic of nn -type. The implied identities

$$\left(\overleftarrow{A}_{\text{sub}} \right)_{\text{sub}} = \overleftarrow{A} \det \left\{ \overleftarrow{A} \right\} \quad (1.8)$$

and

$$2 \text{Sp} \left\{ \overleftarrow{A}_{\text{sub}}^T \cdot \overleftarrow{A}_{\text{sub}} \right\} = \left(\text{Sp} \left\{ \overleftarrow{A}^T \cdot \overleftarrow{A} \right\} \right)^2 - \text{Sp} \left\{ \left(\overleftarrow{A}^T \cdot \overleftarrow{A} \right)^2 \right\} \quad (1.9)$$

are worth remembering.

As an immediate consequence of (1.3) all functions of $\vec{\sigma}$ and $\vec{\tau}$ are linear in these Pauli vector operators. An arbitrary 2-qubit state is therefore specified by a statistical operator of the form

$$\rho = \frac{1}{4} \left(1 + \vec{\sigma} \cdot \vec{s}^\downarrow + \vec{t} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftarrow{C} \cdot \tau^\downarrow \right) ; \quad (1.10)$$

¹We write $\text{Sp} \{ \}$ for the trace of a dyadic and $\text{tr} \{ \}$ for the quantum mechanical operator trace.

it determines the expectation values $\langle f(\vec{\sigma}, \vec{\tau}) \rangle$ of all operator functions $f(\vec{\sigma}, \vec{\tau})$ in accordance with $\langle f(\vec{\sigma}, \vec{\tau}) \rangle = \text{tr}\{f(\vec{\sigma}, \vec{\tau})\rho\}$. Rather than distinguishing pedantically between a 2-qubit state and its statistical operator ρ , we'll simply speak of "the state ρ ." It involves the real *cross dyadic* \overleftrightarrow{C} ,

$$\overleftrightarrow{C} = \langle \sigma^\downarrow \vec{\tau} \rangle = (e_x^\downarrow, e_y^\downarrow, e_z^\downarrow) \begin{pmatrix} C_{xx} & C_{xy} & C_{xz} \\ C_{yx} & C_{yy} & C_{yz} \\ C_{zx} & C_{zy} & C_{zz} \end{pmatrix} \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}, \quad (1.11)$$

in addition to the two real *Pauli vectors* s^\downarrow and \vec{t} ,

$$s^\downarrow = \langle \sigma^\downarrow \rangle = (e_x^\downarrow, e_y^\downarrow, e_z^\downarrow) \begin{pmatrix} s_x \\ s_y \\ s_z \end{pmatrix}, \quad \vec{t} = \langle \vec{\tau} \rangle = (t_x, t_y, t_z) \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}. \quad (1.12)$$

Note that ρ is properly normalized to unit trace by construction, but restrictions apply to \vec{s} , t^\downarrow , and \overleftrightarrow{C} to ensure its positivity, $\rho \geq 0$.

In addition to the pre-chosen *xyz* coordinate systems, we also need to consider 123 coordinate systems that are adapted to the 2-qubit state of interest. Then

$$\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) \begin{pmatrix} \vec{e}_1 \\ \vec{e}_2 \\ \vec{e}_3 \end{pmatrix}, \quad \tau^\downarrow = (n_1^\downarrow, n_2^\downarrow, n_3^\downarrow) \begin{pmatrix} \tau_1 \\ \tau_2 \\ \tau_3 \end{pmatrix} \quad (1.13)$$

are the respective parameterizations of $\vec{\sigma}$ and τ^\downarrow , and \overleftrightarrow{C} is represented by the 9 numbers $\vec{e}_j \cdot \overleftrightarrow{C} \cdot n_k^\downarrow$ with $j, k = 1, 2, 3$.

For 2-qubit states, there are two much used bases in the Hilbert space. One of them is the disentangled basis which consists of common eigenkets (or eigenbras) of σ_z and τ_z . The other basis is called entangled basis, it is also known as *Bell basis*. Hill and Wootters, [21, 22] call it the *magic basis*. It consists of common eigenstates of $\sigma_1\tau_1$, $\sigma_2\tau_2$, and $\sigma_3\tau_3$ as in Table 1.1. One can use this basis to write

ket	Bell Basis	Magic Basis	$\sigma_1\tau_1$	$\sigma_2\tau_2$	$\sigma_3\tau_3$
$ ++\rangle = \frac{1}{2}(10\rangle + 01\rangle)$	$-i \psi^+\rangle$	$ e_3\rangle$	1	1	1
$ +-\rangle = \frac{1}{2}(11\rangle + 00\rangle)$	$ \phi^+\rangle$	$ e_1\rangle$	1	-1	1
$ -\rangle = \frac{i}{2}(11\rangle - 00\rangle)$	$-i \phi^-\rangle$	$ e_2\rangle$	-1	1	1
$ --\rangle = \frac{i}{2}(10\rangle - 01\rangle)$	$-i \psi^-\rangle$	$ e_4\rangle$	-1	-1	-1

Table 1.1: Entanglement basis.

a given operator in matrix form. A 4×4 -matrix representation of the operators has imaginary antisymmetric matrices for the Pauli operators,

$$\vec{\sigma} \cdot s^\downarrow + \vec{t} \cdot \tau^\downarrow \cong \begin{bmatrix} 0 & -i(s_1 + t_1) & i(s_2 + t_2) & -i(s_3 - t_3) \\ i(s_1 + t_1) & 0 & i(s_3 + t_3) & i(s_2 - t_2) \\ -i(s_2 + t_2) & -i(s_3 + t_3) & 0 & i(s_1 - t_1) \\ i(s_3 - t_3) & -i(s_2 - t_3) & -i(s_1 - t_3) & 0 \end{bmatrix}, \quad (1.14)$$

and real symmetric matrices for their products,

$$\vec{\sigma} \cdot \overleftrightarrow{C} \cdot \tau^\downarrow \cong \begin{bmatrix} c_{11} + c_{22} - c_{33} & c_{23} + c_{32} & c_{13} + c_{31} & -c_{12} + c_{21} \\ c_{23} + c_{32} & c_{11} - c_{22} + c_{33} & -c_{12} - c_{21} & -c_{13} + c_{31} \\ c_{13} + c_{31} & -c_{12} - c_{21} & -c_{11} + c_{22} + c_{33} & c_{23} - c_{32} \\ -c_{12} + c_{21} & -c_{13} + c_{31} & c_{23} - c_{32} & -c_{11} - c_{22} - c_{33} \end{bmatrix}. \quad (1.15)$$

Now, if the state ρ is represented by a 4×4 matrix of this kind, then the transposed matrix represents the related state

$$\rho^\top = \frac{1}{4} \left(1 - \vec{\sigma} \cdot s^\downarrow - \vec{t} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftrightarrow{C} \cdot \tau^\downarrow \right), \quad (1.16)$$

the so-called the (*total*) *transpose* of ρ . Although the transformation

$$\vec{\sigma} \rightarrow -\vec{\sigma}, \quad \tau^\downarrow \rightarrow -\tau^\downarrow \quad (1.17)$$

is not unitary, the two states ρ and ρ^\top have the same eigenvalues and are, therefore, unitary equivalent, but the unitary operator U that effects $\rho \rightarrow U^{-1}\rho U = \rho^\top$ is not universal, it depends on the particular ρ under consideration. Equivalently, we can think of $\rho \rightarrow \rho^\top$ as resulting from

$$s^\downarrow \rightarrow -s^\downarrow, \quad \vec{t} \rightarrow -\vec{t}, \quad \overleftrightarrow{C} \rightarrow \overleftrightarrow{C}. \quad (1.18)$$

Consistent with its definition in terms of transposed matrices, but also as implied by the two-fold Pauli algebra specified by (1.3), the total transpose of a product $\rho_1\rho_2$ is given by $\rho_2^\top\rho_1^\top$.

This natural property of a transposition is not possessed by the two kinds of *partial transposition* introduced by

$$\begin{aligned} \rho &\rightarrow \rho^{\top_1} = \frac{1}{4} \left(1 - \vec{\sigma} \cdot s^\downarrow + \vec{t} \cdot \tau^\downarrow - \vec{\sigma} \cdot \overleftrightarrow{C} \cdot \tau^\downarrow \right), \\ \text{that is: } &\vec{\sigma} \rightarrow -\vec{\sigma}, \quad \tau^\downarrow \rightarrow \tau^\downarrow \\ \text{or, equivalently, } &s^\downarrow \rightarrow -s^\downarrow, \quad \vec{t} \rightarrow \vec{t}, \quad \overleftrightarrow{C} \rightarrow -\overleftrightarrow{C} \\ \text{or, compactly, } &\rho \rightarrow \rho^{\top_1} = \frac{1}{2} (\vec{\sigma} \cdot \rho \sigma^\downarrow - \rho) \end{aligned} \quad (1.19)$$

for the first qubit and analogously for the second qubit by

$$\begin{aligned} \rho &\rightarrow \rho^{\overline{T}_2} = \frac{1}{2} (\vec{\tau} \cdot \rho \tau^\downarrow - \rho) \\ \text{or } s^\downarrow &\rightarrow s^\downarrow, \quad \vec{t} \rightarrow -\vec{t}, \quad \overline{C} \rightarrow -\overline{C}. \end{aligned} \quad (1.20)$$

As the two compact versions emphasize, these partially transposed states are weighted sums of 4 unitarily equivalent states with three weights of $+\frac{1}{2}$ and one weight of $-\frac{1}{2}$. As a rule, therefore, the common eigenvalues of $\rho^{\overline{T}_1}$ and $\rho^{\overline{T}_2}$ are different from the common eigenvalues of ρ and $\rho^{\overline{T}}$, and the partial transposes of a given ρ are not assuredly positive, they are not guaranteed to be states themselves.

Although $(\rho_1 \rho_2)^{\overline{T}_1} = \rho_2^{\overline{T}_1} \rho_1^{\overline{T}_1}$ does *not* hold in general, traces of products do behave benignly inasmuch as

$$\text{tr} \{ \rho_1 \rho_2^{\overline{T}} \} = \text{tr} \{ \rho_1^{\overline{T}} \rho_2 \} = \text{tr} \{ \rho_1^{\overline{T}_1} \rho_2^{\overline{T}_2} \} = \text{tr} \{ \rho_1^{\overline{T}_2} \rho_2^{\overline{T}_1} \} \quad (1.21)$$

is true for all 2-qubit states ρ_1, ρ_2 . In this context the positivity of ρ_1 and ρ_2 is not essential. With $s_1^\downarrow, \vec{t}_1, \overline{C}_1$ and $s_2^\downarrow, \vec{t}_2, \overline{C}_2$ parameterizing ρ_1 and ρ_2 , respectively, we have, for example,

$$\begin{aligned} \text{tr} \{ \rho_1 \rho_2 \} &= \frac{1}{4} \left(1 + \vec{s}_1 \cdot \vec{s}_2^\downarrow + \vec{t}_1 \cdot \vec{t}_2^\downarrow + \text{Sp} \{ \overline{C}_1^{\overline{T}} \cdot \overline{C}_2 \} \right), \\ \text{tr} \{ \rho_1^{\overline{T}_1} \rho_2 \} &= \frac{1}{4} \left(1 - \vec{s}_1 \cdot \vec{s}_2^\downarrow + \vec{t}_1 \cdot \vec{t}_2^\downarrow - \text{Sp} \{ \overline{C}_1^{\overline{T}} \cdot \overline{C}_2 \} \right), \\ \text{tr} \{ \rho_1^{\overline{T}} \rho_2 \} &= \frac{1}{4} \left(1 - \vec{s}_1 \cdot \vec{s}_2^\downarrow - \vec{t}_1 \cdot \vec{t}_2^\downarrow + \text{Sp} \{ \overline{C}_1^{\overline{T}} \cdot \overline{C}_2 \} \right), \end{aligned} \quad (1.22)$$

as explicit numerical statements about such traces.

Further we note these properties of transpositions, all of which are immediate consequences of (1.16)–(1.20): they are linear, trace-conserving mappings; the adjoint of a transpose is the transpose of the adjoint; partially transposing the first qubit and the second, in either order, amounts to a total transposition; two successive transpositions of the same kind compensate for each other; and, in a sequence of successive transpositions, the order in which they are executed does not matter.

Following Hill and Wootters [21, 22], we associate a non-negative *concurrence* \mathcal{C} with each 2-qubit state ρ . It is given by

$$\mathcal{C}(\rho) = \max \left\{ 0, 2 \max_k \{ h_k \} - \sum_k h_k \right\}, \quad (1.23)$$

where h_1, h_2, h_3, h_4 are the four non-negative eigenvalues of

$$\left| \sqrt{\rho^{\overline{T}}} \sqrt{\rho} \right| = \sqrt{\sqrt{\rho} \rho^{\overline{T}} \sqrt{\rho}}. \quad (1.24)$$

Roughly speaking, the concurrence vanishes unless one of these eigenvalues is exceedingly large. The roles of ρ and ρ^\top can be interchanged in this definition of \mathcal{C} ; thus the concurrence of ρ^\top is equal to the concurrence of ρ . It is of practical importance that h_1^2, \dots, h_4^2 are the eigenvalues of the products $\rho^\top \rho$ and $\rho \rho^\top$ which, as a rule, are not hermitian themselves. Its convexity,

$$\mathcal{C}(x\rho_1 + (1-x)\rho_2) \leq x\mathcal{C}(\rho_1) + (1-x)\mathcal{C}(\rho_2) \quad \text{for } 0 \leq x \leq 1, \quad (1.25)$$

is a particularly important property of the Hill–Wootters concurrence.

The two product dyadics $\overleftrightarrow{C} \cdot \overleftrightarrow{C}^\top$ and $\overleftrightarrow{C}^\top \cdot \overleftrightarrow{C}$ are symmetric and possess the same eigenvalues which are denoted by c_1^2, c_2^2 and c_3^2 . The non-negative numbers c_1, c_2 , and c_3 are the characteristic values of the dyadic \overleftrightarrow{C} . By convention they are ordered as $c_1 \geq c_2 \geq c_3 \geq 0$. There is a special role played by the two largest characteristic values of the \overleftrightarrow{C} , the sum of their square sets the bounds in the two sided inequality,

$$-2\sqrt{c_1^2 + c_2^2} \leq \vec{a}_1 \cdot \overleftrightarrow{C} \cdot b_1^\downarrow - \vec{a}_1 \cdot \overleftrightarrow{C} \cdot b_2^\downarrow + \vec{a}_2 \cdot \overleftrightarrow{C} \cdot b_1^\downarrow + \vec{a}_2 \cdot \overleftrightarrow{C} \cdot b_2^\downarrow \leq 2\sqrt{c_1^2 + c_2^2}, \quad (1.26)$$

where \vec{a}_1, \vec{a}_2 and $b_1^\downarrow, b_2^\downarrow$ are four unit vectors.

1.3 Separable and entangled 2-qubit states

An arbitrary 2-qubit state is described by the density operator (1.10). If the cross dyadic is a product, $\overleftrightarrow{C} = s^\downarrow \vec{t}$, then the two-qubit state is of product form

$$\rho = \frac{1}{2}(1 + \vec{s} \cdot \sigma^\downarrow) \frac{1}{2}(1 + \vec{\tau} \cdot t^\downarrow), \quad (1.27)$$

so that results of measurements on the first qubit show no correlations whatsoever with measurement results concerning the second qubit. Under these circumstances the 2-qubit system is *not entangled*. Entangled qubit pairs, $\overleftrightarrow{C} \neq s^\downarrow \vec{t}$, may be in a mixed state blended from disentangled ingredients,

$$\rho = \sum_n w_n \frac{1}{2} (1 + \vec{\sigma} \cdot s_n^\downarrow) \frac{1}{2} (1 + \vec{t}_n \cdot \tau^\downarrow) \\ \text{with } w_n > 0, \quad \sum_n w_n = 1; \quad (1.28)$$

then all correlations found in the measurement data can be understood classically. States of this kind are called *separable*. The decomposition (1.28) of a separable state into the convex sum of product states is not unique; if one wishes one can always use pure product states for this purpose. More generally, as demonstrated by Wootters [22], one can always write a given ρ as a mixture of four or fewer pure states with the same concurrence as ρ .

By construction, the subspace of separable states is convex and compact. As Hill and Wootters have shown [21, 22], the concurrence of a separable state vanishes, and non-separable states have truly positive concurrences. Correlations of a genuine quantum character require a non-separable state ρ .

One of the important mathematical problems in quantum information theory is the characterization of separable states. A condition that is satisfied by all separable states and is violated by some non-separable states can serve as a separability criterion. If a separability criterion is violated by a state, the state must be entangled. In the following section I review one of the most popular criteria of separability, called Peres-Horodeccy Criterion, which is used throughout this thesis. In Appendix A, I review some other important criteria.

1.4 Peres-Horodeccy criterion

A state is called separable, if it can be prepared by two parties Alice and Bob in a “classical” way, that is, by agreeing over the phone on the local preparation of states. A density matrix that has been created in this way can only contain classical correlations. Mathematically this means: a state ρ can be written as a decomposition of the form (1.28). Finding such a decomposition for a given state ρ or proving that it does not exist, is a non-trivial task. So, one needs criteria that are easier to test.

An important forward step was taken by Peres [23], when he derived a simple necessary criterion to test the separability of a given state. This criterion is called “positive partial transposition (PPT) criterion”. It is based on the positivity of the operator obtained after partially transposing the given density operator.

Definition: A state ρ is separable if all eigenvalues of its partial transpose, ρ^{T_2} are non negative.

The Peres criterion, PPT, is distinguished from the earlier ones by its structure. It does not say that some scalar function of a state satisfies some inequalities, but it imposes constraints on the structure of the operator resulting from partial transposition. As an example the 2-qubit state (1.10) is separable if all the eigenvalues of ρ^{T_2}

$$\rho^{\text{T}_2} = \frac{1}{4} \left(1 + \vec{\sigma} \cdot s^\downarrow - \vec{t} \cdot \tau^\downarrow - \vec{\sigma} \cdot \vec{C} \cdot \tau^\downarrow \right) ; \quad (1.29)$$

are non-negative.

M., P., and R. Horodecki [24], proved that the positivity of the partial transposition criterion (Peres-Horodeccy criterion) is a necessary and sufficient condition for the separability of systems 2×2 and 2×3 . Their study of separability focuses on positive maps.

Definition: A map Λ is called positive if for every non-negative operator \mathcal{O} the operator $\mathcal{O}' = \Lambda(\mathcal{O})$ is again a non-negative operator.

If $\text{tr} \{\mathcal{O}'\} = \text{tr} \{\mathcal{O}\}$ for every \mathcal{O} , then the map Λ is called a *trace-preserving* map. These kinds of maps are important in quantum mechanics, since they transform the set of density operators to itself.

Theorem: A state ρ that acts on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if and only if for any positive map Λ , the operator $I \otimes \Lambda\rho \geq 0$.

The most famous and physically relevant example of a non-unitary positive map is the matrix transposition. So we can write the Peres-Horodeccy criterion as $I \otimes T\rho \geq 0$ [24, 25].

For high-dimensional states, the Peres-Horodeccy criterion is only necessary. P. Horodecki [26] has constructed some classes of families of inseparable states with positive partial transposition for 3×3 and 2×4 systems. States of this kind are said to possess bound entanglement (BE). More details for the separability of high-dimensional states are given in Appendix A.

Chapter 2

Kinematics of qubit pairs

2.1 Representation of statistical operators

For any general matrix $N \times N$, the complex matrix is specified by $2N^2$ real parameters. If this matrix is a hermitian operator the number is reduced by a factor 2, and the unit trace reduces it by one more, leaving $N^2 - 1$ real parameters. So, one needs $N + 1$ measurements to determine the state uniquely [27].

For the 2-qubit state (1.10), the components of the two Bloch vectors \vec{s}, \vec{t} and the elements c_{ij} for the crosses dyadic \overleftrightarrow{C} are given by:

$$\begin{aligned} s_i &= \text{tr} \{ \rho \sigma_i \} = \langle \sigma_i \rangle, & t_i &= \text{tr} \{ \rho \tau_i \} = \langle \tau_i \rangle, \\ C_{ij} &= \text{tr} \{ \rho (\sigma_i \tau_j) \} = \langle \sigma_i \tau_j \rangle, & i, j, k &= 1, 2, 3. \end{aligned} \quad (2.1)$$

we can see that there are 15 expectation values that constitute \vec{s}, \vec{t} and \overleftrightarrow{C} . They can be obtained by measuring 5 well chosen 2-qubit observables such as the ones specified in Table 2.1. These 5 observables are pairwise complementary and thus represent an optimal set. Performing the partial trace of the second subsystem, one obtains the reduced density operator for the first one, ρ_1 . Also, the reduced density operator ρ_2 for the second subsystem is calculated in an analogous way, namely,

$$\rho_1 = \text{tr}_2 \{ \rho \}, \quad \rho_2 = \text{tr}_1 \{ \rho \}. \quad (2.2)$$

If the direct product of the reduced density operators of the subsystems ρ_1 and ρ_2 gives ρ , i.e. $\rho = \rho_1 \rho_2$, then we are dealing with disentangled qubits, if not, then:

$$\rho = \rho_1 \rho_2 + \frac{1}{4} \overleftrightarrow{\sigma} \cdot \overleftrightarrow{E} \cdot \tau^\downarrow \quad (2.3)$$

where \overleftrightarrow{E} is called *entanglement dyadic*. It is related to the Bloch vectors and the cross dyadic by,

$$\overleftrightarrow{E} = \overleftrightarrow{C} - s^\downarrow t = \langle \sigma^\downarrow \tau \rangle - \langle \sigma^\downarrow \rangle \langle \tau \rangle. \quad (2.4)$$

The 2-qubit observable	
which identifies the joint eigenstates of	determines the three expectation values
σ_x and τ_x	$\langle \sigma_x \rangle, \langle \tau_x \rangle, \langle \sigma_x \tau_x \rangle$
σ_y and τ_y	$\langle \sigma_y \rangle, \langle \tau_y \rangle, \langle \sigma_y \tau_y \rangle$
σ_z and τ_z	$\langle \sigma_z \rangle, \langle \tau_z \rangle, \langle \sigma_z \tau_z \rangle$
$\sigma_x \tau_y$ and $\sigma_y \tau_z$	$\langle \sigma_x \tau_y \rangle, \langle \sigma_y \tau_z \rangle, \langle \sigma_z \tau_x \rangle$
$\sigma_y \tau_x$ and $\sigma_z \tau_y$	$\langle \sigma_y \tau_x \rangle, \langle \sigma_z \tau_y \rangle, \langle \sigma_x \tau_z \rangle$

Table 2.1: A minimal set of five 2-qubit observables whose measurement supplies all 15 parameters that characterize the state ρ of (1.10).

Here are some examples for simple 2-qubit states. All projectors to the members of the disentangled basis have the entanglement dyadic $\overleftarrow{E} = 0$. All projectors to members of the entangled basis, Table 1.1, have vanishing Bloch vectors, so that $\overleftarrow{C} = \overleftarrow{E}$. Another example, for the hydrogen atom filtered through a strong-field Stern-Gerlach device, the component with electron spin-up and proton spin-down is characterised by \vec{s} along the z direction and \vec{t} along the $-z$ direction [28]. The density matrix of the system is,

$$\rho = \frac{1}{4}(1 + \sigma_z)(1 - \tau_z) \quad (2.5)$$

which is disentangled.

2.2 Invariants under local transformations

Unitary transformations that affect only one of the qubits or both qubits independently are *local* transformations. Geometrically speaking, local transformations rotate $\vec{\sigma}$ and τ^\downarrow ,

$$\vec{\sigma} \rightarrow \vec{\sigma} \cdot \overleftarrow{O}_{ee}, \quad \tau^\downarrow \rightarrow \overleftarrow{O}_{nn} \cdot \tau^\downarrow, \quad (2.6)$$

where \overleftarrow{O}_{ee} is a unimodular, orthogonal ee -dyadic, and \overleftarrow{O}_{nn} is one of nn -type. Equivalently, one can think of rotating the Pauli vectors and the cross dyadic,

$$s^\downarrow \rightarrow \overleftarrow{O}_{ee} \cdot s^\downarrow, \quad \vec{t} \rightarrow \vec{t} \cdot \overleftarrow{O}_{nn}, \quad \overleftarrow{C} \rightarrow \overleftarrow{O}_{ee} \cdot \overleftarrow{C} \cdot \overleftarrow{O}_{nn}, \quad (2.7)$$

where,

$$\overleftarrow{O}_{ee} = e_1^\downarrow \vec{e}_x + e_2^\downarrow \vec{e}_y + e_3^\downarrow \vec{e}_z, \quad \overleftarrow{O}_{nn} = n_1^\downarrow \vec{n}_x + n_2^\downarrow \vec{n}_y + n_3^\downarrow \vec{n}_z, \quad . \quad (2.8)$$

These dyadics relate the x, y, z description to the 1, 2, 3 one. The freedom to choose $e_x^\downarrow, e_y^\downarrow, e_z^\downarrow$ and $\vec{n}_x, \vec{n}_y, \vec{n}_z$ turns a given ρ into a physically equivalent

one [19]. It is clearly that each of them needs 3 parameters for its specification, so there are 9 independent combinations of \vec{s} , t^\downarrow , and \overleftarrow{C} that are invariant under the transformations (2.7),

$$\begin{aligned}
a_1^{(2)} &= \text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\}, & a_2^{(2)} &= \vec{s} \cdot s^\downarrow, & a_3^{(2)} &= \vec{t} \cdot t^\downarrow, \\
a_1^{(3)} &= \det \left\{ \overleftarrow{C} \right\}, & a_2^{(3)} &= \vec{s} \cdot \overleftarrow{C} \cdot t^\downarrow, \\
a_1^{(4)} &= \text{Sp} \left\{ \left(\overleftarrow{C}^T \cdot \overleftarrow{C} \right)^2 \right\}, & a_2^{(4)} &= \vec{s} \cdot \overleftarrow{C}_{\text{sub}} \cdot t^\downarrow \\
a_3^{(4)} &= \vec{s} \cdot \overleftarrow{C} \cdot \overleftarrow{C}^T \cdot s^\downarrow, & a_4^{(4)} &= \vec{t} \cdot \overleftarrow{C}^T \cdot \overleftarrow{C} \cdot t^\downarrow.
\end{aligned} \tag{2.9}$$

As an important example consider the determinant of the entanglement dyadic,

$$\det \left\{ \overleftarrow{E} \right\} = \det \left\{ \overleftarrow{C} \right\} - \vec{s} \cdot \overleftarrow{C}_{\text{sub}} \cdot t^\downarrow = a_1^{(3)} - a_2^{(4)}. \tag{2.10}$$

2.3 Generic form of a pure state

The statistical operators $\rho_p = |\psi\rangle\langle\psi|$ that project to arbitrary 2-qubit ket vectors $|\psi\rangle$ make up classes of unitarily equivalent states characteristic by a parameter, say, p , which is equal to the common length of the Bloch vectors,

$$p^2 = \vec{s} \cdot s^\downarrow = \vec{t} \cdot t^\downarrow. \tag{2.11}$$

If one uses the property of the pure states $\rho_p^2 = \rho_p$, then the following equalities hold

$$\begin{aligned}
\vec{s} &= \overleftarrow{C} \cdot t^\downarrow, & \vec{t} &= \vec{s} \cdot \overleftarrow{C}, & \vec{s} \cdot \overleftarrow{C} \cdot t^\downarrow &= p^2, \\
s^\downarrow \vec{t} &= \overleftarrow{C} + \overleftarrow{C}_{\text{sub}} \quad \text{or} \quad \overleftarrow{E} = -\overleftarrow{C}_{\text{sub}}, \\
\text{Sp} \left\{ \overleftarrow{C}^T \overleftarrow{C} \right\} &= 1 - 2 \det \left\{ \overleftarrow{C} \right\}, & \text{Sp} \left\{ \left(\overleftarrow{C}^T \cdot \overleftarrow{C} \right)^2 \right\} &= 1 + 2 \det \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\}.
\end{aligned} \tag{2.12}$$

The characteristic values of the cross dyadic \overleftarrow{C} are

$$c_1 = 1, \quad c_2 = c_3 = \sqrt{1 - p^2} = q. \tag{2.13}$$

As a consequence, a general 2-qubit pure state ρ_p is,

$$\rho_p = \frac{1}{4} \left(1 + p(\sigma_1 - \tau_1) - \sigma_1 \tau_1 - q(\sigma_2 \tau_2 + \sigma_3 \tau_3) \right) \tag{2.14}$$

where $\sigma_j = \vec{\sigma} \cdot e_j^\downarrow$ and $\tau_j = \vec{\tau} \cdot n_j^\downarrow$ for $j = 1, 2, 3$. The components of the Pauli vector operators in the characteristic basis of the cross dyadic \overleftarrow{C} are specified by

$$s^\downarrow = p e_1^\downarrow, \quad \vec{t} = -p \vec{n}_1, \tag{2.15}$$

and the cross dyadic and the entanglement dyadic appear as

$$\begin{aligned}\overline{C} &= -e_1^\downarrow \vec{n}_1 - q(e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3), \\ \overline{E} &= -q^2 e_1^\downarrow \vec{n}_1 - q(e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3).\end{aligned}\quad (2.16)$$

A pure state is converted into another one with the same value of p by a reorientation of the two characteristic bases that consist of the e_j^\downarrow 's and the \vec{n}_j 's. The reorientations are achieved by rotations, one for each qubit. So, the pure states with the same p are related to each other by local unitary transformation for example:

$$(e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \rightarrow (-e_1^\downarrow, -e_2^\downarrow, e_3^\downarrow), \quad \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix} \rightarrow \begin{pmatrix} -\vec{n}_1 \\ -\vec{n}_2 \\ \vec{n}_3 \end{pmatrix} \quad (2.17)$$

These unitary transformations effectively reverse the sign of p in (2.15), (2.16).

Thus, any pure 2-qubit state is essentially characterized by the common length p of its Pauli vectors or by its concurrence q , available as $q^2 = \text{tr} \{ \rho_p^\top \rho_p \}$. For $p = 0$, $q = 1$ we have the family of Bell states (frequently called “maximally entangled states”),

$$\rho_{\text{Bell}} = \frac{1}{4} (1 - \sigma_1 \tau_1 - \sigma_2 \tau_2 - \sigma_3 \tau_3), \quad (2.18)$$

Local unitary transformations turn the generic Bell state (2.18) into any other Bell state. Accordingly, the general form of a Bell state is given by

$$\rho_{\text{Bell}} = \frac{1}{4} (1 - \vec{\sigma} \cdot \overline{O}_{en} \cdot \vec{\tau}^\downarrow), \quad (2.19)$$

where \overline{O}_{en} is any unimodular, orthogonal en -dyadic.

Since ρ_p^\top is obtained from ρ_p of (2.14) by $p \rightarrow -p$, the local transformation $(\sigma_1, \sigma_2, \sigma_3; \tau_1, \tau_2, \tau_3) \rightarrow (-\sigma_1, -\sigma_2, \sigma_3; -\tau_1, -\tau_2, \tau_3)$ turns them into each other. Therefore, ρ_p and ρ_p^\top belong to the same family of pure states. The same unitary transformation relates the two partial transposes. Their spectral decompositions are given by

$$\left. \begin{array}{l} \rho_p^{\top 1} \\ \rho_p^{\top 2} \end{array} \right\} = \frac{1 \pm p}{2} \rho_p^{(1)} + \frac{1 \mp p}{2} \rho_p^{(2)} + \frac{q}{2} \rho_p^{(3)} - \frac{q}{2} \rho_p^{(4)}, \quad (2.20)$$

where $\rho_p^{(1)}$, $\rho_p^{(2)}$ are product states and $\rho_p^{(3)}$, $\rho_p^{(4)}$ are Bell states,

$$\left. \begin{array}{l} \rho_p^{(1)} \\ \rho_p^{(2)} \end{array} \right\} = \frac{1}{4} (1 \mp \sigma_1)(1 \mp \tau_1), \quad \left. \begin{array}{l} \rho_p^{(3)} \\ \rho_p^{(4)} \end{array} \right\} = \frac{1}{4} (1 - \sigma_1 \tau_1 \pm \sigma_2 \tau_2 \pm \sigma_3 \tau_3). \quad (2.21)$$

Matters are particularly simple for Bell states for which we have

$$\rho_{\text{Bell}}^{\text{T}} = \rho_{\text{Bell}} , \quad \rho_{\text{Bell}}^{\text{T}_1} = \rho_{\text{Bell}}^{\text{T}_2} = \frac{1}{2} - \rho_{\text{Bell}} . \quad (2.22)$$

We learn here — what has been noted by Sanpera, Tarrach, and Vidal [29], for instance — that the partial transpose of a pure state with positive concurrence q has three positive and one negative eigenvalue and that, in particular, the eigenstate associated with the negative eigenvalue is a Bell state. More generally, the common eigenstates of $\rho_{\text{p}}^{\text{T}_1}$ and $\rho_{\text{p}}^{\text{T}_2}$ to the eigenvalue pair $\pm \frac{1}{2}q$ are Bell states. These are their one negative eigenvalue and the middle one of their three positive eigenvalues.

While we are at it, let us note that

$$\text{tr} \{ \rho_{\text{p}} \rho_{\text{Bell}} \} \leq \frac{1}{2}(1+q) = \frac{1}{2} + \frac{1}{2}(\text{tr} \{ \rho_{\text{p}}^{\text{T}} \rho_{\text{p}} \})^{\frac{1}{2}} \quad (2.23)$$

for any pure state (2.14) and all Bell states (2.19). If $q > 0$, the equality holds only for the Bell state $\rho_{\text{p}}^{(4)}$ in (2.20).

2.4 Generic form of a 2-qubit state

The general form for a 2-qubit state is given by (1.10), which involves the cross dyadic $\overleftrightarrow{\mathcal{C}}$ (1.11), in addition to the Pauli vectors (1.12). Our aim is transforming the given state (1.10) to a generic form. To perform this, one has to bring the dyadic $\overleftrightarrow{\mathcal{C}}$ to its diagonal form [30, 31]. The eigenrows ($\vec{e}_1, \vec{e}_2, \vec{e}_3$) are obtained by evaluating the eigenvalues and the eigenrows of the dyadic $\overleftrightarrow{\mathcal{C}} \cdot \overleftrightarrow{\mathcal{C}}^{\text{T}}$. In this case, the basis states \vec{n}_i are:

$$\vec{e}_k \cdot \overleftrightarrow{\mathcal{C}} = \pm c_k \vec{n}_k, \quad k = 1, 2, 3, \quad \text{where} \quad \vec{n}_j \cdot \vec{n}_k^{\downarrow} = \delta_{jk} \quad \text{and} \quad \vec{n}_1 \times \vec{n}_2 = \vec{n}_3. \quad (2.24)$$

One can also start with evaluating the eigenvalues and the eigenrows ($\vec{n}_1, \vec{n}_2, \vec{n}_3$) of $\overleftrightarrow{\mathcal{C}}^{\text{T}} \cdot \overleftrightarrow{\mathcal{C}}$. Then the \vec{e}_k states are obtained as

$$\overleftrightarrow{\mathcal{C}} \cdot \vec{n}_k^{\downarrow} = \pm c_k \vec{e}_k^{\downarrow}, \quad \text{where} \quad \vec{e}_j \cdot \vec{e}_k^{\downarrow} = \delta_{jk} \quad \text{and} \quad \vec{e}_1 \times \vec{e}_2 = \vec{e}_3. \quad (2.25)$$

Using the \vec{e}_k and \vec{n}_k basis, one can rewrite $\overleftrightarrow{\mathcal{C}}$ as

$$\overleftrightarrow{\mathcal{C}} = \pm (e_1^{\downarrow} c_1 \vec{n}_1 + e_2^{\downarrow} c_2 \vec{n}_2 + e_3^{\downarrow} c_3 \vec{n}_3) \quad \text{for} \quad \begin{cases} \det \{ \overleftrightarrow{\mathcal{C}} \} \geq 0, \\ \det \{ \overleftrightarrow{\mathcal{C}} \} < 0. \end{cases} \quad (2.26)$$

with its characteristic values ordered in accordance with

$$c_1 \geq c_2 \geq c_3 \geq 0, \quad (2.27)$$

In this case the unimodular orthogonal en -dyadic

$$\overrightarrow{\mathcal{O}}_{en} = e_1^\downarrow \vec{n}_1 + e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3 = (e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix} \quad (2.28)$$

turns the two 123 bases into each other. It also appears in

$$\overleftarrow{\mathcal{C}} = \pm \overrightarrow{\mathcal{O}}_{en} \cdot |\overleftarrow{\mathcal{C}}| = \pm |\overleftarrow{\mathcal{C}}^\text{T}| \cdot \overrightarrow{\mathcal{O}}_{en}, \quad (2.29)$$

which relate the cross dyadic $\overleftarrow{\mathcal{C}}$ to its modulus

$$|\overleftarrow{\mathcal{C}}| = \sqrt{\overleftarrow{\mathcal{C}}^\text{T} \cdot \overleftarrow{\mathcal{C}}} = n_1^\downarrow c_1 \vec{n}_1 + n_2^\downarrow c_2 \vec{n}_2 + n_3^\downarrow c_3 \vec{n}_3 \quad (2.30)$$

(a nn -dyadic) and to the modulus of $\overleftarrow{\mathcal{C}}^\text{T}$ (a ee -dyadic).

The sign in (2.26) and the values of the c_k 's are determined by the three local invariants

$$a_1^{(2)} = \text{Sp} \left\{ \overleftarrow{\mathcal{C}}^\text{T} \cdot \overleftarrow{\mathcal{C}} \right\}, \quad a_1^{(3)} = \det \left\{ \overleftarrow{\mathcal{C}} \right\}, \quad a_1^{(4)} = \text{Sp} \left\{ \left(\overleftarrow{\mathcal{C}}^\text{T} \cdot \overleftarrow{\mathcal{C}} \right)^2 \right\}. \quad (2.31)$$

The 123 bases are not uniquely specified by (2.26), however, because the simultaneous replacements (2.17), for example, do not change the sign of the dyadic $\overleftarrow{\mathcal{C}}$ of (2.26). The resulting freedom in choosing $e_1^\downarrow, e_2^\downarrow, e_3^\downarrow$ is used to enforce conventions imposed on the coefficients in

$$s^\downarrow = \langle \sigma^\downarrow \rangle = (e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}, \quad \vec{t} = \langle \vec{\tau} \rangle = (t_1, t_2, t_3) \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix}. \quad (2.32)$$

of the 15 parameters associated with the Pauli vectors and the cross dyadic in (1.10) or with the expectation values in Table 2.1, six are used up for the geometrical purpose of specifying the two 123 bases relative to the a priori xyz bases, so that nine parameters are left for the characterization of the essential physical properties of the state ρ in question. Three of them are the characteristic values of $\overleftarrow{\mathcal{C}}$, the other six are the coefficients of s^\downarrow and \vec{t} in the 123 bases. Since the 123 bases are not quite unique, one can exploit this freedom of choice to make as many as possible of these coefficients vanish and to give definite signs to as many as possible of the remaining ones [20, 32].

2.5 Families of 2-qubit states

Two density operators are in the same equivalence class if they differ only by local unitary transformation. For example, consider the density operator for one

qubit

$$\rho_1 = \frac{1}{2}(1 + \vec{s} \cdot \sigma^\dagger) = \frac{1}{2}(1 + s\sigma_1). \quad (2.33)$$

It is clear that, the coordinate 123 system has \vec{e}_1 in the \vec{s} direction. Then any two states of the form (2.33) are called locally equivalent if their Pauli vectors have the same length, i.e., the two states can only differ by the direction of \vec{e}_1 . This means that the difference of two equivalent states is only in the 123 basis that go with the generic form $\frac{1}{2}(1 + s\sigma_1)$.

To decide whether two given 2-qubit states belong to the same family, one has to put them into a generic form that is uniquely fixed by convenient conventions. For this aim, we employ the terminology and the notational conventions used in Section 1.2. The orthonormal-right handed vectors (1.13) have nothing to do with each other. In addition to these pre-chosen *xyz* coordinate systems, (1.1), we shall consider the 123 coordinate system that are adapted to the 2-qubit state of interest.

2.5.1 Classes of families of locally equivalent states

These classes of families depend on the characteristic values of the cross dyadic \overline{C} [20]. These values distinguish six classes of families,

$$\begin{aligned} c_1 = c_2 = c_3 = 0: & \quad \text{class A,} \\ c_1 = c_2 = c_3 > 0: & \quad \text{class B,} \\ c_1 > c_2 = c_3 = 0: & \quad \text{class C,} \\ c_1 > c_2 = c_3 > 0: & \quad \text{class D,} \\ c_1 = c_2 > c_3: & \quad \text{class E,} \\ c_1 > c_2 > c_3: & \quad \text{class F.} \end{aligned} \quad (2.34)$$

In classes *A* and *C* the + sign in (2.26) applies, both signs can occur in classes *B*, *D*, *E*, and *F* which, therefore, consist of two subclasses each. Using the local invariants given in (2.31), one finds the auxiliary quantities

$$\begin{aligned} a &= \frac{9}{4} \text{Sp} \{ \overline{C}^T \cdot \overline{C} \} \text{Sp} \left\{ \left(\overline{C}^T \cdot \overline{C} \right)^2 \right\} - \frac{5}{4} \left[\text{Sp} \{ \overline{C}^T \cdot \overline{C} \} \right]^3 + \frac{27}{2} \left[\det \{ \overline{C} \} \right]^2, \\ b &= \frac{3}{2} \text{Sp} \left\{ \left(\overline{C}^T \cdot \overline{C} \right)^2 \right\} - \frac{1}{2} \left[\text{Sp} \{ \overline{C}^T \cdot \overline{C} \} \right]^2, \end{aligned} \quad (2.35)$$

which are subject to $a^2 \leq b^3$. The values of a and b may be used to classify the states

$$\begin{aligned}
\text{class A} & \text{ if } a^2 = b^3 = 0 \text{ and } \det \left\{ \overleftarrow{C} \right\} = 0, \\
\text{class B} & \text{ if } a^2 = b^3 = 0 \text{ and } \det \left\{ \overleftarrow{C} \right\} \neq 0, \\
\text{class C} & \text{ if } a^2 = b^3 > 0 \text{ and } a > 0 \\
& \text{and } \det \left\{ \overleftarrow{C} \right\} = 0, \\
\text{class D} & \text{ if } a^2 = b^3 > 0 \text{ and } a > 0 \\
& \text{and } \det \left\{ \overleftarrow{C} \right\} \neq 0, \\
\text{class E} & \text{ if } a^2 = b^3 > 0 \text{ and } a < 0, \\
\text{class F} & \text{ if } a^2 < b^3.
\end{aligned} \tag{2.36}$$

The generic forms for the various classes are defined as follows.

Class A: Since $\overleftarrow{C} = 0$ one can choose the two sets of 123 coordinates independently, and $s_1 = s > 0$, $s_2 = s_3 = 0$ as well as $t_1 = t \geq 0$, $t_2 = t_3 = 0$ specify the conventions. This class consists of a two-parametric set of families of the generic form

$$\rho = \frac{1}{4}(1 + s\sigma_1 + t\tau_1) \quad \text{with } s \geq 0, t \geq 0. \tag{2.37}$$

For $s = 0$, $t = 0$, we have the chaotic state $\rho_{\text{chaos}} = \frac{1}{4}$ which forms a single-state family all by itself.

Class B: Here one can choose $e_1^\downarrow, e_2^\downarrow, e_3^\downarrow$ freely and the conventional choice is specified by

$$\begin{aligned}
s^\downarrow &= e_1^\downarrow s, \quad \vec{t} = t_1 \vec{n}_1 + t_3 \vec{n}_3 \\
\text{with } &\left\{ \begin{array}{l} s > 0 \text{ and } t_3 \geq 0 \\ \text{or} \\ s = 0 \text{ and } t_1 = t \geq 0, t_3 = 0 \end{array} \right\}.
\end{aligned} \tag{2.38}$$

Each subclass [\pm in (2.26)] consists of four-parametric sets of families. In passing we note that the so-called Werner states constitute the two class-**B** families with $s = 0$ and $t = 0$.

Class C: In this case the replacements (2.17) are used to enforce $s_1 \geq 0$ or $t_1 \geq 0$. If $s_1=0$ then $s_2 = 0, s_3 \geq 0$ and $t_2 = 0, t_3 \geq 0$ are achieved by suitable rotations of $e_2^\downarrow, e_3^\downarrow$ and, independently, of \vec{n}_1, \vec{n}_3 . This establishes

$$s^\downarrow = e_1^\downarrow s_1 + e_3^\downarrow s_3, \quad \vec{t} = t_1 \vec{n}_1 + t_3 \vec{n}_3, \quad \overleftarrow{C} = e_1^\downarrow c_1 \vec{n}_1 \tag{2.39}$$

$$\text{with } \left\{ \begin{array}{l} s_1 \geq 0 \\ \text{or} \\ s_1 = 0 \text{ and } t_1 \geq 0 \end{array} \right\} \text{ and } s_3 \geq 0, t_3 \geq 0$$

for the five-parametric sets of families.

Class D: In distinction from class C, the rotations in the 23 sectors are not independent here. Thus one has to leave $e_1^\downarrow \vec{n}_1$ and $e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3$ unchanged. In other words, we make a rotation round the 1-axis, so we have the following transformations:

$$\begin{aligned} e_1^\downarrow &\rightarrow e_1^\downarrow, & e_2^\downarrow &\rightarrow \cos \alpha e_2^\downarrow - \sin \alpha e_3^\downarrow, & e_3^\downarrow &\rightarrow \sin \alpha e_2^\downarrow + \cos \alpha e_3^\downarrow, \\ \vec{n}_1 &\rightarrow \vec{n}_1, & \vec{n}_2 &\rightarrow \cos \alpha \vec{n}_2 - \sin \alpha \vec{n}_3, & \vec{n}_3 &\rightarrow \sin \alpha \vec{n}_2 + \cos \alpha \vec{n}_3. \end{aligned} \quad (2.40)$$

Thus we get

$$\begin{aligned} s^\downarrow &= e_1^\downarrow s_1 + e_3^\downarrow s_3, & \vec{t} &= t_1 \vec{n}_1 + t_2 \vec{n}_2 + t_3 \vec{n}_3, \\ \vec{C} &= \pm (e_1^\downarrow c_1 \vec{n}_1 + e_2^\downarrow c_2 \vec{n}_2 + e_3^\downarrow c_3 \vec{n}_3) \end{aligned}$$

$$\text{with } \left\{ \begin{array}{l} s_1 \geq 0 \\ \text{or} \\ s_1 = 0 \text{ and } t_1 \geq 0 \end{array} \right\} \text{ and } \left\{ \begin{array}{l} s_3 \geq 0 \text{ and } t_2 \geq 0 \\ \text{or} \\ s_3 = 0 \text{ and } t_2 = 0, t_3 \geq 0 \end{array} \right\}. \quad (2.41)$$

Each subclass contains seven-parametric sets of families.

Class E: This class is very similar to class D, but now the degeneracy is in the 12 sector as

$$\begin{aligned} e_1^\downarrow &\rightarrow \cos \alpha e_1^\downarrow - \sin \alpha e_2^\downarrow, & e_2^\downarrow &\rightarrow \sin \alpha e_1^\downarrow + \cos \alpha e_2^\downarrow, & e_3^\downarrow &\rightarrow e_3^\downarrow, \\ \vec{n}_1 &\rightarrow \cos \alpha \vec{n}_1 - \sin \alpha \vec{n}_2, & \vec{n}_2 &\rightarrow \sin \alpha \vec{n}_1 + \cos \alpha \vec{n}_2, & \vec{n}_3 &\rightarrow \vec{n}_3. \end{aligned} \quad (2.42)$$

So we have

$$\begin{aligned} s^\downarrow &= e_1^\downarrow s_1 + e_3^\downarrow s_3, & \vec{t} &= t_1 \vec{n}_1 + t_2 \vec{n}_2 + t_3 \vec{n}_3, \\ \vec{C} &= \pm (e_1^\downarrow c_1 \vec{n}_1 + e_2^\downarrow c_1 \vec{n}_2 + e_3^\downarrow c_3 \vec{n}_3) \end{aligned}$$

$$\text{with } \left\{ \begin{array}{l} s_1 \geq 0 \text{ and } t_2 \geq 0 \\ \text{or} \\ s_1 = 0 \text{ and } t_1 \geq 0, t_2 = 0 \end{array} \right\} \text{ and } \left\{ \begin{array}{l} s_3 \geq 0 \\ \text{or} \\ s_3 = 0 \text{ and } t_3 \geq 0 \end{array} \right\}. \quad (2.43)$$

Here, too, each subclass is made up of seven-parametric sets of families.

Class F: The lack of degeneracy limits changes of the 123 bases to discrete 180° rotations as in (2.17) where the rotations are around the 3rd axes. The generic form is defined by the choice of 123 coordinates for which as many as possible of the coefficients $s_1, t_1, s_2, t_2, s_3, t_3$ are non-negative. Here we get, in each subclass, sets of families specified by the full number of nine parameters, of which five or more are non-negative.

Arbitrary local unitary transformations turn members of a family into other members of the same family. This, we recall, is the defining property of a family of locally equivalent states. Also there are some local transformation that have no effect at all, as exemplified by the local unitary transformation $\exp(i\phi\sigma_1 + i\psi\tau_1)$ acting on the class A state (2.37). If one just wants to check if two given states are locally equivalent, without identifying the family they belong to, one could evaluate Makhlin's 18 polynomial invariants [33], which are minimal in this respect; a general method for generating all polynomial invariants of any degree has been given by Grassl, Rötteler, and Beth [34].

As an example, the pure states are of the generic form (2.14). One verifies easily the purity condition

$$\rho_p (1 - \rho_p) = 0. \quad (2.44)$$

For $p = 0, q = 1$ we have the family of Bell states,

$$\rho_{\text{Bell}} = \frac{1}{4} (1 - \sigma_1\tau_1 - \sigma_2\tau_2 - \sigma_3\tau_3), \quad (2.45)$$

which is in class B; the $p = 1, q = 0$ family consists of the product states $[\frac{1}{2}(1 + \sigma_1)\frac{1}{2}(1 - \tau_1)]$ and is in class C; and the $0 < p < 1$ families belong to class D.

Chapter 3

Positivity and separability

In this chapter, the positivity and separability in the spirit of the Peres-Horodeccy criterion are investigated. A simple criterion for separability is obtained. The relation between the separability and the cross dyadic is introduced.

3.1 A separability criterion

An arbitrary choice for the nine family-defining parameters plus the 123 coordinate systems specifies a hermitian ρ of unit trace, but its positivity must be ensured by imposing restrictions on the Pauli vectors s^\downarrow , \vec{t} , and the cross dyadic \vec{C} . It is expedient to switch the emphasis from ρ to the traceless operator K introduced by

$$K = 1 - 4\rho = -\vec{\sigma} \cdot s^\downarrow - \vec{t} \cdot \tau^\downarrow - \vec{\sigma} \cdot \vec{C} \cdot \tau^\downarrow, \quad (3.1)$$

so that $\rho = \frac{1}{4}(1 - K) \geq 0$ requires

$$K \leq 1. \quad (3.2)$$

Convex sums of two states correspond to weighted sums of their K 's. Admixing ρ_{chaos} to a given ρ amounts to multiplying its K by a factor.

One could, of course, check the positivity criterion (3.2) by calculating the eigenvalues of K , possibly with the aid of the 4×4 -matrices (1.14) and (1.15). But precise knowledge of the actual eigenvalues of K is not needed if we only want to verify (3.2).

Since K is traceless, its eigenvalues κ_j ($j = 1, 2, 3, 4$) have a vanishing sum and solve a quartic equation without a cubic term,

$$\kappa^4 - A_2\kappa^2 + A_1\kappa - A_0 = 0, \quad (3.3)$$

where

$$\begin{aligned} A_2 &= \frac{1}{2}\text{tr} \{K^2\}, & A_1 &= -\frac{1}{3}\text{tr} \{K^3\}, \\ A_0 &= \frac{1}{4}\text{tr} \{K^4\} - \frac{1}{8}[\text{tr} \{K^2\}]^2. \end{aligned} \quad (3.4)$$

These three numbers are invariant under arbitrary (local or not) unitary transformations, they are three independent *global* invariants of the given ρ .

Upon establishing

$$\begin{aligned} K^2 &= \text{Sp}\left\{\overleftarrow{C}^T \cdot \overleftarrow{C}\right\} + \vec{s} \cdot s^\downarrow + \vec{t} \cdot t^\downarrow \\ &\quad + 2\vec{\sigma} \cdot \overleftarrow{C} \cdot t^\downarrow + 2\vec{s} \cdot \overleftarrow{C} \cdot \tau^\downarrow + 2\vec{\sigma} \cdot \left(s^\downarrow \vec{t} - \overleftarrow{C}_{\text{sub}}\right) \cdot \tau^\downarrow \end{aligned} \quad (3.5)$$

with the aid of (1.4) and (1.6), it is easy to evaluate the traces in (3.4) and express A_2 , A_1 , A_0 in terms of s^\downarrow , \vec{t} , and \overleftarrow{C} . Explicitly they read

$$\begin{aligned} A_2 &= 2\text{Sp}\left\{\overleftarrow{C}^T \cdot \overleftarrow{C}\right\} + 2\vec{s} \cdot s^\downarrow + 2\vec{t} \cdot t^\downarrow, \\ A_1 &= 8\vec{s} \cdot \overleftarrow{C} \cdot t^\downarrow - 8\det\left\{\overleftarrow{C}\right\}, \\ A_0 &= \left(\text{Sp}\left\{\overleftarrow{C}^T \cdot \overleftarrow{C}\right\}\right)^2 - 2\text{Sp}\left\{\left(\overleftarrow{C}^T \cdot \overleftarrow{C}\right)^2\right\} \\ &\quad - 2(\vec{s} \cdot s^\downarrow + \vec{t} \cdot t^\downarrow) \text{Sp}\left\{\overleftarrow{C}^T \cdot \overleftarrow{C}\right\} - (\vec{s} \cdot s^\downarrow - \vec{t} \cdot t^\downarrow)^2 \\ &\quad + 4\vec{s} \cdot \overleftarrow{C} \cdot \overleftarrow{C}^T \cdot s^\downarrow + 4\vec{t} \cdot \overleftarrow{C}^T \cdot \overleftarrow{C} \cdot t^\downarrow - 8\vec{s} \cdot \overleftarrow{C}_{\text{sub}} \cdot t^\downarrow, \end{aligned} \quad (3.6)$$

One can express those three numbers as a functions of the invariants $a_m^{(n)}$ in (2.9),

$$\begin{aligned} A_2 &= 2(a_1^{(2)} + a_2^{(2)} + a_3^{(2)}), \\ A_1 &= 8(a_2^{(3)} - a_1^{(3)}), \\ A_0 &= \left(a_1^{(2)}\right)^2 - 2a_1^{(2)} \left(a_2^{(2)} + a_2^{(3)}\right) - \left(a_2^{(2)} - a_3^{(2)}\right)^2 \\ &\quad - 2a_1^{(4)} - 8a_2^{(4)} + 4a_3^{(4)} + 4a_4^{(4)}. \end{aligned} \quad (3.7)$$

All solutions of the quartic equation (3.3) are real by construction — it is, after all, the characteristic polynomial of a hermitian operator. Then, if all solutions are in the range $\kappa \leq 1$, this polynomial and its derivatives must be non-negative for $\kappa \geq 1$. Consequently, the positivity requirement (3.2) implies

$$A_2 - A_1 + A_0 \leq 1, \quad 2A_2 - A_1 \leq 4, \quad A_2 \leq 6. \quad (3.8)$$

It is reasonably obvious, and can be demonstrated in a rather simple manner [19], that the converse is also true: If these three inequalities are obeyed, the four real solutions of (3.3) are in the range $\kappa \leq 1$, so that $K \leq 1$ and $\rho \geq 0$. In other words, the restrictions on s^\downarrow , \vec{t} , and \overleftarrow{C} alluded to at the beginning of this section are just the inequalities (3.8).

Correlations of a genuine quantum character require a non-separable state ρ . Peres [23] observed that the partial transposes of a separable ρ are non-negative, that they are 2-qubit states themselves, and his conjecture of the converse, namely

that ρ is separable if $\rho^{\text{T}_1} \geq 0$ was proven by M., P., and R. Horodecki [24]. This profound insight is the very important

Peres–Horodeccy criterion

A 2-qubit state ρ is separable if its partial transpose ρ^{T_1} is non-negative, and only then. (3.9)

As a matter of record we remark that Peres actually considered a partial transpose of the form $\rho \rightarrow \sigma_y \rho^{\text{T}_1} \sigma_y$ rather than $\rho \rightarrow \rho^{\text{T}_1}$. Inasmuch as the sandwiching by the two σ_y 's is a local unitary transformation, it is irrelevant for the separability criterion (3.9). Equivalently, one could single out the x or z components of $\vec{\sigma}$ or any other one, but $\rho \rightarrow \rho^{\text{T}_1}$, which treats all components on equal footing, has its obvious advantages.

To decide whether a given 2-qubit state is separable or not, we could calculate its Hill–Wootters concurrence or employ the Peres–Horodeccy criterion. The latter is easier to use in practice because the positivity of ρ^{T_1} , or

$$1 - 4\rho^{\text{T}_1} = K^{\text{T}_1} = \frac{1}{2} (\vec{\sigma} \cdot K\sigma^\perp - K) \leq 1, \quad (3.10)$$

can be checked analogously to the positivity of ρ . The quartic equation solved by the common eigenvalues of K^{T_1} and K^{T_2} is obtained from (3.3) by the replacements

$$A_1 \rightarrow A_1 + 16 \det \left\{ \overleftarrow{C} \right\}, \quad A_0 \rightarrow A_0 + 16 \vec{s} \cdot \overleftarrow{C}_{\text{sub}} \cdot t^\perp. \quad (3.11)$$

With the aid of the identity

$$\begin{aligned} \det \left\{ \overleftarrow{A} - \overleftarrow{B} \right\} &= \det \left\{ \overleftarrow{A} \right\} - \det \left\{ \overleftarrow{B} \right\} \\ &+ \text{Sp} \left\{ \overleftarrow{A}^{\text{T}} \cdot \overleftarrow{B}_{\text{sub}} \right\} - \text{Sp} \left\{ \overleftarrow{B}^{\text{T}} \cdot \overleftarrow{A}_{\text{sub}} \right\}, \end{aligned} \quad (3.12)$$

an implication of (1.6), here used for $\overleftarrow{A} = \overleftarrow{C}$ and $\overleftarrow{B} = s^\perp t$, we thus find that

$$A_2 - A_1 + A_0 \leq 1 + 16 \det \left\{ \overleftarrow{E} \right\}, \quad 2A_2 - A_1 \leq 4 + 16 \det \left\{ \overleftarrow{C} \right\} \quad (3.13)$$

are equivalent to (3.10); the third inequality, $A_2 \leq 6$, is always obeyed by a positive ρ . So, a non-separable state must violate either the first or the second inequality in (3.13), or both. The equal sign holds in the first inequality if the partial transposes of the given ρ have a zero eigenvalue; both are equalities, if they have two zero eigenvalues. Accordingly, the partial transposes of a non-separable ρ can at most have one zero eigenvalue and thus must be of rank 3 or 4 [29].

Thus the separability of a given ρ is checked as easily as its positivity. Neither test requires actual knowledge of the solutions of (3.3) or the quartic equation resulting from the replacements (3.11). They could, of course, be stated analytically but these explicit expressions are not very transparent unless special relations exist among the coefficients of the quartic equations.

As a simple application of the Peres–Horodeccy criterion, in the form of the inequalities (3.13), we note that a state ρ with $\det\{\overleftarrow{C}\} \geq 0$ and $\det\{\overleftarrow{E}\} \geq 0$ is surely separable. Therefore, for example, all states in classes A and C are separable.

3.2 Separability and the cross dyadic

It is known that the violation of the Bell’s inequalities [35], or of the more appropriate CHSH inequality, is an indication that the state ρ in question is not separable [36], but the converse is not true because there are non-separable states that obey the CHSH inequality [37]. Here the largest values of the characteristic values of the cross dyadic \overleftarrow{C} are employed to decide if the given state obeys or violates the CHSH inequality.

A measurement on one of the qubits determines the component of the spin vector along a chosen direction. The probability for finding the first qubit’s spin vector in the \vec{a} direction and the second qubit in \vec{b} direction are given by:

$$P_1(\vec{a}) = \frac{1}{2}(1 + \vec{a} \cdot \vec{s}^\downarrow), \quad P_2(\vec{b}) = \frac{1}{2}(1 + \vec{b} \cdot \vec{t}^\downarrow), \quad (3.14)$$

where \vec{a} and \vec{b} are unit vectors. The joint probability for finding the first qubit along \vec{a} and the second along \vec{b} is

$$P_{12}(\vec{a}, \vec{b}) = \frac{1}{4}(1 + \vec{a} \cdot \vec{s}^\downarrow + \vec{b} \cdot \vec{t}^\downarrow + \vec{a} \cdot \overleftarrow{C} \cdot \vec{b}^\downarrow). \quad (3.15)$$

Using (3.15), one can rewrite $P_1(\vec{a})$ and $P_2(\vec{b})$ as

$$\begin{aligned} P_1(\vec{a}) &= P_{12}(\vec{a}, \vec{b}) + P_{12}(\vec{a}, -\vec{b}), \\ P_2(\vec{b}) &= P_{12}(\vec{a}, \vec{b}) + P_{12}(-\vec{a}, \vec{b}). \end{aligned} \quad (3.16)$$

The difference between the joint probability $P_{12}(\vec{a}, \vec{b})$ and the product of the individual probabilities $P_1(\vec{a})$ and $P_1(\vec{b})$, involves the entanglement dyadic \overleftarrow{E}

$$P_{12}(\vec{a}, \vec{b}) - P_1(\vec{a})P_2(\vec{b}) = \frac{1}{4}\vec{a} \cdot \overleftarrow{E} \cdot \vec{b}^\downarrow \quad (3.17)$$

Now, the CHSH inequality [35, 38, 39, 40] is

$$-1 \leq P_{12}(\vec{a}_1, \vec{b}_1) - P_{12}(\vec{a}_1, \vec{b}_2) + P_{12}(\vec{a}_2, \vec{b}_1) + P_{12}(\vec{a}_2, \vec{b}_2) - P_1(\vec{a}_2) - P_2(\vec{b}_1) \leq 0. \quad (3.18)$$

Using (3.15), (3.16) one obtains CHSH inequality in terms of the cross dyadic \overleftarrow{C}

$$-2 \leq \vec{a}_1 \cdot \overleftarrow{C} \cdot \vec{b}_1^\downarrow - \vec{a}_1 \cdot \overleftarrow{C} \cdot \vec{b}_2^\downarrow + \vec{a}_2 \cdot \overleftarrow{C} \cdot \vec{b}_1^\downarrow + \vec{a}_2 \cdot \overleftarrow{C} \cdot \vec{b}_2^\downarrow \leq 2. \quad (3.19)$$

In view of what is said at (1.26), one observes that the two largest characteristic values of the cross dyadic \overleftarrow{C} decide whether the CHSH inequality is obeyed or not,

$$\text{CHSH is } \begin{cases} \text{obeyed if } c_1^2 + c_2^2 \leq 1, \\ \text{violated if } c_1^2 + c_2^2 > 1. \end{cases} \quad (3.20)$$

There is another important application of the characteristic values for the cross dyadic in the field of quantum purification and teleportation. According to the proposition 1 in [24], any mixed spin- $\frac{1}{2}$ state is useful for teleportation iff $\text{Sp} \left\{ |\overleftarrow{C}| \right\} > 1$. Bennett *et.al* [14] have introduced a purification protocol known as IBM or BBPSSW protocol. It produces Bell states from mixed states. The value of $\text{Sp} \left\{ |\overleftarrow{C}| \right\}$ determines if the given states could be purified or not. It is possible if $\text{Sp} \left\{ |\overleftarrow{C}| \right\} > 1$. For $\text{Sp} \left\{ |\overleftarrow{C}| \right\} \leq 1$, however, the BBPSSW protocol does not work.

3.3 Examples

1. Let us consider the simple Werner state [41], which could be written as

$$\rho_w = \frac{1}{4}(1 - x\vec{\sigma} \cdot \overleftarrow{O}_{en} \cdot \tau^\downarrow). \quad (3.21)$$

By using (3.6), the three numbers A_2, A_1 , and A_0 are,

$$A_2 = 6x^2, \quad A_1 = -8x^3, \quad A_0 = 3x^4, \quad \det \left\{ \overleftarrow{C} \right\} = \det \left\{ \overleftarrow{E} \right\} = -x^3. \quad (3.22)$$

The separability inequalities (3.13) are fulfilled for $x \in [-\frac{1}{3}, \frac{1}{3}]$. This means that the state (3.21), is non-separable if $\frac{1}{3} < x \leq 1$. Note that a violation of the CHSH inequality would require $x > 1/\sqrt{2}$, so that Werner states with $\frac{1}{3} < x \leq 1/\sqrt{2}$ are not separable and obey the CHSH inequality.

2. Consider the generic pure state (2.14). In this case,

$$A_2 = 6, \quad A_1 = 8, \quad A_0 = 3, \quad \det \left\{ \overleftarrow{C} \right\} = -q^2, \quad \text{and} \quad \det \left\{ \overleftarrow{E} \right\} = -(pq)^2. \quad (3.23)$$

The conditions of separability (3.6) show that the state (2.14) is separable for $p = 1$. Also, this arbitrary projector obeys the CHSH inequality only for $p = 1$ and violates it for any other values.

Chapter 4

Lewenstein-Sanpera Decompositions

According to the findings of Lewenstein and Sanpera [42], any 2-qubit state ρ can be written as a mixture of a separable state ρ_s and a non-separable pure state ρ_p ,

$$\rho = \lambda\rho_s + (1 - \lambda)\rho_p \quad \text{with } 0 \leq \lambda \leq 1. \quad (4.1)$$

Rare exceptions aside, the *Lewenstein-Sanpera decomposition* (LSD) of a given (non-separable) ρ is not unique, there is usually a continuum of LSDs to choose from. Among them is the *optimal LSD*, the one with the largest value of λ ,

$$\rho = \mathcal{S}\rho_s + (1 - \mathcal{S})\rho_p \quad \text{with } \mathcal{S} = \max\{\lambda\}. \quad (4.2)$$

The number \mathcal{S} measures to which extent the correlations associated with ρ are classical; in rough terms, a state ρ is the more useful for quantum communication purposes, the smaller its degree of separability. Therefore, we would like to express \mathcal{S} and ρ in terms of the Pauli vectors \vec{s} , t^\dagger and the cross dyadic \overline{C} that specify the state ρ . We are still searching for the general answer, but for a number of important special cases the problem is solved already. Whereas it is relatively easy to find LSDs for a given state ρ , it is usually rather difficult to check whether a certain decomposition is the optimal one. Just like its concurrence, the degree of separability is not an individual property of a 2-qubit state. It is a family property, locally equivalent states have the same value of \mathcal{S} . Here, then, is the challenge:

$$\text{Find an analytical method that determines the optimal LSD of any given 2-qubit state } \rho. \quad (4.3)$$

By “analytical” we mean that the answer is surely known after a finite number of steps. There is, of course, the option of using iterative methods which produce a series of LSDs that converge toward the optimal LSD. Such methods are not regarded as analytical, unless they assuredly give the answer after a finite number

of iterations. Incidentally, the first ρ considered by Lewenstein and Sanpera as an illustrating example [42], one for which the optimal LSD is now known analytically [19], was then decomposed by a numerical iteration of the non-analytical kind.

The complete solution of this problem is not known as yet. But there has been considerable progress, and the optimal LSDs are known for a variety of 2-qubit states. Before turning to these matters in detail, let us offer a few general remarks.

The mapping $\rho \rightarrow \mathcal{S}$ is concave,

$$\mathcal{S}(x\rho_1 + (1-x)\rho_2) \geq x\mathcal{S}(\rho_1) + (1-x)\mathcal{S}(\rho_2) \quad \text{for } 0 \leq x \leq 1. \quad (4.4)$$

Unless $x = 0$ or $x = 1$, the equal sign only holds if the same pure state shows up in the optimal LSDs of both ρ_1 and ρ_2 . Otherwise the convex sum of the two ρ 's is a rank-2 state that has LSDs of its own and a non-zero degree of separability.

In the Introduction, we introduced a quantity called *concurrence*, for a two qubit state it is given by (1.23). To evaluate this value, Hill and Wootters [21], considered the transformation (1.20). One can notice that the replacement $(s^\downarrow, \vec{t}, \vec{C}) \rightarrow (-s^\downarrow, -\vec{t}, \vec{C})$ has no effect on the invariants A_2, A_1, A_0 of (3.7), thus ρ^\top has the same eigenvalues as ρ , therefore ρ^\top is unitarily equivalent to ρ . On the other hand the quantity $\mathcal{C} \in [0, 1]$, so that one can look at the concurrence \mathcal{C} as a measure of entanglement. For separable states, one has $\lambda_{\max} = 1$ and $\mathcal{C} = 0$, and for the non-separable states, $\mathcal{S} < 1$ and $\mathcal{C} > 0$. This suggests that there might be a close relation between the degree of separability and the concurrence. Since the concurrence of a separable state vanishes, applying the convexity property (1.25) to (4.2) implies

$$\mathcal{C} \leq (1 - \mathcal{S})q \leq 1 - \mathcal{S}, \quad (4.5)$$

where \mathcal{C} and q are the concurrences of ρ and ϱ , respectively. The concurrence of a 2-qubit state thus sets an upper bound on its degree of separability. Eisert and Briegel [50] have observed that \mathcal{S} is a separability monotone. Also as is noted by Wellens and Kuś, Karnas and Lewenstein [49], the product $(1 - \mathcal{S})q$ possesses the most crucial ones of the properties that Vedral *et.al.* [51, 52] require from a good entanglement measure.

The spectral decomposition of the partial transpose of a pure state (2.14) is of the generic form (2.20). Therefore, the partial transpose of any 2-qubit state ρ can be written as

$$\rho^{\top_1} = (1+x)\rho' - x\rho_{\text{Bell}}, \quad 0 \leq x \leq \frac{1}{2}(1 - \mathcal{S}) \quad (4.6)$$

with some state ρ' and a Bell state ρ_{Bell} . As a consequence, ρ^{\top_1} and ρ^{\top_2} can have at most one negative eigenvalue.

Since ρ' is a mixture of four or fewer pure states (4.6) shows that the partial transpose of a non-separable state is a pseudo-mixture of up to five pure states

with one negative weight only, carried by a Bell state. There is a very similar observation by Sanpera *et al.* [29] about ρ itself: It can always be presented as a pseudo-mixture of four or five separable pure states; as an immediate consequence its partial transpose is also such a pseudo-mixture.

4.1 Basic properties of optimal LSDs

The optimal LSD (4.2) has a number of properties that help in decomposing given states in the optimal way. Here are some particularly important ones:

Existence: The degree of separability \mathcal{S} is really the maximum of all possible λ values in (4.1), not just their supremum, because the subset of separable states is compact. Therefore, a LSD with $\lambda = \mathcal{S}$ does exist.

Uniqueness: It is clear that the LSD is not unique, there is usually a continuum of LSDs to choose from, among them one of the optimal LSD (4.2), the one with the largest value of λ . To show the uniqueness of the optimal LSD, assume that we have a two different LSD's with the same nonzero λ ,

$$\rho = \lambda\rho_s^{(1)} + (1 - \lambda)\rho_p^{(1)} = \lambda\rho_s^{(2)} + (1 - \lambda)\rho_p^{(2)}. \quad (4.7)$$

The symmetric convex sum of the two LSDs is also equal to the given ρ . It contains the convex sum of the two different ρ_s 's which is separable, and the convex sum of the two pure ρ_p states, which has a LSD of its own,

$$\rho = \frac{\lambda}{2}(\rho_s^{(1)} + \rho_s^{(2)}) + \frac{1 - \lambda}{2}(\rho_p^{(1)} + \rho_p^{(2)}). \quad (4.8)$$

Another time one splits $\frac{1}{2}(\rho_p^{(1)} + \rho_p^{(2)})$ to its pure and separable parts as

$$\frac{1}{2}(\rho_p^{(1)} + \rho_p^{(2)}) = \lambda^{(12)}\rho_s^{(12)} + (1 - \lambda^{(12)})\rho_p^{(12)}. \quad (4.9)$$

Finally, the density operator ρ could be written as

$$\rho = \lambda^{\text{new}}\rho_s^{\text{new}} + (1 - \lambda^{\text{new}})\rho_p^{\text{new}}, \quad (4.10)$$

with

$$\begin{aligned} \lambda^{\text{new}} &= \lambda + \lambda^{(12)} - \lambda\lambda^{(12)}, \\ \rho_s^{\text{new}} &= \frac{1}{\lambda^{\text{new}}} \left[\frac{\lambda}{2}(\rho_s^{(1)} + \rho_s^{(12)}) + (1 - \lambda)\lambda^{(12)}\rho_p^{(12)} \right], \\ \rho_p^{\text{new}} &= \rho_p^{(12)}. \end{aligned} \quad (4.11)$$

So, we obtain a new LSD of ρ with a larger λ value, consequently the common λ of the original two LSDs is not maximal. As a formal statement we thus note that

$$\begin{aligned} \varrho_s + (1/\mathcal{S} - 1)(\varrho - \rho_p) \\ \text{is either non-positive or non-separable for} \\ \text{each } \rho_p \neq \varrho. \end{aligned} \quad (4.12)$$

This does not imply that one can always find another LSD with the same λ value if $\lambda < \mathcal{S}$. There are states with a continuum of LSDs in which each value of λ occurs only once. Examples are the rank-2 states (4.91) that obey inequality (4.108) below.

ϱ_s is barely separable: Consider the optimal LSD of some non-separable state ρ and a parameter ϵ in the range of $0 < \epsilon \leq 1 - \mathcal{S}$ then,

$$\rho = (\mathcal{S} + \epsilon) \left[\frac{\mathcal{S}}{\mathcal{S} + \epsilon} \varrho_s + \frac{\epsilon}{\mathcal{S} + \epsilon} \varrho \right] + (1 - \mathcal{S} - \epsilon) \varrho. \quad (4.13)$$

It is clear that the convex sum in the square brackets is surely non-negative, but it cannot be separable, because if it were separable, then we would have found a LSD with $\lambda > \mathcal{S}$. Therefore,

$$\begin{aligned} &\text{the state } \rho_\epsilon = (1 + \epsilon)^{-1}(\varrho_s + \epsilon\varrho) \\ &\text{is non-separable for } \epsilon > 0. \end{aligned} \quad (4.14)$$

Thus, $\rho_\epsilon^{\text{T}_1}$ has a negative eigenvalue for $\epsilon > 0$, but none for $\epsilon = 0$. Since the eigenvalues are continuous functions of ϵ , it follows that $\varrho_s^{\text{T}_1}$ and $\varrho_s^{\text{T}_2}$ must have at least one zero eigenvalue. Formally,

$$\varrho_s^{\text{T}_1}, \varrho_s^{\text{T}_2} \geq 0 \quad \text{but not} \quad \varrho_s^{\text{T}_1}, \varrho_s^{\text{T}_2} > 0; \quad (4.15)$$

for ϱ_s , the equal sign holds in the first inequality of (3.13). A useful terminology calls ϱ_s *barely separable* with respect to ϱ .

When searching for the optimal LSD of a given ρ it is, therefore, sufficient to consider LSDs with ρ_s 's that are barely separable with respect to the ρ_p with which they are paired in (4.1). If the ρ_s of some LSD does not have this property, one adds the appropriate amount of the respective ρ_p to it (in the sense of a convex sum, of course) and gets a barely separable ρ_s .

Pairing property: Since the infinitesimal neighbourhoods of ϱ_s and ϱ are critical in (4.12) and (4.14), the actual value of \mathcal{S} is irrelevant and, as a consequence, we note the *pairing property*:

$$\begin{aligned} &\text{If } \rho_\lambda = \lambda\rho_s + (1 - \lambda)\rho_p \text{ is the optimal LSD for} \\ &\text{one value of } \lambda \text{ in the range } 0 < \lambda < 1, \text{ then it is} \\ &\text{optimal also for all other } \lambda \text{ values.} \end{aligned} \quad (4.16)$$

It is also implied by the concavity (4.4). Obviously, a systematic method for identifying all ρ_s 's that pair with a given ρ_p , or vice versa, would be quite helpful, but we are not aware of one.

Local invariance is passed on: Suppose that the given ρ is invariant under some local unitary transformation, i.e.

$$U_{\text{loc}}^\dagger \rho U_{\text{loc}} = \rho. \quad (4.17)$$

Then its ϱ_s and ϱ must be invariant under this local transformation as well, otherwise we could apply it to the optimal LSD and get another LSD with the same value λ , in conflict with the uniqueness of the optimal LSD. This argument builds on the elementary observation that local transformations do not affect the purity and separability of a state. The limitations resulting from this “inheritance of local invariance” can facilitate the search for the optimal LSD substantially. The optimal decompositions of some states were found this way.

Swapping invariance is passed on: Similarly one finds that ϱ_s and ϱ of ρ that is invariant under the swapping transformation

$$\sigma_k \leftrightarrow \tau_k \quad \text{for } k = 1, 2, 3 \quad (4.18)$$

or, more generally,

$$\sigma^\downarrow \rightarrow \vec{O}_{en} \cdot \tau^\downarrow, \quad \vec{\tau} \rightarrow \vec{\sigma} \cdot \vec{O}_{en} \quad (4.19)$$

must be invariant themselves because swapping does not affect the separability or the purity of a state. Clearly this swapping invariance is only possible if the Pauli vectors s^\downarrow and \vec{t} are of equal length.

Orthogonality is passed on: If the state ρ in question is orthogonal to a certain other state ρ_\perp , i.e $\text{tr} \{\rho\rho_\perp\} = 0$, then the ρ_s 's and ρ_p 's of all LSD's of ρ are also orthogonal to ρ_\perp because both traces in

$$0 = \lambda \text{tr} \{\rho_s \rho_\perp\} + (1 - \lambda) \text{tr} \{\rho_p \rho_\perp\} \quad (4.20)$$

must be non-negative, so both must vanish. In particular, the ϱ_s and ϱ of ρ must have this orthogonality property.

No locally optimal LSDs: Suppose that $\rho = \lambda\rho_s + (1 - \lambda)\rho_p$ is a non-optimal LSD of ρ . Then, if ρ_s is *not* barely separable with respect to ρ_p , there is a range of positive ϵ values such that $\lambda \rightarrow (1 + \epsilon)\lambda$ and $\rho_s \rightarrow (1 + \epsilon)^{-1}(\rho_s + \epsilon\rho_p)$ specify other LSDs with a continuum of larger λ values. If, however, ρ_s is barely separable with respect to ρ_p , then $\rho_p \neq \varrho$ and the convex sums of the optimal LSD and the non-optimal LSD give further, different LSDs upon decomposing the rank-2 state formed by the convex sum of ϱ and ρ_p . In all of these new LSDs, the separable parts carry weights that are larger than λ and less than \mathcal{S} . Therefore, the given non-optimal LSD is not only globally non-optimal, it is also locally non-optimal. There must be neighbouring LSDs with larger λ values.

4.2 Optimal LSDs of truly positive states

Since any state ρ can be regarded as the $0 < x \rightarrow 0$ limit of the rank-4 states $x\rho_{\text{chaos}} + (1 - x)\rho$, the generic situation is that of $\rho > 0$, rather than $\rho \geq 0$, as it is the case for the rank-2 states in Section 4.3.3 or the rank-3 states in Section 4.3.5. Accordingly, we shall assume throughout this Section that $\rho > 0$. The

following results are excerpts from recent work by Karnas and Lewenstein [43] and, in particular, by Wellens and Kuś [44].

So we consider a non-separable ρ of rank 4. The separable state ϱ_s of its optimal LSD is then either of rank 3 or rank 4, and its partial transposes $\varrho_s^{\text{T}_1}$, $\varrho_s^{\text{T}_2}$ are of rank 3, as follows from (4.15). The unique pure states ρ_1 and ρ_2 that are associated with the non-degenerate null eigenvalue of $\varrho_s^{\text{T}_1}$ and $\varrho_s^{\text{T}_2}$, respectively,

$$\varrho_s^{\text{T}_1} \rho_1 = \rho_1 \varrho_s^{\text{T}_1} = 0, \quad \varrho_s^{\text{T}_2} \rho_2 = \rho_2 \varrho_s^{\text{T}_2} = 0, \quad (4.21)$$

are related to each other by transposition,

$$\rho_1^\text{T} = \rho_2, \quad \rho_2^\text{T} = \rho_1, \quad \rho_1^{\text{T}_1} = \rho_2^{\text{T}_2}. \quad (4.22)$$

Now, for $\epsilon > 0$, the ‘‘barely separable’’ condition (4.14) requires the existence of a pure state $\rho_{\text{pure}}^{(\epsilon)}$ such that

$$\text{tr} \{ (\varrho_s + \epsilon \varrho)^{\text{T}_1} \rho_{\text{pure}}^{(\epsilon)} \} < 0, \quad (4.23)$$

and since the eigenvalues and eigenstates of $(\varrho_s + \epsilon \varrho)^{\text{T}_1}$ depend continuously on ϵ , we have $\rho_{\text{pure}}^{(\epsilon)} \rightarrow \rho_1$ as $\epsilon \rightarrow 0$ and get

$$\text{tr} \{ \varrho^{\text{T}_1} \rho_1 \} \leq 0 \quad \text{or} \quad \text{tr} \{ \varrho \rho_1^{\text{T}_1} \} = \text{tr} \{ \varrho \rho_2^{\text{T}_2} \} \leq 0 \quad (4.24)$$

in this limit.

Next, we exploit the uniqueness condition (4.12) where we put

$$\Delta_\epsilon \rho = \varrho - \rho_{\text{pure}} = \varrho - e^{-i\epsilon G} \varrho e^{i\epsilon G} = i\epsilon [G, \varrho] + O(\epsilon^2) \quad (4.25)$$

with a hermitian generator G that does not commute with ϱ . Then, for $\epsilon \neq 0$, there exists either a pure state $\rho_{\text{pure}}^{(\epsilon)}$ such that

$$\text{tr} \{ [\varrho_s + (1/\mathcal{S} - 1)\Delta_\epsilon \rho] \rho_{\text{pure}}^{(\epsilon)} \} < 0 \quad (4.26)$$

or a pure state $\bar{\rho}_{\text{pure}}^{(\epsilon)}$ such that

$$\text{tr} \left\{ [\varrho_s + (1/\mathcal{S} - 1)\Delta_\epsilon \rho]^{\text{T}_1} \bar{\rho}_{\text{pure}}^{(\epsilon)} \right\} < 0. \quad (4.27)$$

In the limit $\epsilon \rightarrow 0$, the positivity violation (4.26) can only occur if ϱ_s is of rank 3.

4.2.1 The separable part has full rank

Let us, therefore, first deal with the situation in which ϱ_s has full rank, $\varrho_s > 0$, so that the separability violation (4.27) must be the case. Here, too, the eigenvalues and eigenstates of $[\dots]^{\text{T}_1}$ depend continuously on ϵ , and $\bar{\rho}_{\text{pure}}^{(\epsilon)} \rightarrow \rho_1$ obtains as

$\epsilon \rightarrow 0$. But, in marked contrast to the reasoning that took us from (4.23) to (4.24), ϵ is not restricted to positive values here (alternatively, if G is a permissible generator, so is $-G$), and so we get

$$\operatorname{tr} \left\{ i[G, \varrho]^{\text{T}_1} \rho_1 \right\} = 0 \quad \text{or} \quad \operatorname{tr} \left\{ [\rho_1^{\text{T}_1}, \varrho] G \right\} = 0. \quad (4.28)$$

This must hold for all G 's that do not commute with ϱ , and since it's always true for those that do, it must in fact hold for all hermitian G 's. Therefore, ϱ commutes with $\rho_1^{\text{T}_1}$, it is an eigenstate of $\rho_1^{\text{T}_1} = \rho_2^{\text{T}_2}$,

$$\rho_1^{\text{T}_1} \varrho = \varrho \rho_1^{\text{T}_1} = -\frac{1}{2} \bar{q} \varrho \quad \text{with} \quad \bar{q} = \sqrt{\operatorname{tr} \left\{ \rho_1^{\text{T}_1} \rho_1 \right\}} = \sqrt{\operatorname{tr} \left\{ \rho_1 \rho_2 \right\}}. \quad (4.29)$$

That the eigenvalue is related in this way to the concurrence \bar{q} of the family of pure states to which ρ_1 and ρ_2 belong, follows from (2.20) in conjunction with (4.24).

Taking the trace in (4.21), $\operatorname{tr} \left\{ \varrho_s^{\text{T}_1} \rho_1 \right\} = \operatorname{tr} \left\{ \varrho_s \rho_1^{\text{T}_1} \right\} = 0$, tells us that $\rho_1^{\text{T}_1} \not\propto 0$, since $\varrho_s > 0$. Accordingly, $\bar{q} > 0$ and ϱ is the Bell state $\rho_p^{(4)}$ that (2.20) and (2.21) associate with ρ_1 , and

$$\operatorname{tr} \left\{ \rho_1 \varrho \right\} = \frac{1}{2} (1 + \bar{q}), \quad \varrho^{\text{T}_1} = \varrho^{\text{T}_2} = \frac{1}{2} - \varrho \quad (4.30)$$

follow immediately. Then, partially transposing the optimal LSD of ρ establishes

$$\rho^{\text{T}_1} = \mathcal{S} \varrho_s^{\text{T}_1} - (1 - \mathcal{S}) \varrho + \frac{1}{2} (1 - \mathcal{S}), \quad (4.31)$$

so that

$$\operatorname{tr} \left\{ \rho^{\text{T}_1} \rho_p \right\} \geq \frac{1}{2} (1 - \mathcal{S}) - (1 - \mathcal{S}) \operatorname{tr} \left\{ \varrho \rho_p \right\} \quad (4.32)$$

for all pure states ρ_p , with the equal sign holding only for $\rho_p = \rho_1$, and since ϱ is a Bell state, (2.23) implies

$$\begin{aligned} \operatorname{tr} \left\{ \rho^{\text{T}_1} \rho_p \right\} &\geq -\frac{1}{2} (1 - \mathcal{S}) \sqrt{\operatorname{tr} \left\{ \rho_p^{\text{T}_1} \rho_p \right\}} \\ &\text{with “=” only for } \rho_p = \rho_1 = \rho_2^{\text{T}_1}. \end{aligned} \quad (4.33)$$

Accordingly, for $\rho_p = e^{i\epsilon G} \rho_1 e^{-i\epsilon G}$ with any hermitian generator G , the first-order terms must take care of each other, so that

$$\operatorname{tr} \left\{ \rho^{\text{T}_1} i[G, \rho_1] \right\} = -\frac{1 - \mathcal{S}}{2\bar{q}} \operatorname{tr} \left\{ \rho_2 i[G, \rho_1] \right\} \quad (4.34)$$

for all G , and therefore ρ_1 is an eigenstate of $\rho^{\text{T}_1} + (2\bar{q})^{-1} (1 - \mathcal{S}) \rho_2$,

$$\left(\rho^{\text{T}_1} + \frac{1 - \mathcal{S}}{2\bar{q}} \rho_2 \right) \rho_1 = 0. \quad (4.35)$$

That the eigenvalue is 0 follows from the vanishing trace of the left-hand side as required by the “=” case of (4.33). Equally well, we could have employed partial transposition of the second qubit in this line of reasoning, so that

$$\left(\rho^{\text{T}_2} + \frac{1 - \mathcal{S}}{2\bar{q}}\rho_1\right)\rho_2 = 0 \quad (4.36)$$

must hold as well. Indeed, total transposition turns one of the equations into the other. Jointly they state

$$\rho^{\text{T}_2}\rho^{\text{T}_1}\rho_1 = \frac{1}{4}(1 - \mathcal{S})^2\rho_1 \quad \text{or} \quad \rho^{\text{T}_1}\rho^{\text{T}_2}\rho_2 = \frac{1}{4}(1 - \mathcal{S})^2\rho_2, \quad (4.37)$$

where $\rho_1\rho_2\rho_1 = \bar{q}^2\rho_1$ and $\rho_2\rho_1\rho_2 = \bar{q}^2\rho_2$ have entered.

In summary, then, the problem of finding the optimal LSD of a given rank-4 ρ is reduced to solving (either one of) these eigenstate equations, because as soon as $\rho_1 = \rho_2^{\text{T}}$ is known, the pure state ϱ of the optimal LSD is available. Further we note that $\frac{1}{4}(1 - \mathcal{S})^2$ is the smallest eigenvalue of $\rho^{\text{T}_1}\rho^{\text{T}_2}$ and that $1 - \mathcal{S} = \mathcal{C}$ relates it to \mathcal{C} , the concurrence of ρ [which is to say that here both “=” signs hold in (4.5)]; see [44] for the technical details justifying these two assertions.

To complete the argument, we must convince ourselves that (4.37) in conjunction with (4.30) et cetera are not only necessarily obeyed by the ingredients of the optimal LSD, but are indeed sufficient to determine it. Suppose, then, that we have solved these equations and thus identified ϱ_s , ϱ , and \mathcal{S} , and assume that there is another LSD with $\lambda = \mathcal{S} + \epsilon > \mathcal{S}$. So, the first decomposition in

$$\rho = \mathcal{S}\varrho_s + (1 - \mathcal{S})\varrho = (\mathcal{S} + \epsilon)\rho_s^{(\epsilon)} + (1 - \mathcal{S} - \epsilon)\rho_p^{(\epsilon)} \quad (4.38)$$

is obtained from (4.37) and (4.30), and the second is better ($\epsilon > 0$) by assumption. Since there are no locally optimal LSDs, there must then be a continuum of “better” LSDs, such that $\rho_s^{(\epsilon)} \rightarrow \varrho_s$ and $\rho_p^{(\epsilon)} \rightarrow \varrho$ as $\epsilon \rightarrow 0$. Upon setting

$$\rho_p^{(\epsilon)} = \varrho + i\epsilon[\varrho, G] + O(\epsilon^2) \quad (4.39)$$

with some hermitian generator G and recalling (4.21), (4.28), and (4.30), we conclude that

$$\begin{aligned} & (\mathcal{S} + \epsilon) \text{tr} \left\{ \rho_s^{(\epsilon)\text{T}_1} \rho_1 \right\} \\ &= \mathcal{S} \text{tr} \left\{ \varrho_s^{\text{T}_1} \rho_1 \right\} + \epsilon \text{tr} \left\{ \varrho^{\text{T}_1} \rho_1 \right\} - (1 - \mathcal{S})\epsilon \text{tr} \left\{ i[\varrho, G]^{\text{T}_1} \rho_1 \right\} + O(\epsilon^2) \\ &= -\frac{1}{2}\epsilon\bar{q} + O(\epsilon^2). \end{aligned} \quad (4.40)$$

But $\bar{q} > 0$, so that this right-hand side is negative for sufficiently small positive ϵ values. Accordingly, $\rho_s^{(\epsilon)}$ is not separable after all, and we arrive at a contradiction.

All of this is, however, only true if the separable remainder ϱ_s of the optimal LSD is of rank 4, about which one has no prior knowledge. Nevertheless, we can accept $\varrho_s > 0$ as a working hypothesis, determine ϱ in accordance with (4.29), and then check whether the resulting $\varrho_s = \mathcal{S}^{-1}[\rho - (1 - \mathcal{S})\varrho]$ is truly positive and separable. If it is, we have found the optimal LSD with ϱ_s of full rank and ϱ a Bell state. Otherwise, we learn that the actual ϱ_s is of rank 3.

4.2.2 The separable part has reduced rank

In this case, there is a pure state ρ_0 associated with the null eigenvalue of ϱ_s ,

$$\varrho_s \rho_0 = \rho_0 \varrho_s = 0 . \quad (4.41)$$

But ρ_0 is not orthogonal to ϱ ,

$$\text{tr} \{ \varrho \rho_0 \} > 0 , \quad (4.42)$$

because ρ is of rank 4.

In the limit $\epsilon \rightarrow 0$, we must have $\rho_{\text{pure}}^{(\epsilon)} \rightarrow \rho_0$ in the positivity criterion (4.26) and, as before, $\bar{\rho}_{\text{pure}}^{(\epsilon)} \rightarrow \rho_1$ in the separability criterion (4.27). Looking at the terms linear in ϵ , we find that

$$\begin{aligned} \text{either (i) } & \text{tr} \{ i [G, \varrho] \rho_0 \} \geq 0 \quad \text{and} \quad \text{tr} \{ i [G, \varrho]^{\text{T}_1} \rho_1 \} \leq 0 \\ \text{or (ii) } & \text{tr} \{ i [G, \varrho] \rho_0 \} \leq 0 \quad \text{and} \quad \text{tr} \{ i [G, \varrho]^{\text{T}_1} \rho_1 \} \geq 0 \end{aligned} \quad (4.43)$$

must be the case. There is no other possibility: if, for instance, both traces were negative, so that $\epsilon > 0$ would be all right with the generator G considered, then $\epsilon \rightarrow -\epsilon$ (or, equivalently, $G \rightarrow -G$) would lead to the contradictory situation in which neither (4.26) nor (4.27) holds.

Again, any hermitian G is permitted in (4.43), which implies

$$[\rho_1^{\text{T}_1}, \varrho] = -y [\rho_0, \varrho] \quad \text{with} \quad y \geq 0 . \quad (4.44)$$

We conclude that ϱ is an eigenvalue of $\rho_1^{\text{T}_1} + y\rho_0 = \rho_2^{\text{T}_2} + y\rho_0$,

$$(\rho_1^{\text{T}_1} + y\rho_0) \varrho = -\mu \varrho , \quad (4.45)$$

which turns into (4.29) for $y = 0$, $\mu = \frac{1}{2}\bar{q}$. This feeds the expectation that $\mu \geq 0$, and this is indeed the case, as Wellens and Kuš have shown [44] with a continuity argument that exploits the known optimal LSD of a state of the form (4.63) [19] and an observation by Karnas and Lewenstein [43], namely that there is a pure product state orthogonal to ρ_0 with its partial transpose orthogonal to ρ_1 (or ρ_2 if the second qubit is transposed).

As it stands, the eigenstate equation (4.45) is of little use because it involves ρ_0 , which is unknown as yet. We determine it with an argument from the Lewenstein–Sanpera paper [42]. For any positive operator A , we note this application of the Cauchy–Schwarz inequality (actually a particular case of a more general statement):

$$\text{tr} \{ A \varrho \} = \text{tr} \{ (\rho^{\frac{1}{2}} A \rho^{\frac{1}{2}}) (\rho^{-\frac{1}{2}} \varrho \rho^{-\frac{1}{2}}) \} \leq \text{tr} \{ A \rho \} \text{tr} \{ \rho^{-1} \varrho \} , \quad (4.46)$$

or

$$\begin{aligned} \text{tr}\{(\text{tr}\{\rho^{-1}\varrho\}\rho - \varrho)A\} &\geq 0 \\ \text{with “=” only for } A &\propto \rho^{-1}\varrho\rho^{-1}, \end{aligned} \quad (4.47)$$

so that $\text{tr}\{\rho^{-1}\varrho\}\rho - \varrho$ is a positive operator of rank 3. This operator is a linear combination of ϱ_s and ϱ and, as a consequence of (4.42), it must be just a multiple of ϱ_s because if it had a non-zero contribution from ϱ it would be either non-positive or of rank 4. Consistency then requires that

$$\text{tr}\{\rho^{-1}\varrho\}(1 - \mathcal{S}) = 1, \quad (4.48)$$

and the “=” case of (4.47) tells us that

$$\rho_0 = \frac{\rho^{-1}\varrho\rho^{-1}}{\text{tr}\{\rho^{-2}\varrho\}}. \quad (4.49)$$

So, with $y = \nu \text{tr}\{\rho^{-2}\varrho\}(1 - \mathcal{S})$, the eigenstate equation (4.45) becomes

$$(\rho_1^{\text{T}_1} + \nu\rho^{-1})\varrho = -\mu\varrho. \quad (4.50)$$

We supplement it with the eigenstate equation for ρ_1 ,

$$(\text{tr}\{\rho^{-1}\varrho\}\rho - \varrho)^{\text{T}_1}\rho_1 = 0, \quad (4.51)$$

which is (4.21) after expressing ϱ_s in terms of ρ and ϱ with the aid of (4.48) and (4.1). The equation pair (4.50), (4.51) determines ϱ and ρ_1 for the given ρ . As Wellens and Kuś remark, there may be several solutions, but there is only one with $\mu, \nu \geq 0$ that gives a positive and separable ϱ_s ; see [44] for the technical details justifying this uniqueness assertion.

Here, too, one can show that these equations are not only necessary but sufficient to determine the optimal LSD. We do not reproduce the argument though. It exploits the insights gained when demonstrating that $\mu \geq 0$ in (4.45) and is technically more involved than the argument given above for the case that ϱ_s is of rank 4 [44].

Presently we are not aware of an analytical method for solving (4.50), (4.51). But they certainly enable one to design a rapidly converging numerical scheme.

4.2.3 Summary

In summary: For a 2-qubit state ρ of full rank, $\rho > 0$, the optimal LSD has either (i) a separable state ϱ_s of rank 4 or (ii) one of rank 3; in case (i) the pure state ϱ is a Bell state. There is an analytical procedure to decide which is the actual situation, and if (i) is the case, then the optimal LSD is available analytically. In case (ii), however, we do not have, as yet, an analytical method to determine the optimal LSD.

4.3 Examples

In this section we present a couple of special examples for which the optimal LSD is known. The optimal LSDs in Section 4.3.1-4.3.3 were first reported in [19] in a very concise manner; here we give all the details necessary for understanding how the results were obtained.

These examples have a feature in common that helps enormously, namely that the search can be limited to a one-parametric set of LSDs. The optimal one must be contained in this set and can thus be identified straightforwardly.

4.3.1 Self-transposed states

If both Pauli vectors vanish, $s^\downarrow = 0$ and $\vec{t} = 0$, the 2-qubit state ρ is equal to its total transpose ρ^\top , it is *self-transposed*. In view of (2.22), all Bell states are of this kind, and so are all convex sums of Bell states. The converse is also true: All self-transposed states are convex sums of Bell states. Indeed, the eigenstates of a self-transposed ρ are Bell states. Put differently, the pure states $\rho_p^{(k)}$ in the spectral decomposition

$$\rho = \sum_{k=1}^4 r_k \rho_p^{(k)} \quad (4.52)$$

are Bell states if $\rho = \rho^\top$.¹ To be more explicit about these matters, we invoke the generic form of a self-transposed state,

$$\rho = \rho^\top = \frac{1}{4} \left(1 + \vec{\sigma} \cdot \overleftrightarrow{C} \cdot \tau^\downarrow \right) = \frac{1}{4} [1 \pm (c_1 \sigma_1 \tau_1 + c_2 \sigma_2 \tau_2 + c_3 \sigma_3 \tau_3)] , \quad (4.53)$$

where c_1, c_2, c_3 are the characteristic values of \overleftrightarrow{C} and, as in (2.26), the upper sign applies for $\det \left\{ \overleftrightarrow{C} \right\} \geq 0$, the lower for $\det \left\{ \overleftrightarrow{C} \right\} < 0$. Since $\sigma_3 \tau_3 = -(\sigma_1 \tau_1)(\sigma_2 \tau_2)$, the eigenstates of ρ are the common eigenstates of $\sigma_1 \tau_1$, $\sigma_2 \tau_2$, and $\sigma_3 \tau_3$, the four Bell states

$$\begin{aligned} \rho_{\text{Bell}}^{(++-)} &= \frac{1}{4} (1 + \sigma_1 \tau_1 + \sigma_2 \tau_2 - \sigma_3 \tau_3) , \\ \rho_{\text{Bell}}^{(+--)} &= \frac{1}{4} (1 + \sigma_1 \tau_1 - \sigma_2 \tau_2 + \sigma_3 \tau_3) , \\ \rho_{\text{Bell}}^{(-++)} &= \frac{1}{4} (1 - \sigma_1 \tau_1 + \sigma_2 \tau_2 + \sigma_3 \tau_3) , \\ \rho_{\text{Bell}}^{(---)} &= \frac{1}{4} (1 - \sigma_1 \tau_1 - \sigma_2 \tau_2 - \sigma_3 \tau_3) , \end{aligned} \quad (4.54)$$

which are mutually orthogonal.

The superscripts refer to the ± 1 eigenvalues of $\sigma_1 \tau_1$, $\sigma_2 \tau_2$, $\sigma_3 \tau_3$. The corresponding eigenvalues of ρ are given in Table 4.1. The positivity of ρ imposes the

¹For this reason, self-transposed states are sometimes called ‘‘Bell-diagonal states.’’

eigenvalues of			eigenvalues of ρ	monotonic order for	
$\sigma_1\tau_1$	$\sigma_2\tau_2$	$\sigma_3\tau_3$		" ≥ 0 "	" < 0 "
1	1	-1	$\frac{1}{4}[1 \pm (c_1 + c_2 - c_3)]$	r_1	r_4
1	-1	1	$\frac{1}{4}[1 \pm (c_1 - c_2 + c_3)]$	r_2	r_3
-1	1	1	$\frac{1}{4}[1 \mp (c_1 - c_2 - c_3)]$	r_3	r_2
-1	-1	-1	$\frac{1}{4}[1 \mp (c_1 + c_2 + c_3)]$	r_4	r_1

Table 4.1: Eigenvalues of self-transposed 2-qubit states. The upper and lower signs correspond to the two cases of (4.53). The last two columns report the respective ordered assignment required by the standardized spectral decomposition (4.52) for the two cases.

restriction $r_4 \geq 0$, that is:

$$\begin{aligned}
 c_1 + c_2 \leq 1 - c_3 \quad \text{for} \quad \det\{\overline{\mathcal{C}}\} \geq 0, \\
 \text{and} \quad c_1 + c_2 \leq 1 + c_3 \quad \text{for} \quad \det\{\overline{\mathcal{C}}\} < 0,
 \end{aligned} \tag{4.55}$$

which require that the triplet (c_1, c_2, c_3) — which is not a 3-vector — is inside the tetrahedron that R. and M. Horodecki speak of in [46].

In the " ≥ 0 " case, then, the largest eigenvalue of ρ cannot exceed $\frac{1}{2}$,

$$\det\{\overline{\mathcal{C}}\} \geq 0 : \quad r_1 = \frac{1}{4}(1 + c_1 + c_2 - c_3) \leq \frac{1}{2} - \frac{1}{2}c_3, \tag{4.56}$$

so that $\rho^{\tau_1} = \rho^{\tau_2} = \frac{1}{2} - \rho \geq 0$ here, and the Peres–Horodeccy criterion (3.9) says that ρ is separable. In the " < 0 " case, however, we have

$$\det\{\overline{\mathcal{C}}\} < 0 : \quad r_1 = \frac{1}{4}(1 + c_1 + c_2 + c_3) = \frac{1}{4} + \frac{1}{4}\text{Sp}\left\{\left|\overline{\mathcal{C}}\right|\right\}, \tag{4.57}$$

so that $r_1 > \frac{1}{2}$ and $\text{tr}\{\rho^{\tau_1}\rho_{\text{Bell}}^{(---)}\} = \frac{1}{2} - r_1 < 0$ if $\text{Sp}\left\{\left|\overline{\mathcal{C}}\right|\right\} > 1$. Accordingly, the self-transposed state (4.53) is

$$\begin{aligned}
 \text{separable if } \det\{\overline{\mathcal{C}}\} \geq 0 \text{ or } \text{Sp}\left\{\left|\overline{\mathcal{C}}\right|\right\} \leq 1; \\
 \text{non-separable if } \det\{\overline{\mathcal{C}}\} < 0 \text{ and } \text{Sp}\left\{\left|\overline{\mathcal{C}}\right|\right\} > 1.
 \end{aligned} \tag{4.58}$$

Rather than exploiting the Peres–Horodeccy criterion, we could have arrived at this observation by evaluating the Hill–Wootters concurrence of ρ . Here $\left|\sqrt{\rho^{\tau}}\sqrt{\rho}\right| = \rho$, and so the h_k 's of (1.23) are identical with the r_k 's of Table

4.1, and we get

$$\begin{aligned} \mathcal{C} &= \max \{0, r_1 - r_2 - r_3 - r_4\} = \max \{0, 2r_1 - 1\} \\ &= \begin{cases} 0 & \text{if } \det\{\overline{\mathcal{C}}\} \geq 0 \text{ or } \text{Sp}\{|\overline{\mathcal{C}}|\} \leq 1; \\ \frac{1}{2} \text{Sp}\{|\overline{\mathcal{C}}|\} - \frac{1}{2} & \text{if } \det\{\overline{\mathcal{C}}\} < 0 \text{ and } \text{Sp}\{|\overline{\mathcal{C}}|\} > 1. \end{cases} \end{aligned} \quad (4.59)$$

The search for the optimal LSD of a non-separable self-transposed state is facilitated by the intrinsic symmetry of (4.53). In particular, ρ is invariant under the local transformations effected by the unitary operators $\sigma_1\tau_1$, $\sigma_2\tau_2$, $\sigma_3\tau_3$; it is also invariant under the swapping transformation (4.18). Therefore, the pure state ρ of the optimal LSD must also be invariant under these transformations, and so it must be one of the Bell states in (4.54), namely the one associated with the largest eigenvalue r_1 , that is $\rho_{\text{Bell}}^{(---)}$. Thus we arrive at

$$\mathcal{S} = \begin{cases} 1 & \text{if } \det\{\overline{\mathcal{C}}\} \geq 0 \text{ or } \text{Sp}\{|\overline{\mathcal{C}}|\} \leq 1 \\ \frac{3}{2} - \frac{1}{2} \text{Sp}\{|\overline{\mathcal{C}}|\} & \text{if } \det\{\overline{\mathcal{C}}\} < 0 \text{ and } \text{Sp}\{|\overline{\mathcal{C}}|\} > 1 \end{cases} = 1 - \mathcal{C} \quad (4.60)$$

We remark that the concavity (4.4) — applied, for $x = \frac{1}{2}$, to $\rho_1 = \rho$ and $\rho_2 = \rho^\top$ with an *arbitrary* 2-qubit state ρ — tells us that

$$\mathcal{S}\left(\frac{1}{2}(\rho + \rho^\top)\right) \geq \frac{1}{2}\mathcal{S}(\rho) + \frac{1}{2}\mathcal{S}(\rho^\top) = \mathcal{S}(\rho). \quad (4.61)$$

Since $\frac{1}{2}(\rho + \rho^\top)$ is self-transposed by construction, the \mathcal{S} value of (4.60), evaluated for the cross dyadic $\overline{\mathcal{C}}$ of the arbitrary ρ considered, sets an upper bound on $\mathcal{S}(\rho)$.

Another remark concerns the degenerate situation of $c_1 = c_2 = c_3 = |x| \geq 0$. Then the self-transposed state (4.53) takes the form of Werner states (3.21) where,

$$\rho_w = \rho_w^\top = \frac{1}{4} \left(1 - x \vec{\sigma} \cdot \overline{\mathcal{O}}_{en} \cdot \tau^\downarrow \right) \quad \text{with} \quad -\frac{1}{3} \leq x \leq 1. \quad (4.62)$$

For $x \leq \frac{1}{3}$ they are separable, and for $x > \frac{1}{3}$ their degree of separability is $\frac{3}{2}(1-x)$ and their concurrence is $\frac{1}{2}(3x-1)$.

4.3.2 Generalized Werner states

The generic form for these states is

$$\begin{aligned} \rho_{\text{gw}} &= \frac{1+3x}{4} \rho_p + \frac{1-x}{4} (1 - \rho_p) \\ &= \frac{1}{4} (1 + xp(\sigma_1 - \tau_1) - x\sigma_1\tau_1 - xq(\sigma_2\tau_2 + \sigma_3\tau_3)), \end{aligned} \quad (4.63)$$

where ρ_p is any arbitrary pure state (2.14).

To study the positivity of this state, one could calculate the corresponding three numbers A_2, A_1 and A_0 ,

$$A_2 = 6x^2, \quad A_1 = 8x^3, \quad A_0 = 3x^4 \quad (4.64)$$

for the generalized Werner states (4.63), the particular values of p and q being irrelevant here. They are crucial in

$$\det\{\overline{C}\} = -x^3q^2, \quad \det\{\overline{E}\} = -x^3q^2(1 - xp^2), \quad (4.65)$$

however, which we can use in (3.13) to establish that the state (4.63) is separable if $(1 + 2q)x \leq 1$, and non-separable otherwise. Equivalently, we can determine the h_k 's of (1.23),

$$h_1 = h_2 = \frac{1}{4}(1 - x); \quad \left. \begin{matrix} h_3 \\ h_4 \end{matrix} \right\} = \frac{1}{4} \sqrt{(1 + x)^2 - 4x^2p^2} \mp \frac{1}{2}xq, \quad (4.66)$$

and then the concurrence

$$\mathcal{C} = \max \left\{ 0, \frac{1}{2}(1 + 2q)x - \frac{1}{2} \right\}, \quad (4.67)$$

with the same conclusion concerning the separability of ρ . Or, perhaps simplest, we recall (2.20) and note that the smallest eigenvalue of ρ^{T_1} is

$$\frac{1}{4}(1 - x) - \frac{1}{2}xq = \frac{1}{4} - \frac{1}{4}(1 + 2q)x \quad (4.68)$$

and learn once more that the sign of $(1 + 2q)x - 1$ decides whether a generalized Werner state (4.63) is separable or not.

The local unitary transformations generated by $\sigma_1 + \tau_1$, the only local generator in (4.135), leave the state (4.63) unchanged. When looking for the optimal LSD, it is therefore sufficient to consider only those LSDs in which the separable and pure parts commute with $\sigma_1 + \tau_1$ as well. This is, in particular, the case for (4.64), which is one of the many LSDs of ρ .

Accordingly, the pure state of the optimal LSD must be of the form

$$\varrho = \frac{1}{4} [1 + p_0(\sigma_1 - \tau_1) - \sigma_1\tau_1 - q_0(\sigma_2\tau_2 + \sigma_3\tau_3)] \quad (4.69)$$

with $p_0^2 + q_0^2 = 1$, and the separable part must have the structure

$$\varrho_s = \frac{1}{4} [1 + s(\sigma_1 - \tau_1) - c_1\sigma_1\tau_1 - c_2(\sigma_2\tau_2 + \sigma_3\tau_3)]. \quad (4.70)$$

Now, this ϱ_s is positive if $c_1 \leq 1$ and $2\sqrt{c_2^2 + s^2} \leq 1 + c_1$, and it is separable if $c_1 + 2|c_2| \leq 1$ and $2|s| \leq 1 + c_1$. Accordingly, the restrictions

$$c_1 + 2|c_2| \leq 1 \quad \text{and} \quad 2\sqrt{c_2^2 + s^2} \leq 1 + c_1 \quad (4.71)$$

apply. Since ϱ_s is barely separable with respect to ϱ , its partial transpose has at least one zero eigenvalue, so that the equal sign has to hold in the left inequality of (4.71). Further, since q and p are positive by convention, it will suffice to consider non-negative values for q_0, p_0 .

Writing then $c \equiv c_2 \geq 0, c_1 = 1 - 2c$, the right inequality of (4.71) insists on

$$s^2 \leq 1 - 2c, \quad (4.72)$$

and (4.2) is equivalent to the set of equations

$$\begin{aligned} xp &= \mathcal{S}s + (1 - \mathcal{S})p_0, \\ x &= \mathcal{S}c_1 + (1 - \mathcal{S}) = 1 - 2\mathcal{S}c, \\ xq &= \mathcal{S}c_2 + (1 - \mathcal{S})q_0 = \mathcal{S}c + (1 - \mathcal{S})q_0. \end{aligned} \quad (4.73)$$

These are three equations for four unknowns: $s, c, q_0 = \sqrt{1 - p_0^2}$, and \mathcal{S} . Each solution consistent with (4.72) would give one LSD (with a barely separable ρ_s), but we are only interested in the optimal LSD, the solution with the largest value of \mathcal{S} . It is expedient to regard q_0 , the concurrence of ϱ , as the basic parameter and the others as functions of q_0 . Equations (4.73) supply

$$s = p_0 + \frac{xp - p_0}{\mathcal{S}} \quad \text{and} \quad c = \frac{1 - x}{2\mathcal{S}} \quad (4.74)$$

with

$$\mathcal{S} = 1 - \frac{(1 + 2q)x - 1}{2q_0}. \quad (4.75)$$

This tells us that the largest value of q_0 allowed by (4.72) specifies the optimal LSD.

Having expressed s and c in terms of q_0 , we note that (4.72) restricts q_0 by

$$\frac{1 + x - 2xpp_0}{q_0} \leq \left(qx - \frac{1 - x}{2} \right) + \left(qx - \frac{1 - x}{2} \right)^{-1} (x - x^2p^2), \quad (4.76)$$

which gives $q_0 > q$ for $x < 1$ and $q_0 \rightarrow q$ in the limit $x \rightarrow 1$. We are now ready to ask the crucial question: Under which circumstances is (4.76) obeyed by $q_0=1$? In other words: Under which circumstances is ϱ a Bell state? Well, for $q_0 = 1, p_0 = 0$ inequality (4.76) reads

$$2(2qx - 1)^2 \geq 5x^2 - 2x - 1 \quad \text{or} \quad \left(\frac{3}{2}x^{-1} - 2q + \frac{1}{2} \right)^2 \geq 2(1 - q)(2 + q), \quad (4.77)$$

and one verifies easily that there are cases, such as $x = q = 0.8$, for which these equivalent inequalities are violated, so that $q_0 = 1$ is not possible and the largest

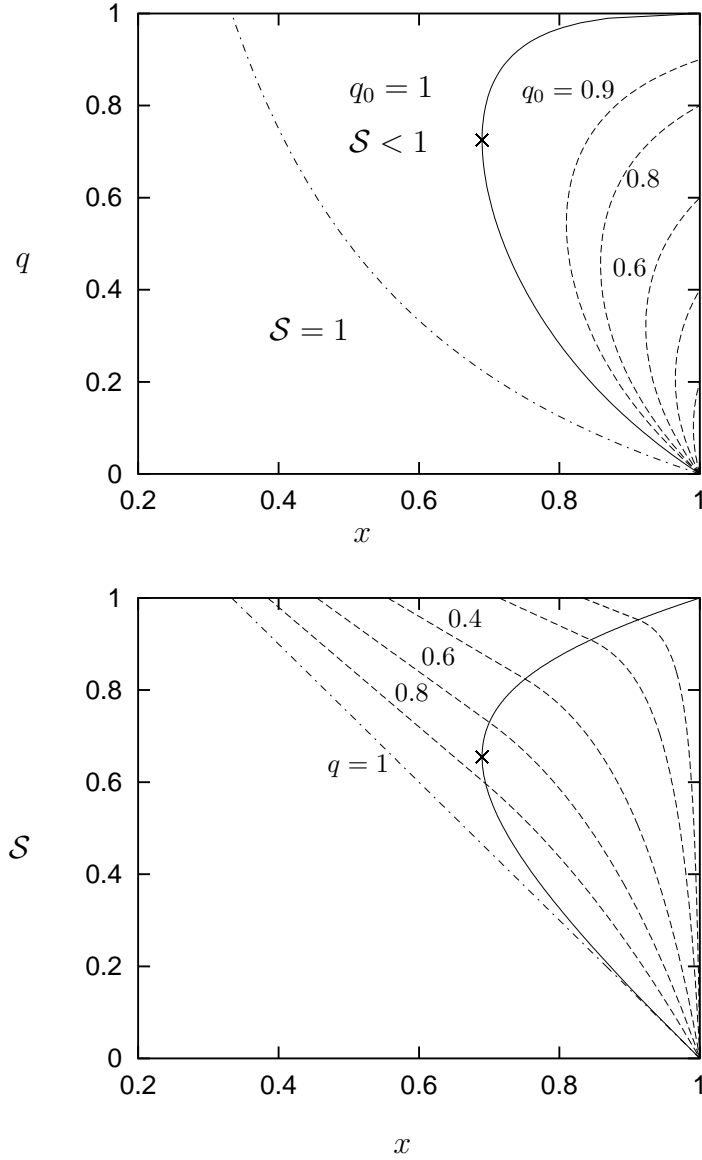


Figure 4.1: Optimal LSDs of generalized Werner states. Top: Lines of constant q_0 in the x, q plane. Bottom: Degree of separability \mathcal{S} as a function of x for various values of q . Both plots cover $\frac{1}{5} \leq x \leq 1$, the more interesting part of the full range $-\frac{1}{3} \leq x \leq 1$.

q_0 value consistent with (4.76) must be really less than 1. More explicitly, the optimal LSD has

$$\begin{aligned} q_0 = 1 & \quad \text{if } x \leq \frac{3}{2} \left[2q - \frac{1}{2} + \sqrt{2(1-q)(2+q)} \right]^{-1}, \\ q_0 < 1 & \quad \text{if } x > \frac{3}{2} \left[2q - \frac{1}{2} + \sqrt{2(1-q)(2+q)} \right]^{-1}, \end{aligned} \quad (4.78)$$

In the latter case, one finds q_0 from the quadratic equation obtained by equating the two sides of (4.76).

A graphical summary of these observations is presented in Figure 4.1. The two solid lines show where the equal sign holds in (4.77); it is the border line between the two cases of (4.78). The crosses mark the point with $x = \frac{1}{5}(\sqrt{6} + 1)$, $q = \frac{1}{2}(\sqrt{6} - 1)$, $\mathcal{S} = \frac{1}{10}(9 - \sqrt{6})$, where $q_0 = 1$, $2qx = 1$, and $\mathcal{S} = 1 - \frac{1}{2}x$. — The top figure displays the lines of constant q_0 . The solid line separates the regions $q_0 = 1$ from $q_0 < 1$. The dash-dotted line separates the separable states ($\mathcal{S} = 1$) from the non-separable ones ($\mathcal{S} < 1$). The dashed lines indicate where $q_0 = 0.9, 0.8, 0.6, 0.4, \text{ and } 0.2$, respectively. — The bottom figure shows \mathcal{S} as a function of x . To the left of the solid line one has $q_0 = 1$ and \mathcal{S} depends linearly on x , to the right one has $q_0 < 0$ and \mathcal{S} is a non-linear function of x . The dash-dotted line corresponds to the standard Werner states ($q = 1$); the dashed lines indicate $q = 0.8, 0.6, 0.4, 0.2, \text{ and } 0.1$, respectively.

If the equal sign holds in (4.76), then it holds in (4.72), which is to say that ϱ_s is of rank 3. The two cases of (4.78) thus illustrate the observation of Karnas and Lewenstein [43] that a state of full rank, here exemplified by the generalized Werner state (4.63), has an optimal LSD with either ϱ_s of rank 4 and ϱ a Bell state (the $q_0 = 1$ case) or with ϱ_s of rank 3 (the $q_0 < 1$ case).

4.3.3 States of rank 2

States for which the equal signs hold in the first and the second inequality of (3.8), but not in the third, are states of rank 2. When we write their eigenvalues as

$$r_1 = \frac{1}{2}(1+x), \quad r_2 = \frac{1}{2}(1-x), \quad r_3 = r_4 = 0 \quad \text{with } 0 \leq x < 1, \quad (4.79)$$

the coefficients of the characteristic polynomial (3.3) are

$$A_2 = 4x^2 + 2, \quad A_1 = 8x^2, \quad A_0 = 4x^2 - 1. \quad (4.80)$$

In the following steps a technique for obtaining the optimal LSD is given:

1. Express the projectors of the eigenkets and eigenbars of $\rho_{\text{rk}2}$ in terms of the given $\rho_{\text{rk}2}$ and construct the projector to the 2D-subspace associated with $\rho_{\text{rk}2}$.

2. Find the subset of parameter values that specify separable $\rho_{\text{rk}2}$.
3. Write the given $\rho_{\text{rk}2}$ in the desired form as:

$$\rho_{\text{rk}2} = \lambda_{\text{max}}\rho_s + (1 - \lambda_{\text{max}})\rho_p.$$

(1) Projectors: For $0 < x < 1$, we want to determine the projectors, $\rho_1 = |\psi^{(1)}\rangle\langle\psi^{(1)}|$ and $\rho_2 = |\psi^{(2)}\rangle\langle\psi^{(2)}|$. To perform this task consider the following forms for the statistical operator $\rho_{\text{rk}2}$ and ρ_1

$$\begin{aligned}\rho_{\text{rk}2} &= y\rho_1 + (1 - y)\rho_2, \\ \rho_1 &= \alpha\rho_{\text{rk}2} + \beta\rho_{\text{rk}2}^2.\end{aligned}\tag{4.81}$$

In terms of $\rho_{\text{rk}2}$ one can rewrite ρ_1 as

$$\begin{aligned}\rho_1 &= \frac{1}{y(1 - 2y)} \left[y\rho_{\text{rk}2} + \rho_{\text{rk}2}(\rho_{\text{rk}2} - 1) \right], \\ \text{with } \alpha &= \frac{1 - y}{y(1 - 2y)}, \quad \beta = -\frac{1}{y(1 - 2y)}.\end{aligned}\tag{4.82}$$

Similarly one can obtain ρ_2 . For $y = \frac{1+x}{2}$ we have,

$$\begin{aligned}\rho_1 &= \frac{1}{x(1 + x)} \left[x\rho_{\text{rk}2} + \rho_{\text{rk}2}(\rho_{\text{rk}2} - 1) \right], \\ \rho_2 &= \frac{1}{x(1 - x)} \left[x\rho_{\text{rk}2} - \rho_{\text{rk}2}(\rho_{\text{rk}2} - 1) \right].\end{aligned}\tag{4.83}$$

The Pauli vectors and the cross dyadics of the two projectors ρ_1 and ρ_2 are functions \vec{s} , t^\downarrow , and \overleftarrow{C} of the given $\rho_{\text{rk}2}$,

$$\begin{aligned}s^{\downarrow(j)} &= \frac{1}{x(1 \pm x)} \left(xs^{\downarrow} \pm \overleftarrow{C} \cdot t^{\downarrow} \right), \\ \vec{t}^{(j)} &= \frac{1}{x(1 \pm x)} \left(x\vec{t} \pm \vec{s} \cdot \overleftarrow{C} \right), \\ \overleftarrow{C}^{(j)} &= \frac{1}{x(1 \pm x)} \left(x\overleftarrow{C} - s^{\downarrow}\vec{t} + \overleftarrow{C}_{\text{sub}} \right), \quad j = 1, 2.\end{aligned}\tag{4.84}$$

As we have seen in Chapter 2, a pure state satisfies relations (2.12). In our case ρ_j , $j = 1, 2$ are projectors by construction. This supplies three more relations among s^{\downarrow} , \vec{t} , and \overleftarrow{C} namely

$$\begin{aligned}\vec{s} \cdot \left(\overleftarrow{C} + \overleftarrow{C}_{\text{sub}} \right) &= \vec{t} \cdot \left[\overleftarrow{C}^{\text{T}} \cdot \overleftarrow{C} + (s^2 - x^2)\overleftarrow{1} \right], \\ \left(\overleftarrow{C} + \overleftarrow{C}_{\text{sub}} \right) \cdot t^{\downarrow} &= \left[\overleftarrow{C} \cdot \overleftarrow{C}^{\text{T}} + (t^2 - x^2)\overleftarrow{1} \right] \cdot s^{\downarrow}, \\ s^{\downarrow}\vec{t} - \left(\text{Sp} \left\{ \overleftarrow{C}^{\text{T}} \cdot \overleftarrow{C} \right\} - x^2 \right) \overleftarrow{C} &= \overleftarrow{C} \cdot t^{\downarrow}\vec{t} + s^{\downarrow}\vec{s} \cdot \overleftarrow{C} + \overleftarrow{E}_{\text{sub}} - \overleftarrow{C} \cdot \overleftarrow{C}^{\text{T}} \cdot \overleftarrow{C}.\end{aligned}\tag{4.85}$$

The parameter x which appears in (4.84), could be written as a function of s^\downarrow , \vec{t} , and \overleftarrow{C} ,

$$\begin{aligned} x^2 &= \vec{s} \cdot \overleftarrow{C} \cdot t^\downarrow - \det \left\{ \overleftarrow{C} \right\}, \\ &= \frac{1}{2} \left(\text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} + s^2 + t^2 - 1 \right). \end{aligned} \quad (4.86)$$

Finally, the projector $\rho^{(2D)}$ to the 2D subspace of $\rho^{(2D)}$ is

$$\begin{aligned} \rho^{(2D)} &= \frac{2}{1-x^2} \rho_{\text{rk}2} (1 - \rho_{\text{rk}2}), \\ &= \frac{1}{2} (1 + \vec{u} \cdot \sigma^\downarrow + \vec{v} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftarrow{Z} \cdot \tau^\downarrow), \end{aligned} \quad (4.87)$$

where \vec{u} , \vec{v} and \overleftarrow{Z} are the Pauli vectors and the cross dyadic for $\rho_{\text{pure}}^{(2D)}$. They are connected with those for $\rho_{\text{rk}2}$ through the following relations

$$\begin{aligned} u^\downarrow &= \frac{1}{1-x^2} \left(s^\downarrow - \overleftarrow{C} \cdot t^\downarrow \right), \\ \vec{v} &= \frac{1}{1-x^2} \left(\vec{t} - \vec{s} \cdot \overleftarrow{C} \right), \\ \overleftarrow{Z} &= \frac{1}{1-x^2} \left(\overleftarrow{C} + \overleftarrow{C}_{\text{sub}} - s^\downarrow \vec{t} \right). \end{aligned} \quad (4.88)$$

(2) A generic form of a projector of rank 2: It could be written as

$$\Sigma_0 = \frac{1}{2} (1 + u\sigma_3 + v\tau_3 + z_1\sigma_1\tau_1 + z_2\sigma_2\tau_2) \quad (4.89)$$

with the non-negative parameters u, v, z_1, z_2 restricted by $z_1 \geq z_2$ as well as $uv = z_1 z_2$ and $u^2 + v^2 + z_1^2 + z_2^2 = 1$, and

$$\begin{aligned} u &= \cos \gamma_1 \cos \gamma_2, & v &= \sin \gamma_1 \sin \gamma_2, \\ z_1 &= \sin \gamma_1 \cos \gamma_2, & z_2 &= \cos \gamma_1 \sin \gamma_2, \\ && \text{with } \frac{1}{2}\pi &\geq \gamma_1 \geq \gamma_2 \geq 0 \end{aligned} \quad (4.90)$$

is a convenient, unambiguous way of writing them. The projector property $\Sigma_0(1 - \Sigma_0) = 0$ is easily verified, and $\text{tr}\{\Sigma_0\} = 2$ is immediate. Clearly, $\rho = \frac{1}{2}\Sigma_0$ has the properties of a 2-qubit state; its concurrence is z_2 , which cannot exceed $\frac{1}{2}$, the value it acquires for $\gamma_1 = \gamma_2 = \pi/4$.

Since the subspace specified by Σ_0 is kinematically equivalent to the state space of a single qubit, the general state in this subspace must be of the 3-parametric form

$$\rho_{\text{rk}2} = \frac{1}{2} (\Sigma_0 + x_1\Sigma_1 + x_2\Sigma_2 + x_3\Sigma_3) \quad \text{with } x_1^2 + x_2^2 + x_3^2 \leq 1, \quad (4.91)$$

where $\Sigma_{1,2,3}$ are analogs of Pauli's spin operators, traceless hermitian operators with the basic algebraic properties

$$\begin{aligned}\Sigma_0 \Sigma_k &= \Sigma_k \quad \text{for } k = 0, 1, 2, 3, \\ \Sigma_j \Sigma_k &= \delta_{jk} \Sigma_0 + i \sum_{l=1}^3 \epsilon_{jkl} \Sigma_l \quad \text{for } j, k = 1, 2, 3.\end{aligned}\tag{4.92}$$

The choice

$$\begin{aligned}\Sigma_1 &= \frac{1}{2} (\sin \gamma_1 \sigma_1 + \cos \gamma_2 \tau_1 + \sin \gamma_2 \sigma_1 \tau_3 + \cos \gamma_1 \sigma_3 \tau_1), \\ \Sigma_2 &= \frac{1}{2} (\sin \gamma_2 \sigma_2 + \cos \gamma_1 \tau_2 + \sin \gamma_1 \sigma_2 \tau_3 + \cos \gamma_2 \sigma_3 \tau_2), \\ \Sigma_3 &= \frac{1}{2} (v \sigma_3 + u \tau_3 - z_2 \sigma_1 \tau_1 - z_1 \sigma_2 \tau_2 + \sigma_3 \tau_3)\end{aligned}\tag{4.93}$$

is particularly convenient. It is such that the limiting situations of $u = 1$, when $\rho_{\text{rk}2} = \frac{1}{4}(1 + \sigma_3)(1 + x_1 \tau_1 + x_2 \tau_2 + x_3 \tau_3)$, and $v = 1$, when $\rho_{\text{rk}2} = \frac{1}{4}(1 + x_1 \sigma_1 + x_2 \sigma_2 + x_3 \sigma_3)(1 + \tau_3)$, are parameterized most naturally.

(3) Barely separable: As described in Section 4.1, the ϱ_s of the optimal decomposition, must be such that $\varrho_s^{\text{T}2}$ has a zero eigenvalue. In terms of the parameters x_1, x_2, x_3 in the generic form (4.91) of rank-2 states $\rho_{\text{rk}2}$, the value of x is given by

$$x = \sqrt{x_1^2 + x_2^2 + x_3^2}.\tag{4.94}$$

Not unexpectedly, x is the distance from the center of the unit sphere $x_1^2 + x_2^2 + x_3^2 \leq 1$. The surface of the sphere is composed of the pure states on the boundary of this subspace of rank-2 states.

In view of (4.80), the (3.13) version of the Peres–Horodeccy criterion requires

$$\det\{E\} \geq 0 \quad \text{and} \quad \det\{\overline{C}\} \geq 0\tag{4.95}$$

for a separable rank-2 state. The first determinant,

$$\begin{aligned}\det\{E\} &= -\left[(z_2 - z_1 x_3)^2 + (1 - x_1^2 - x_3^2)(z_1^2 - z_2^2)\right] \\ &\quad \times \left[(z_2 - z_1 x_3)^2 + x_2^2(z_1^2 - z_2^2)\right],\end{aligned}\tag{4.96}$$

is non-positive and vanishes only if (recall that $z_1 \geq z_2 \geq 0$ by convention)

$$z_1 = 0 \quad \text{or} \quad z_1 x_3 = z_2 \quad \text{and} \quad x_2 = 0,\tag{4.97}$$

and then

$$\begin{aligned}\det\{\overline{C}\} &= x_3(z_1 - z_2 x_3)(z_2 - z_1 x_3) \\ &\quad - z_1 x_2^2(z_1 - z_2 x_3) - z_2 x_1^2(z_2 - z_1 x_3)\end{aligned}\tag{4.98}$$

vanishes too. Now, we have the following possibilities

1. If $z_1 = z_2 = 0$, then $\det \{\overleftrightarrow{E}\} = \det \{\overleftrightarrow{C}\} = 0$, then all $\rho_{\text{rk}2}$'s are separable. In this case there are two possibilities: The *first*, $u = 1$ and $v = 0$, for this limit $\rho_{\text{rk}2}$ is separable and defined by the product states

$$\rho_{\text{rk}2} = \frac{1}{4}(1 + \sigma_3)(1 + x_1\tau_1 + x_2\tau_2 + x_3\tau_3). \quad (4.99)$$

The *second*, $u = 0$ and $v = 1$ in this case,

$$\rho_{\text{rk}2} = \frac{1}{4}(1 + x_1\sigma_1 + x_2\sigma_2 + x_3\sigma_3)(1 + \tau_3). \quad (4.100)$$

2. For $z_1 > 0$, the pure separable states are specified by

$$-\sqrt{1 - (z_2/z_1)^2} \leq x_1 \leq \sqrt{1 - (z_2/z_1)^2}, \quad x_2 = 0, \quad x_3 = z_2/z_1. \quad (4.101)$$

Then the barely separable states are those for which (4.101) determines the values of (x_2, x_3) . Different values of x_1 distinguish different barely separable states, ρ_{bsep} . Accordingly, we write

$$\rho_{\text{bsep}}(x_0) \equiv \rho_{\text{rk}2}(x_1, x_2, x_3)|_{x_1=x_0, x_2=0, x_3=z_2/z_1}. \quad (4.102)$$

The barely separable is described by its Pauli vectors and its cross dyadic as:

$$\begin{aligned} s_{\text{b}}^{\downarrow} &= x_0 \sqrt{v^2 + z_1^2} e_1^{\downarrow} + (u + \frac{z_2}{z_1} v) e_3^{\downarrow}, \\ \vec{t}_{\text{b}} &= x_0 \sqrt{u^2 + z_1^2} \vec{n}_1 + (v + \frac{z_2}{z_1} u) \vec{n}_3, \\ \overleftrightarrow{C}_{\text{b}} &= (z_1 - \frac{z_2^2}{z_1}) e_1^{\downarrow} \vec{n}_1 + \frac{z_2}{z_1} e_3^{\downarrow} \vec{n}_1 \\ &\quad + x_0 (\sqrt{v^2 + z_2^2} e_1^{\downarrow} \vec{n}_3 + \sqrt{u^2 + z_2^2} e_3^{\downarrow} \vec{n}_1), \end{aligned} \quad (4.103)$$

where $(e_1^{\downarrow}, e_2^{\downarrow}, e_3^{\downarrow})$ and $(\vec{n}_1, \vec{n}_2, \vec{n}_3)$ are the bases of the characteristic representation of the dyadic \overleftrightarrow{Z} .

(4) Decomposition and the degree of separability: With this visualization it is clear that, for $z_1 > z_2 \geq 0$, there is a one-parametric set of LSDs for each non-separable rank-2 state. The given state corresponds to point $X = (x_1, x_2, x_3)$ inside the sphere. Pick any point $X_{\text{sep}} = (x_0, 0, z_2/z_1)$ on the line of separable states, and find the pure-state surface point $X_{\text{pure}} = (\sin \vartheta \cos \varphi, \sin \vartheta \sin \varphi, \cos \vartheta)$ on the ray from X_{sep} through X . Then one can write the decomposition (4.1) as

$$\rho_{\text{rk}2}(x_1, x_2, x_3) = \lambda \rho_{\text{bsep}}(x_0) + (1 - \lambda) \rho_{\text{pure}}(X_{\text{pure}}) \quad (4.104)$$

this construction produces one LSD for each X_{sep} . More explicitly, one needs to solve the set of equations

$$\begin{aligned} x_1 &= \lambda x_0 + (1 - \lambda) \sin \vartheta \cos \varphi, \\ x_2 &= (1 - \lambda) \sin \vartheta \sin \varphi, \\ x_3 &= \lambda z_2/z_1 + (1 - \lambda) \cos \vartheta, \end{aligned} \quad (4.105)$$

where we regard x_1, x_2, x_3 as given and the unknowns $\vartheta, \varphi, \lambda$ as functions of y . After eliminating ϑ and φ , we get a single equation that relates λ to x_0 ,

$$(1 - \lambda)^2 = (x_1 - \lambda x_0)^2 + x_2^2 + (x_3 - \lambda z_2/z_1)^2. \quad (4.106)$$

For each x_0 with $x_0^2 \leq 1 - (z_2/z_1)^2$ there is one λ in the range $0 \leq \lambda \leq 1$, and the degree of separability is the largest one of them. This optimum is either at one of the boundaries of the x_0 range or inside the range. In the first case, ρ_s is a pure state, that is: it is of reduced rank; in the second case, ρ_s is of rank 2. Let us consider the two cases:

(1) x_0 is on the edge, i.e., $x_0 = \pm \sqrt{1 - (z_2/z_1)^2}$. From (4.106), we have

$$\mu_{\pm} = \frac{2}{1 - x^2} \lambda_{\pm}^2 (x_1 - x_0 \lambda_{\pm}) \quad (4.107)$$

where $\mu_{\pm} = \frac{\partial \lambda}{\partial x_0} |_{x_0}$ and $\lambda_{\pm} = \mathcal{S}$. On the boundary $\mu_- \mu_+ \geq 0$, this requires that the following inequality

$$|x_1| \left(1 - \frac{z_2}{z_1} x_3 \right) \geq \left(\frac{1 - x^2}{2} + x_1^2 \right) \sqrt{1 - \left(\frac{z_2}{z_1} \right)^2} \quad (4.108)$$

holds. In this case, the degree of separability is given by

$$\mathcal{S} = \frac{(1 - x^2)/2}{1 - \frac{z_2}{z_1} x_3 - x_0 x_1}, \quad (4.109)$$

with

$$x_0 = \pm \sqrt{1 - \left(\frac{z_2}{z_1} \right)^2} \quad \text{where} \quad \begin{cases} + & \text{for } x_1 > 0, \\ - & \text{for } x_1 < 0. \end{cases} \quad (4.110)$$

(2) x_0 is in the range, i.e., $-\sqrt{1 - (z_2/z_1)^2} < x_0 < \sqrt{1 - (z_2/z_1)^2}$: In this case, the inequality (4.108) is violated and the degree of separability is

$$\mathcal{S} = \frac{1}{1 - (z_2/z_1)^2} \left[1 - x_3 \frac{z_2}{z_1} - \sqrt{\left(x_3 - \frac{z_2}{z_1} \right)^2 - x_2^2 \left(1 - \frac{z_2^2}{z_1^2} \right)} \right], \quad (4.111)$$

and

$$\begin{aligned} x_0 &= \frac{x_1}{\mathcal{S}}, \\ X_{\text{pure}} &= (x_1 - x_0\mathcal{S}, x_2, x_3 - (z_2/z_1)\mathcal{S})/(1 - \mathcal{S}), \end{aligned} \quad (4.112)$$

which tells us the coordinates of the surface point that specifies ϱ , the pure state of the optimal LSD. Tersely: If (4.108) is obeyed, then X_{sep} is the endpoint closest to X on the $x_2 = 0, x_3 = z_2/z_1$ line of X_{sep} 's; if it is violated, then X_{pure} is the $x_1 = 0$ point closest to X on the circumference of the circular cross section that the sphere $x \leq 1$ has with the plane defined by the point X and the line of X_{sep} 's. These matters are illustrated in Figure 4.2

Note that this exemplifies the pairing property (4.16). The pure states with $x_1 = 0$ are paired with all separable states, those with $x_1 \geq 0$ are paired only with the product states specified by $x_1 = \pm\sqrt{1 - (z_2/z_1)^2}$, $x_2 = 0$, $x_3 = z_2/z_1$, respectively.



Figure 4.2: Optimal LSDs of 2-qubit states of rank 2. The $x_2 = 0, x_3 = z_2/z_1$ line of X_{sep} 's (thick horizontal line) and the point $X = (x_1, x_2, x_3)$ corresponding to the given non-separable state (indicated by \otimes for two different examples) define a plane that has a circular cross section with the sphere $x_1^2 + x_2^2 + x_3^2 \leq 1$. Vertical lines have constant x_1 ; horizontal lines have constant x_2 and x_3 . The direction normal to the plane is $(0, z_2 - z_1x_3, x_2) \propto (0, -\sin\theta, \cos\theta)$ where θ is the tilt angle relative to the plane $x_3 = 0$. The center of the circle is at $(z_2/z_1) \cos\theta(0, -\sin\theta, \cos\theta)$; its radius is $\sqrt{1 - [(z_2/z_1) \cos\theta]^2}$. The concurrence of a rank-2 state is proportional to the distance of its cross \otimes from the thick line of separable states. **Left:** Different LSDs for the two exemplary states are indicated by the dotted lines that connect a separable state with a pure state through the \otimes 's. The point \otimes divides the lines in proportions of $(1 - \lambda) : \lambda$. The respective sets of pure states are marked by arcs just outside the circle. **Right:** The two optimal LSDs are indicated by the dash-dotted lines. Inequality (4.108) is violated inside the kite-shaped area bounded by the dashed lines.

In the caption to Figure 4.2, there is a remark about the geometrical significance of the concurrence of rank-2 states. Its calculation is straightforward, but a bit tedious (it helps to observe that $\rho^\top \rho$ and $\Sigma_0 \rho^\top \Sigma_0 \rho$ have the same eigenvalues), with the outcome

$$\mathcal{C} = \sqrt{(z_1^2 - z_2^2)x_2^2 + (z_2 - z_1 x_3)^2} . \quad (4.113)$$

Geometrically speaking, this says that the points X of states with common concurrence \mathcal{C} constitute the surface of an elliptical cylinder, specified by

$$(x_1, x_2, x_3) = \left(x_1, \left[\mathcal{C} / (z_1^2 - z_2^2) \right]^{\frac{1}{2}} \cos \varphi, z_2 / z_1 + (\mathcal{C} / z_1) \sin \varphi \right) \quad (4.114)$$

with arbitrary (real) values for x_1 and φ .

Now note that we can write the concurrence also as

$$\mathcal{C} = z_1 R d , \quad (4.115)$$

where

$$R = \left(\frac{[1 - (z_2/z_1)^2]x_2^2 + (x_3 - z_2/z_1)^2}{x_2^2 + (x_3 - z_2/z_1)^2} \right)^{1/2} \quad (4.116)$$

is the radius of the circle in Figure 4.2 and

$$d = [x_2^2 + (x_3 - z_2/z_1)^2]^{1/2} \quad (4.117)$$

is the Hilbert-Schmidt distance between ρ and the nearest separable state.² In Figure 4.2 this is simply the Euclidean distance from the point \otimes that specifies ρ to the thick line that represents the separable states.³ Since \otimes divides the line representing the optimal LSD in proportions of $(1 - \mathcal{S}) : \mathcal{S}$, the first inequality in (4.5) is actually an equality for all rank-2 states, as it is also for the self-transposed states of Section 4.3.1 and the generalized Werner states of Section 4.3.2. This can hardly be accidental, but we don't know why the states of these three kinds are particular in this respect. There is an obvious challenge here: Find the conditions on ρ under which the equal sign holds.

The various LSDs on the left of Figure 4.2 involve pure states with a variety of concurrences. In view of the geometrical significance of the concurrence just noted, we observe that the pure state ϱ of the optimal LSD is the one with the largest concurrence. The same is clearly true for the self-transposed states and

²That is: The nearest one among the separable states in the rank-2 subspace under consideration. There could be other separable states with an even smaller distance, but they cannot show up in a LSD of $\rho_{\text{rk}2}$.

³The nearest separable state may or may not be equal to ϱ_s , the one that shows up in the optimal LSD.

also for those LSDs of the generalized Werner states that we had to consider to find the optimal LSD. We surmise that

$$\begin{aligned} & \text{The concurrence of the pure state in any LSD (4.1)} \\ & \text{cannot exceed the concurrence of } \rho, \text{ the pure state} \\ & \text{of the optimal LSD (4.2).} \end{aligned} \quad (4.118)$$

is generally true, but presently we cannot demonstrate the case.

(5) Summary: Now, the preceding procedure could be summarized in the following steps,

1. Check equations (4.80), if they hold, then we are dealing with a state ρ of rank 2 and the value of x^2 is obtained from (4.86).
2. Find u^\downarrow, \vec{v} and \overleftrightarrow{Z} in accordance with (4.88) and calculate the characteristic values z_1, z_2 of \overleftrightarrow{Z} as well as its characteristic representation.
3. If $z_1 = 0$, the $\rho_{\text{rk}2}$ is separable, i.e., $\mathcal{S} = 1$; otherwise one employs,

$$\begin{aligned} x_1 &= \frac{\vec{e}_1 \cdot s^\downarrow}{\sqrt{v^2 + z_1^2}} = \frac{\vec{t} \cdot n_1^\downarrow}{\sqrt{u^2 + z_1^2}}, \\ x_2 &= \frac{\vec{e}_2 \cdot \overleftrightarrow{C} \cdot n_3^\downarrow}{\sqrt{v^2 + z_1^2}} = \frac{\vec{e}_3 \cdot \overleftrightarrow{C} \cdot n_2^\downarrow}{\sqrt{u^2 + z_1^2}}, \\ x_3 &= \vec{e}_3 \cdot \overleftrightarrow{C} \cdot n_3^\downarrow, \end{aligned} \quad (4.119)$$

4. Now, if inequality (4.108) holds then the degree of separability is given by (4.110), otherwise it is given by (4.111).
5. To obtain the barely separable states, by direct substitution in (4.103) for the values of x_0, z_1 and z_2 , one obtains $s_b^\downarrow, \vec{t}_b, \overleftrightarrow{C}_b$.

Now, we give two examples to show how this procedure works: (1) As a simple example consider $\rho_{\text{rk}2} = \frac{1}{2}\Sigma_0$: where

$$\frac{1}{2}\Sigma_0 = \frac{1}{4}(1 + u\sigma_3 + v\tau_3 + z_1\sigma_1\tau_1 + z_2\sigma_2\tau_2). \quad (4.120)$$

Using equations (3.6) to calculate the three numbers A_2, A_1, A_0 as well as x from (4.86), one gets

$$A_2 = 2, \quad A_1 = 0, \quad A_0 = -1, \quad \text{and} \quad x^2 = 0. \quad (4.121)$$

Now u^\downarrow, \vec{v} and \overleftrightarrow{Z} are given by

$$u^\downarrow \hat{=} \begin{pmatrix} 0 \\ 0 \\ u \end{pmatrix}, \quad \vec{v} \hat{=} (0, 0, v), \quad \text{and} \quad \overleftrightarrow{Z} \hat{=} \begin{pmatrix} z_1 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \quad (4.122)$$

The characteristic values of \vec{Z} are $z_1 \geq z_2 \geq 0$ and the characteristic representations are

$$(e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \hat{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix} \hat{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (4.123)$$

From (4.119), one obtains $x_1 = x_2 = x_3 = 0$. Also we notice that $x_0=0$ is the value at which $\frac{\partial \lambda}{\partial x_0} = 0$. The inequality (4.108) is violated, so the degree of separability is obtained from (4.111). Using the value of x_0 in (4.103), one obtains the barely separable ρ_{bsep} . To obtain the corresponding pure state ρ_{p} we evaluate X_{pure} from (4.112). Then we have

$$\begin{aligned} \mathcal{S} &= \frac{z_1}{z_1 + z_2} \\ \rho_{\text{bsep}} &= \frac{1}{4} \left[1 + \left(u + \frac{z_2}{z_1}v\right)\sigma_3 + \left(v + \frac{z_2}{z_1}u\right)\tau_3 + \left(z_1 - \frac{z_2^2}{z_1}\right)\sigma_1\tau_1 + \frac{z_2}{z_1}\sigma_3\tau_3 \right], \\ \rho_{\text{p}} &= \frac{1}{4} \left[1 + (u - v)\sigma_3 + (v - u)\tau_3 + (z_1 + z_2)\sigma_1\tau_1 + (z_1 + z_2)\sigma_2\tau_2 - \sigma_3\tau_3 \right]. \end{aligned} \quad (4.124)$$

(2) In this example, a rank-2 case is constructed from two orthogonal pure states

$$\begin{aligned} \rho_{\text{p}}^{(1)} &= \frac{1}{4} (1 + (u - v)\sigma_3 + (v - u)\tau_3 + (z_1 + z_2)\sigma_1\tau_1 + (z_1 + z_2)\sigma_2\tau_2 - \sigma_3\tau_3), \\ \rho_{\text{p}}^{(2)} &= \frac{1}{4} (1 - (u + v)\sigma_3 - (v + u)\tau_3 - (z_1 - z_2)\sigma_1\tau_1 - (z_2 - z_1)\sigma_2\tau_2 - \sigma_3\tau_3). \end{aligned} \quad (4.125)$$

where $\text{tr} \left\{ \rho_{\text{p}}^{(1)} \rho_{\text{p}}^{(2)} \right\} = 0$. Then

$$\rho_{\text{rk2}} = \frac{1 + \alpha}{2} \rho_{\text{p}}^{(1)} + \frac{1 - \alpha}{2} \rho_{\text{p}}^{(2)}. \quad (4.126)$$

Following the same aforementioned steps, one gets

$$\begin{aligned} \mathcal{S} &= \frac{1 - |\alpha|}{1 - \frac{z_2}{z_1}}, \\ \rho_{\text{bsep}} &= \frac{1}{4} \left[1 - \left(v + \frac{z_2}{z_1}u\right)\sigma_3 - \left(u + \frac{z_2}{z_1}v\right)\tau_3 + \left(z_1 - \frac{z_2^2}{z_1}\right)\sigma_2\tau_2 + \frac{z_2}{z_1}\sigma_3\tau_3 \right], \\ \rho_{\text{p}} &= \frac{1}{4} \left[1 + (u - v)(\sigma_3 - \tau_3) + (z_1 + z_2)(\sigma_1\tau_1 + \sigma_2\tau_2) - \sigma_3\tau_3 \right]. \end{aligned} \quad (4.127)$$

4.3.4 States of rank “2+2”

This kind of states could be described by:

$$\begin{aligned}\rho^{(2+2)} &= \frac{1+y}{2}\rho_p^{(2D)} + \frac{1-y}{2}\left(\frac{1}{2} - \rho_p^{(2D)}\right) \\ &= \frac{1-y}{4} + \frac{y}{2}\Sigma_0.\end{aligned}\quad (4.128)$$

As we have seen in Example 1, the operator $\frac{1}{2}\Sigma_0$ is decomposed to a separable and entangled part as

$$\frac{1}{2}\Sigma_0 = \frac{z_1}{z_1+z_2}\frac{1}{2}(\Sigma_0 + \frac{z_2}{z_1}\Sigma_3) + \frac{z_2}{z_1+z_2}\frac{1}{2}(\Sigma_0 - \Sigma_3), \quad (4.129)$$

where the first term is a separable and the second one is non-separable. In our case there is an extra separable part, so we consider that the entangled part for our case is also $\frac{1}{2}(\Sigma_0 - \Sigma_3)$ and study the positivity of the new state.

$$\rho^{(2+2)} = \lambda\rho_s + (1-\lambda)\frac{1}{2}(\Sigma_0 - \Sigma_3), \quad (4.130)$$

where,

$$\rho_s = \frac{1-y}{4\lambda} + \frac{y+\lambda-1}{2\lambda}\Sigma_0 + \frac{1-\lambda}{2\lambda}\Sigma_3. \quad (4.131)$$

Let us study the positivity of the new separable part (4.131). From (3.6), the three numbers A_2, A_1 and A_0 are

$$A_2 = 2\alpha^2 + 4\beta^2, \quad A_1 = 8\alpha\beta^2, \quad A_0 = \alpha^2(4\beta^2 - \alpha^2) \quad (4.132)$$

where $\alpha = \frac{y+\lambda-1}{\lambda}$ and $\beta = \frac{1-\lambda}{\lambda}$. The positivity of (4.131) requires $\alpha \leq 1$ and $|\beta| \leq \frac{1+\alpha}{2}$. On the other hand the eigenvalues of $\rho_s^{\text{T}_2}$ are,

$$\begin{aligned}\nu_{1,2} &= \frac{1}{4} \left[1 + \beta \pm \sqrt{(\alpha - \beta)^2 q_1^2 + (\alpha + \beta)^2 (p_2)^2} \right], \\ \nu_{3,4} &= \frac{1}{4} \left[1 - \beta \pm \sqrt{(\alpha - \beta)^2 q_1^2 + (\alpha + \beta)^2 (p_2)^2} \right].\end{aligned}\quad (4.133)$$

The LSD decomposition is an optimal one if $\rho_s^{\text{T}_2}$ has a one zero eigenvalues, see Section 4.1, when it is *barely separable*. To perform this task, one has to equate the largest eigenvalue with zero. Then the degree of separability is

$$\mathcal{S} = \begin{cases} 1 & \text{for } y \leq (\sqrt{1+4z_1z_2})^{-1}, \\ 1 - \frac{y}{2} + \frac{1}{2q_1} \sqrt{1-y^2+y^2q_2^2} & \text{for } y > (\sqrt{1+4z_1z_2})^{-1}. \end{cases} \quad (4.134)$$

4.3.5 States of rank 3

The 2-qubit state that corresponds to a projector of rank 3 is of the form $\rho = \frac{1}{3}(1 - \rho_p)$ with any pure state ρ_p ; this ρ has vanishing concurrence. All states that are orthogonal to the chosen ρ_p are in the subspace thus defined. With ρ_p in its generic form (2.14), all ρ 's in this subspace are obtained by adding to $\rho = \frac{1}{3}(1 - \rho_p)$ linear combinations of the 8 hermitian operators

$$\begin{aligned} & \sigma_1 + \tau_1, \quad \sigma_2\tau_2 - \sigma_3\tau_3, \quad \sigma_2\tau_3 + \sigma_3\tau_2, \\ & p(\sigma_2 - \tau_2) + (1 + q)(\sigma_1\tau_2 + \sigma_2\tau_1), \\ & (1 + q)(\sigma_2 + \tau_2) - p(\sigma_1\tau_2 - \sigma_2\tau_1), \\ & p(\sigma_3 - \tau_3) + (1 + q)(\sigma_1\tau_3 + \sigma_3\tau_1), \\ & (1 + q)(\sigma_3 + \tau_3) - p(\sigma_1\tau_3 - \sigma_3\tau_1), \\ & 2\sigma_1\tau_1 + p(\sigma_1 - \tau_1) - q(\sigma_2\tau_2 + \sigma_3\tau_3), \end{aligned} \quad (4.135)$$

which commute with ρ_p , are traceless, and have traceless products among each other.

In this section, the technique of the rank-2 case, Section (4.3.3), is used to find the optimal decomposition for a rank-3 case. A rank-3 case could be defined as a sum of three pure states,

$$\rho_{\text{rk3}} = r_1\rho_p^{(1)} + r_2\rho_p^{(2)} + r_3\rho_p^{(3)}, \quad (4.136)$$

where $r_1 \geq r_2 \geq r_3 > 0$ are the eigenvalues of ρ_{rk3} . To split this state, one needs to construct a rank-2 state from the $\rho_p^{(1)}$ and $\rho_p^{(2)}$. This ρ_{rk2} is decomposed to its pure and separable parts as:

$$\rho_{\text{rk}}^{(12)} = \lambda^{(12)}\rho_s^{(12)} + (1 - \lambda^{(12)})\rho_p^{(12)}. \quad (4.137)$$

Another time a new rank-2 state, $\rho_{\text{rk2}}^{(123)}$ is constructed from the new pure part, $\rho_p^{(12)}$, and $\rho_p^{(3)}$, which again is decomposed to

$$\rho_{\text{rk2}}^{(123)} = \lambda^{(123)}\rho_s^{(123)} + (1 - \lambda^{(123)})\rho_p^{(\text{final})}. \quad (4.138)$$

Then the final decomposition of the ρ_{rk3} case is

$$\rho_{\text{rk3}} = \lambda_{\text{max}}\rho_s^{(\text{final})} + (1 - \lambda_{\text{max}})\rho_p^{(\text{final})}, \quad (4.139)$$

where

$$\begin{aligned} \rho_s^{(\text{final})} &= \lambda^{(12)}\rho_s^{(12)} + \lambda^{(123)}\rho_s^{(123)}, \\ \lambda_{\text{max}} &= \lambda^{(12)} + \lambda^{(123)}. \end{aligned} \quad (4.140)$$

It is clear that this decomposition is not unique, because one can construct a different rank-2 state. For, any rank-3 state, we have three possibilities, the first

one which is described as above is called $[1+2]+[3]$ case, the other is $[2+3]+[1]$ case, and $[1+3]+[2]$ case. There is another possibility of using the technique of the rank-2 case, where one reduces the rank-3 case to a rank-2 case. This last possibility could be described as

$$\rho_{\text{rk}3} = (r_1 + r_2 - 2r_3)\rho_{\text{rk}2}^{(12)} + 3r_3\rho_{\text{s}}^{(1)} \quad (4.141)$$

where

$$\rho_{\text{s}}^{(1)} = \frac{1}{3}(\rho_{\text{p}}^{(1)} + \rho_{\text{p}}^{(2)} + \rho_{\text{p}}^{(3)}). \quad (4.142)$$

This $\rho_{\text{rk}2}^{(12)}$ is a rank-2 state that is decomposed to its pieces, separable and entangled parts. Finally we obtain

$$\begin{aligned} \rho_{\text{rk}3} &= \lambda\rho_{\text{s}} + (1 - \lambda)\rho_{\text{p}} \quad \text{with} \\ \lambda &= 3r_3 + \lambda^{(12)}(r_1 + r_2 - 2r_3) \end{aligned} \quad (4.143)$$

where $\lambda^{(12)}$ is the degree of separability of $\rho_{\text{rk}2}^{(12)}$. In fact, when this method is applied to a lot of examples, we obtain that the λ value is always smaller than the λ value which is obtained by using the technique of rank-2. After one performs all these possibilities, we choose the one of them which has the largest degree of separability, λ_{max} . Then we perform the “ ϵ optimization”, i.e., one adds an ϵ part from the pure part to the separable one. We study the positivity of the new state and find the maximum value of ϵ at which the new state is separable. To show this idea consider the following example. Suppose that three pure states which appear in (4.136) are given by:

$$\begin{aligned} \rho_{\text{p}}^{(1)} &= \frac{1}{4}[1 + p_1\sigma_z - p_1\tau_z + q_1\sigma_x\tau_x + q_1\sigma_y\tau_y - \sigma_z\tau_z], \\ \rho_{\text{p}}^{(2)} &= \frac{1}{4}[1 - p_1\sigma_z + p_1\tau_z - q_1\sigma_x\tau_x - q_1\sigma_y\tau_y - \sigma_z\tau_z], \\ \rho_{\text{p}}^{(3)} &= \frac{1}{4}[1 + p_2\sigma_z + p_2\tau_z + q_2\sigma_x\tau_x - q_2\sigma_y\tau_y + \sigma_z\tau_z]. \end{aligned} \quad (4.144)$$

Following the aforementioned procedure there are three possibilities with eigenvalues

$$r_1 = \frac{1+y}{2} \frac{1+x}{2}, \quad r_2 = \frac{1+y}{2} \frac{1-x}{2}, \quad r_3 = \frac{1-y}{2}. \quad (4.145)$$

1. Case $[1+2]+[3]$: In an explicit form $\rho_{\text{rk}3}$ is

$$\rho_{\text{rk}3} = \frac{1+y}{2}\rho_{\text{rk}2}^{(12)} + \frac{1-y}{2}\rho_{\text{p}}^{(3)}, \quad (4.146)$$

with

$$\rho_{\text{rk}2}^{(12)} = \frac{1}{4}[1 + \alpha^{(12)}p_1(\sigma_3 - \tau_3) + \alpha^{(12)}q_1(\sigma_1\tau_1 + \sigma_2\tau_2) - \sigma_3\tau_3], \quad (4.147)$$

where $\alpha^{(12)} = x$. Using the procedure of rank-2 case, we decompose $\rho_{\text{rk2}}^{(12)}$ such that

$$\begin{aligned}\rho_s^{(12)} &= \frac{1}{4}[1 - \sigma_3\tau_3], \\ \rho_p^{(12)} &= \frac{1}{4}[1 + p_1(\sigma_3 - \tau_3) + q_1(\sigma_1\tau_1 + \sigma_2\tau_2) - \sigma_3\tau_3], \\ \lambda^{(12)} &= \frac{1+y}{2}(1-x) = 2r_2.\end{aligned}\tag{4.148}$$

In the next step one uses $\rho_p^{(12)}$ and $\rho_p^{(3)}$ to construct a new rank-2, defined as:

$$\begin{aligned}\rho_{\text{rk2}}^{(123)} &= \frac{1}{4}[1 + (u - \alpha^{(123)}v)\sigma_3 + (v - \alpha^{(123)}u)\tau_3 + (z_1 + \alpha^{(123)}z_2)\sigma_1\tau_1 + \\ &\quad + (z_2 + \alpha^{(123)}z_1)\sigma_2\tau_2 - \alpha^{(123)}\sigma_3\tau_3]\end{aligned}\tag{4.149}$$

where $\alpha^{(123)} = \frac{2(1-\lambda^{(12)})-(1-y)}{2(1-\lambda^{(12)})+(1-y)}$. Again we obtain the following decomposition:

$$\begin{aligned}\rho_s^{(123)} &= \frac{1}{4}\left[1 + \frac{p_1q_2 + p_2q_1}{q_1 + q_2}\sigma_3 - \frac{p_1q_2 - p_2q_1}{q_1 + q_2}\tau_3 - \frac{p_1q_2 - p_2q_1}{q_1 + q_2}\sigma_1\tau_1\right. \\ &\quad \left.+ \frac{q_1 - q_2}{q_1 + q_2}\sigma_3\tau_3\right], \\ \rho_p^{(123)} &= \frac{1}{4}[1 + p_1\sigma_3 - p_1\tau_3 + q_1\sigma_1\tau_1 + q_1\sigma_2\tau_2 - \sigma_3\tau_3], \\ \lambda^{(123)} &= \frac{r_3}{q_1}[q_1 + q_2].\end{aligned}\tag{4.150}$$

2. Case $[1+3]+[2]$: For the case $[1+3]$ straightforward calculation, one obtains, the same result as the case $\rho_{\text{rk2}}^{(123)}$ and the new rank-2 case $\rho_{\text{rk2}}^{(132)}$ is the same as $\rho_{\text{rk2}}^{(12)}$, i.e.,

$$\begin{aligned}\rho_s^{(13)} &= \rho_s^{(123)}, & \rho_s^{(132)} &= \rho_s^{(12)}, \\ \rho_p^{(13)} &= \rho_p^{(123)}, & \rho_p^{(132)} &= \rho_p^{(12)}, \\ \lambda^{(13)} &= \lambda^{(123)}, & \lambda^{(132)} &= \lambda^{(12)}.\end{aligned}\tag{4.151}$$

3. Case $[2+3]+[1]$: For this case we have

$$\begin{aligned}\rho_{\text{sep}}^{(23)} &= \frac{1}{4}\left[1 + \frac{p_1q_2 + p_2q_1}{q_1 + q_2}\sigma_3 - \frac{p_1q_2 - p_2q_1}{q_1 + q_2}\tau_3 + \frac{q_1q_2}{q_1 + q_2}\sigma_1\tau_1 + \frac{q_1 - q_2}{q_1 + q_2}\sigma_3\tau_3\right], \\ \rho_{\text{pure}}^{(23)} &= \frac{1}{4}[1 - p_1\sigma_3 - p_1\tau_3 - q_1\sigma_1\tau_1 - q_1\sigma_2\tau_2 - \sigma_3\tau_3], \\ \lambda^{(23)} &= \frac{r_3}{q_1}[q_1 + q_2].\end{aligned}\tag{4.152}$$

Finally we have

$$\begin{aligned}
\rho_s^{(231)} &= \frac{1}{4}[1 - \sigma_3\tau_3], \\
\rho_p^{(231)} &= \frac{1}{4}[1 - p_1\sigma_3 + p_1\tau_3 - q_1\sigma_1\tau_1 - q_1\sigma_2\tau_2 - \sigma_3\tau_3], \\
\lambda^{(231)} &= 2r_1.
\end{aligned} \tag{4.153}$$

From the three decompositions, we note that there is only one decomposition whose λ value is greater than the others. So one chooses the one with the largest λ_{\max} ,

$$\begin{aligned}
\rho_s^{(\max)} &= \frac{1}{4} \left(1 - \alpha \frac{p_1q_2 - p_2q_1}{q_1 + q_2} \sigma_3 - \alpha \frac{p_1q_2 + p_2q_1}{q_1 + q_2} \tau_3 + \alpha \frac{q_1q_2}{q_1 + q_2} \sigma_2\tau_2 + \beta \sigma_3\tau_3 \right), \\
\rho_p^{(\max)} &= \frac{1}{4} [1 - p_1\sigma_3 - p_1\tau_3 - q_1\sigma_1\tau_1 - q_1\sigma_2\tau_2 - \sigma_3\tau_3], \\
\lambda_{\max} &= 2r_1 + \frac{r_3}{q_1}[q_1 + q_2]
\end{aligned} \tag{4.154}$$

where

$$\alpha = \left[\frac{2r_1q_1}{r_3(q_1 + q_2)} + 1 \right]^{-1}, \quad \beta = \frac{1}{\lambda_{\max}} \left[r_3 \left(1 - \frac{q_2}{q_1} \right) - 2r_1 \right].$$

The eigenvalues of the separable part $\rho_s^{(\max)}$ are

$$\begin{aligned}
\nu_1 &= \frac{1}{2\lambda_{\max}} \left[2r_1 - r_3 \left(1 - \frac{q_2}{q_1} \right) \right], \\
\nu_2 &= \frac{1}{\lambda_{\max}} \left[r_1 + \frac{q_2}{q_1} r_3 \right], \\
\nu_3 &= \frac{1}{2\lambda_{\max}} \left[2r_1 + r_3 \left(1 - \frac{q_2}{q_1} \right) \right], \\
\nu_4 &= 0.
\end{aligned} \tag{4.155}$$

The positivity requires $\nu_1 > 0$, where ν_2 and ν_4 are positive. The eigenvalues for the partial transposition of ρ_s^{\max} are

$$\begin{aligned}
\tilde{\nu}_1 &= \frac{r_3}{2\lambda_{\max}}, \\
\tilde{\nu}_2 &= \frac{r_3}{\lambda_{\max}} \left[1 - \frac{q_2}{q_1} \right], \\
\tilde{\nu}_3 &= \frac{r_3}{2\lambda_{\max}} \left[1 + \frac{q_2}{q_1} \right], \\
\tilde{\nu}_4 &= 0.
\end{aligned} \tag{4.156}$$

These are all positive, so it is of rank-3 as $\rho_s^{(\max)}$. In the next step, we have to optimize this decomposition, i.e., we study the positivity of the state $\rho(\epsilon)$, and find the value of ϵ which makes the state

$$\rho(\epsilon) = \rho_s^{(\max)} + \epsilon \rho_p^{(\max)} \quad (4.157)$$

is still separable. According to the barely separable property of the LSD, if we find that $\rho(\epsilon)$ is non-separable for $\epsilon > 0$ this means that our decomposition (4.154) is the optimal one and $\lambda_{\max} = \mathcal{S}$ and $\rho_{\text{sep}}^{(\max)} = \varrho_s$. If for some values of ϵ , $\rho(\epsilon)$ is separable, then our decomposition (4.154) is not an optimal one and $\mathcal{S} = \lambda_{\max} + \epsilon$, $\varrho_s = \rho(\epsilon)$. The $\rho(\epsilon)$ is specified by:

$$\begin{aligned} \vec{s}(\epsilon) &\stackrel{\wedge}{=} [(1+\epsilon)(q_1+q_2)]^{-1} \left(0, 0, \alpha(p_2q_1 - q_1p_2) - \epsilon p_1(q_1+q_2) \right), \\ \vec{t}(\epsilon) &\stackrel{\wedge}{=} [(1+\epsilon)(q_1+q_2)]^{-1} \left(0, 0, \alpha(p_1q_2 + q_2p_1) + \epsilon p_1(q_1+q_2) \right), \\ \vec{\sigma} \cdot \vec{C}(\epsilon) \cdot \tau^\downarrow &= \frac{1}{1+\epsilon} \left[-\epsilon \sigma_1 \tau_1 + \left(\frac{\alpha q_1 q_2}{q_1+q_2} - \epsilon q_1 \right) \sigma_2 \tau_2 + (\beta - \epsilon) \sigma_z \tau_z \right]. \end{aligned} \quad (4.158)$$

The eigenvalues for $\rho^{\text{T}1}(\epsilon)$ are

$$\begin{aligned} \tilde{\nu}(\epsilon)_{1,2} &= 1 + \beta \pm \left| \frac{q_1}{q_1+q_2} \right| \sqrt{[2\epsilon(q_1+q_2) - \alpha q_2]^2 + \alpha^2(1-q_2)^2}, \\ \tilde{\nu}(\epsilon)_{3,4} &= 1 - \beta + 2\epsilon \pm \sqrt{\left(\frac{q_1 q_2}{q_1+q_2} \right)^2 + (1-q_1^2) \left[2\epsilon + \alpha \frac{q_2}{q_1+q_2} \right]^2}. \end{aligned} \quad (4.159)$$

Equating the smallest eigenvalue with zero to obtain a barely separable state one gets the value of ϵ ,

$$\epsilon = \frac{r_3}{\lambda_{\max}} \frac{q_2}{q_1} \left[1 + \sqrt{1 + 3 \left(\frac{r_3}{q_2} \right)^2} \right]. \quad (4.160)$$

The final value of λ is given by

$$\lambda_{\text{final}} = \lambda_{\max} + \epsilon. \quad (4.161)$$

In fact, one cannot say that this $\lambda_{\text{final}} = \mathcal{S}$, so one has to check its optimality. Also, since we are dealing with a rank-3 state, one cannot apply what is said in Section 4.2.3. Using the criterion of optimality given in Chapter 5, one can prove, however, that this decomposition is optimal indeed.

4.3.6 States of rank 4

The projector of the full rank 4 is the identity operator. The corresponding properly normalized statistical operator $\rho_{\text{chaos}} = \frac{1}{4}$ is the so-called ‘‘chaotic state’’ of the qubit pair. Consider the particular situation that we have a full rank case as a mixture of four orthogonal pure states,

$$\rho_{\text{rk4}} = r_1 \rho_{\text{p}}^{(1)} + r_3 \rho_{\text{p}}^{(3)} + r_3 \rho_{\text{p}}^{(3)} + r_2 \rho_{\text{p}}^{(4)}, \quad (4.162)$$

where $\rho_{\text{p}}^{(i)}$, $i = 1, 2, 3$ are given in (4.144), while $\rho_{\text{p}}^{(4)}$ is

$$\rho_{\text{p}}^{(4)} = \frac{1}{2}(1 - p_2 \sigma_3 - p_2 \tau_3 - q_2 \sigma_1 \tau_1 + q_2 \sigma_2 \tau_2 + \sigma_3 \tau_3). \quad (4.163)$$

To decompose this state, one uses the same method as in case of rank-3. This means one must obtain all the possible decompositions and its corresponding degree of separability. Compare between them, choose the one with largest decomposition and then perform the ϵ optimization. Table (4.2) gives all the possible decompositions for this case. From all those decompositions, there are some of them that have the same largest λ_{max} , those are the cases $[2 + 3] + [1] + [4]$, $[2 + 3] + [4] + [1]$, $[2 + 4] + [1] + [3]$, $[2 + 4] + [3] + [2]$. So we consider one of those decompositions, then we have

$$\begin{aligned} \rho_s^{\text{max}} &= \frac{1}{4} \left[1 + (\alpha v - \beta u) \sigma_3 + (\alpha u - \beta v) \tau_3 - \mu_1 \left(z_1 - \frac{z_2^2}{z_1} \right) \sigma_1 \tau_1 \right. \\ &\quad \left. - \mu_2 \left(z_1^2 - \frac{z_2^2}{z_1} \right) \sigma_2 \tau_2 + \mu_3 \sigma_2 \tau_3 \right], \\ \rho_{\text{p}} &= \frac{1}{4} \left[1 - (u - v) \sigma_3 - (v - u) \tau_3 - (z_1 + z_2) \sigma_1 \tau_1 - (z_1 + z_2) \sigma_2 \tau_2 - \sigma_3 \tau_3 \right], \\ \lambda_{\text{max}} &= \lambda^{(23)} + \lambda^{(231)} + \lambda^{(2314)}, \end{aligned} \quad (4.164)$$

with

Case: $[i + j] + [k] + [l]$	$\lambda^{(ij)}$	$\lambda^{(ijk)}$	$\lambda^{(ijkl)}$
$[1 + 2] + [3] + [4]$	$2r_2$	$\frac{r_3}{q_1}(q_1 + q_2)$	$\frac{r_4}{q_1}q_1 + q_2$
$[1 + 2] + [4] + [3]$	$2r_2$	$\frac{r_4}{q_1}(q_1 + q_2)$	$\frac{r_3}{q_1}(q_1 + q_2)$
$[1 + 3] + [2] + [4]$	$\frac{r_3}{q_1}(q_1 + q_2)$	$2r_2$	$\frac{r_4}{q_1}(q_1 + q_2)$
$[1 + 3] + [4] + [2]$	$\frac{r_3}{q_1}(q_1 + q_2)$	$\frac{r_4}{q_1}(q_1 + q_2)$	$2r_2$
$[1 + 4] + [2] + [3]$	$\frac{r_4}{q_1}(q_1 + q_2)$	$2r_2$	$\frac{r_3}{q_1}(q_1 + q_2)$
$[1 + 4] + [3] + [2]$	$\frac{r_4}{q_1}(q_1 + q_2)$	$\frac{r_3}{q_1}(q_1 + q_2)$	$2r_2$
$[2 + 3] + [1] + [4]$	$\frac{r_3}{q_1}(q_1 + q_2)$	$2r_1$	$\frac{r_4}{q_1}(q_1 + q_2)$
$[2 + 3] + [4] + [1]$	$\frac{r_3}{q_1}(q_1 + q_2)$	$\frac{r_4}{q_1}(q_1 + q_2)$	$2r_1$
$[2 + 4] + [1] + [3]$	$\frac{r_4}{q_1}(q_1 + q_2)$	$2r_1$	$\frac{r_3}{q_1}(q_1 + q_2)$
$[2 + 4] + [3] + [1]$	$\frac{r_4}{q_1}(q_1 + q_2)$	$\frac{r_3}{q_1}(q_1 + q_2)$	$2r_1$
$[3 + 4] + [1] + [2]$	$2r_4$	$\frac{r_1}{q_2}(q_1 + q_2)$	$\frac{r_2}{q_2}(q_1 + q_2)$
$[3 + 4] + [2] + [1]$	$2r_4$	$\frac{r_2}{q_2}(q_1 + q_2)$	$\frac{r_1}{q_2}(q_1 + q_2)$
$[1 + 2] + [3 + 4]$	$2r_2$	$\frac{r_4}{q_2}(q_1 + q_2)$	$\frac{r_3+r_4}{q_1} [(1 - 2r_4)(q_1 + q_2)]$
$[1 + 3] + [2 + 4]$	$\frac{r_3}{q_1}(q_1 + q_2)$	$\frac{r_4}{q_1}(q_1 + q_2)$	$\frac{r_2+r_4}{q_1} \left[1 - \frac{r_4}{q_1}(q_1 + q_2) \right]$
$[2 + 3] + [1 + 4]$	$\frac{r_4}{q_1}(q_1 + q_2)$	$\frac{r_3}{q_1}(q_1 + q_2)$	$\frac{r_2+r_3}{q_1} \left[1 - \frac{r_3}{q_1}(q_1 + q_2) \right]$

Table 4.2: These are different LSD's, each with a particular value of λ ; but there is only one optimal LSD with $\lambda^{(\text{opt})} = \mathcal{S}$.

$$\begin{aligned}
\alpha &= \frac{1}{\lambda_{\max}} \left[(r_3 - r_4) - \frac{q_2}{q_1} (r_3 + r_4) \right], \\
\beta &= \frac{1}{\lambda_{\max}} \left[(r_3 - r_4) + \frac{q_2}{q_1} (r_3 + r_4) \right], \\
\lambda^{(23)} &= \frac{r_3}{q_1} (q_1 + q_2), \\
\lambda^{(231)} &= \frac{r_4}{q_1} (q_1 + q_2), \\
\lambda^{(2314)} &= 2r_1. \\
\mu_1 &= \frac{\lambda^{(231)}}{\lambda_{\max}}, \\
\mu_2 &= \frac{\lambda^{(23)}}{\lambda_{\max}}, \\
\mu_3 &= \frac{1}{\lambda_{\max}} [\lambda^{(23)} + \lambda^{(231)} - \lambda^{(2314)}].
\end{aligned} \tag{4.165}$$

The eigenvalues of the partial transpoe for the ρ_{sep}^{\max} are

$$\begin{aligned}
\tilde{\nu}_{1,2} &= \frac{1}{2\lambda_{\max}} \left[r_1 \pm (r_3 - r_4) \sqrt{q_2^2 + p_1^2} \right], \\
\tilde{\nu}_{3,4} &= \frac{r_3 + r_4}{2\lambda_{\max}} \left[(q_1 + q_2) \pm q_2 \sqrt{q_1^2 + p_2^2} \right],
\end{aligned} \tag{4.166}$$

which are positive. For $r_4 = 0$ one obtains those for rank-3 case (4.155) also it is of rank-4, i.e., this separable state does not lie on the boundary of the set of separable states. This means that our decomposition is not optimal. So in the next step we have to optimize this decomposition as usual. The $\rho(\epsilon)$ is given by

$$\begin{aligned}
\rho(\epsilon) = \frac{1}{4} \left[1 + \frac{(\alpha - \beta)p_2 - (\alpha + \beta + 2\epsilon)p_1}{2(1 + \epsilon)} \sigma_3 + \frac{(\alpha + \beta + 2\epsilon)p_1 + (\alpha - \beta)p_2}{2(1 + \epsilon)} \tau_3 \right. \\
- \left(\frac{q_1}{q_1 + q_2} \right) \frac{\epsilon q_1 + (\mu_1 + \epsilon)q_2}{1 + \epsilon} \sigma_1 \tau_1 - \frac{q_1}{q_1 + q_2} \frac{\epsilon q_1 + (\mu_2 + \epsilon)q_2}{1 + \epsilon} \sigma_2 \tau_2 \\
\left. + \frac{\mu_3 - \epsilon}{1 + \epsilon} \sigma_3 \tau_3 \right].
\end{aligned} \tag{4.167}$$

Now, we study the positivity of $\rho(\epsilon)$, i.e., one find the value of ϵ at which $\rho(\epsilon)$ is still separable. So, we evaluate the eigenvalues of $\rho^{\text{T}_1}(\epsilon)$ and equating the smallest one with zero we obtain the value of ϵ which maximizes the value λ_{\max} ,

$$\epsilon = \frac{1}{\lambda_{\max}} \frac{(r_3 + r_4) \frac{q_2 - q_1}{q_1} - 2r_1}{1 + 4q_1 - 4q_1^2} \left[1 + q_1 + \sqrt{(q_1^2 + 2q_1) + \frac{(r_3 + r_4)^2 - 4r_3 r_4 q_1^2}{[(r_3 + r_4) \frac{q_2 - q_1}{q_1} - 2r_1]^2}} \right]. \tag{4.168}$$

Now $\rho^{\text{T}_1}(\epsilon)$ has only three non-zero eigenvalues, i.e., its rank is 3. So this decomposition is an optimal one where the pure state is not a Bell state [43]. Also, as we shall see from Chapter 5, this decomposition is optimal.

Chapter 5

Optimality of decompositions

Sections 4.2.1 and 4.2.2 describe a method to get the optimal decomposition. This method depends on the separable part. If the separable part of a given decomposition is of rank 4, then one can obtain analytically the optimal LSD by solving one of the two equations (4.37). If the separable part has a reduced rank, then one has to solve the two eigenvalue equations (4.50), (4.51), but cannot decide if this decomposition is the optimal one or not. In this chapter I show how one can check the optimality of a given decomposition. This method depends in the infinitesimal changes in the separability inequalities (3.13).

5.1 Infinitesimal changes and optimality

In this section we study the infinitesimal changes in the separability criteria (3.13). This requires evaluating the infinitesimal changes in the three numbers A_2, A_1, A_0 which are given by (3.6) as well as $\det \{\overline{C}\}$ and $\det \{\overline{E}\}$ which are given by (1.11) and (2.4) respectively. In Section 5.1.1, we give a general formula of the infinitesimal changes for any two-qubit state. In Section 5.1.2, we construct a criteria for checking if a LSD is optimal or not.

5.1.1 Infinitesimal unitary transformations

The infinitesimal changes in a 2-qubit state ρ (1.10) require evaluating $\delta\vec{s}$, δt^\downarrow and $\delta\overline{C}$. So consider that we have a generator \mathcal{G} ,

$$\mathcal{G} = g_1^\downarrow \cdot \sigma^\downarrow + \vec{\tau} \cdot g_2^\downarrow + \vec{\sigma} \cdot \overline{G} \cdot \tau^\downarrow \quad (5.1)$$

where \vec{g}_1, \vec{g}_2 and \overleftarrow{G} are infinitesimal. The infinitesimal changes in \vec{s}, t^\downarrow and \overleftarrow{C} are given by

$$\begin{aligned} \delta\vec{s} \cdot \sigma^\downarrow + \vec{\tau} \cdot \delta t^\downarrow + \vec{\sigma} \cdot \delta\overleftarrow{C} \cdot \tau^\downarrow \\ = -\frac{i}{2} \left[\vec{g}_1 \cdot \sigma^\downarrow + \vec{g}_2 \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftarrow{G} \cdot \tau^\downarrow, \vec{s} \cdot \sigma^\downarrow + \vec{t} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftarrow{C} \cdot \tau^\downarrow \right]. \end{aligned} \quad (5.2)$$

In explicit forms we have

$$\begin{aligned} \delta\vec{s} &= \vec{g}_1 \times \vec{s} + \sum_{k=1}^3 \vec{e}_k \cdot \text{Sp} \left\{ e_k^\downarrow \times \overleftarrow{G} \cdot \overleftarrow{C}^T \right\}, \\ \delta t^\downarrow &= g_2^\downarrow \times t^\downarrow + \sum_{k=1}^3 n_k^\downarrow \cdot \text{Sp} \left\{ \overleftarrow{G}^T \cdot \overleftarrow{C} \times \vec{n}_k \right\}, \\ \delta\overleftarrow{C} &= g_1^\downarrow \times \overleftarrow{C} - \overleftarrow{C} \times \vec{g}_2 - s^\downarrow \times \overleftarrow{G} + \overleftarrow{G} \times \vec{t}. \end{aligned} \quad (5.3)$$

As an example, for the pure state defined by (2.14), one finds there are 6 relevant generators of the infinitesimal changes. Table 5.1 shows the generators and its corresponding effect.

Generators	Changes
$\sigma_2 - \tau_2$	$p(\sigma_3 + \tau_3) + (1 + q)(\sigma_1\tau_3 - \sigma_3\tau_3)$
$\sigma_3 - \tau_3$	$p(\sigma_2 + \tau_2) + (1 + q)(\sigma_1\tau_2 - \sigma_2\tau_1)$
$q(\sigma_1 - \tau_1) + p(\sigma_2\tau_2 + \sigma_3\tau_3)$	$\sigma_2\tau_3 - \sigma_3\tau_2$
$\sigma_2\tau_3 - \sigma_3\tau_2$	$q(\sigma_1 - \tau_1) + p(\sigma_2\tau_2 + \sigma_3\tau_3)$
$\sigma_3\tau_1 - \sigma_1\tau_3$	$(1 + q)(\sigma_2 - \tau_2) - p(\sigma_1\tau_2 + \sigma_2\tau_1)$
$\sigma_1\tau_2 - \sigma_2\tau_1$	$(1 + q)(\sigma_3 - \tau_3) - p(\sigma_1\tau_3 + \sigma_3\tau_1)$

Table 5.1: Generators and their corresponding changes of ρ_p .

To evaluate the first and second order infinitesimal unitary transformation of a pure state, one notes that for this case one needs 7 parameters; one for the change of p , three for the change of $(e_1^\downarrow, e_2^\downarrow, e_3^\downarrow)$ and three for the change of $(n_1^\downarrow, n_2^\downarrow, n_3^\downarrow)$. The change of p is effected by a transformation like e^{iA} with $A = \frac{\gamma}{4}(\sigma_2\tau_3 - \sigma_3\tau_2)$, but the rotations of the local unit vectors are effected by e^{iB} with $B = \frac{1}{2}\vec{\alpha} \cdot \sigma^\downarrow + \frac{1}{2}\vec{\beta} \cdot \tau^\downarrow$. Up to the second order we have

$$\begin{aligned} \rho + \delta_1\rho + \delta_2\rho &= \rho - i[A + B, \rho] \\ &\quad - \frac{1}{2}[A, [A, \rho]] - [B, [A, \rho]] - \frac{1}{2}[B, [B, \rho]]. \end{aligned} \quad (5.4)$$

An explicit form for the first order changes $\delta_1\rho$ is specified by

$$\begin{aligned}\delta_1 s^\downarrow &= \alpha^\downarrow \times s^\downarrow - q\gamma e_1^\downarrow, \\ \delta_1 \vec{t} &= -\vec{t} \times \vec{\beta} + q\gamma \vec{n}_1, \\ \delta_1 \overleftarrow{C} &= \alpha^\downarrow \times \overleftarrow{C} - \overleftarrow{C} \times \vec{\beta} - p\gamma(e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3).\end{aligned}\quad (5.5)$$

For the second order $\delta_2\rho$,

$$\begin{aligned}2\delta_2 s^\downarrow &= \alpha^\downarrow \times (\alpha^\downarrow \times s^\downarrow) - 2q\gamma \alpha^\downarrow \times e_1^\downarrow - \gamma^2 s^\downarrow, \\ 2\delta_2 \vec{t} &= (\vec{t} \times \vec{\beta}) \times \vec{\beta} - 2q\gamma \vec{n}_1 \times \vec{\beta} - \gamma^2 \vec{t}, \\ 2\delta_2 \overleftarrow{C} &= \alpha^\downarrow \times (\alpha^\downarrow \times \overleftarrow{C}) - 2\alpha^\downarrow \times \overleftarrow{C} \times \vec{\beta} + (\overleftarrow{C} \times \vec{\beta}) \times \vec{\beta} \\ &\quad - 2p\gamma[\alpha^\downarrow \times (e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3) - (e_2^\downarrow \vec{n}_2 + e_3^\downarrow \vec{n}_3) \times \vec{\beta}] \\ &\quad - \gamma^2(\overleftarrow{C} + e_1^\downarrow \vec{n}_1).\end{aligned}\quad (5.6)$$

As a simple and important example, consider the infinitesimal changes in Bell states. Since they have $\vec{s} = \vec{t} = 0$, one can not distinguish the directions of e_1^\downarrow and n_1^\downarrow , for example, from the others, so one can consider the following generator

$$A = \frac{1}{4}[\gamma_1(\sigma_2\tau_3 - \sigma_3\tau_2) + \gamma_2(\sigma_3\tau_1 - \sigma_1\tau_3) + \gamma_3(\sigma_1\tau_2 - \sigma_2\tau_1)].\quad (5.7)$$

Then the infinitesimal changes for the first order of $\delta_1\rho$ are

$$\delta_1 s^\downarrow = -\gamma^\downarrow, \quad \delta_1 \vec{t} = \vec{\gamma} \cdot \overleftarrow{O}, \quad \delta_1 \overleftarrow{C} = -\alpha^\downarrow \times \overleftarrow{O} + \overleftarrow{O} \times \vec{\beta}.\quad (5.8)$$

For the second order one just evaluates (5.6) with $p = 0$ and $q = 1$, then

$$\begin{aligned}\delta_2 s^\downarrow &= -\alpha^\downarrow \times \gamma^\downarrow, \quad \delta_2 \vec{t} = -\vec{\gamma} \cdot \overleftarrow{O} \times \vec{\beta}, \\ \delta_2 \overleftarrow{C} &= -\frac{1}{2}\alpha^\downarrow \times (\alpha^\downarrow \times \overleftarrow{O}) + \alpha^\downarrow \times \overleftarrow{O} \times \vec{\beta} - \frac{1}{2}(\overleftarrow{O} \times \vec{\beta}) \times \vec{\beta} \\ &\quad - \frac{1}{2}\gamma^\downarrow \times (\gamma^\downarrow \times \overleftarrow{O}).\end{aligned}\quad (5.9)$$

5.1.2 Checking the optimality of a decomposition

If a state is separable or not could be checked by evaluating the three numbers A_2 , A_1 and A_0 , as well as $\det\{\overleftarrow{C}\}$ and $\det\{\overleftarrow{E}\}$. These values are used to check the two inequalities (3.13); if they are obeyed then the state in question is separable, if one of them or both are violated, then the state is non-separable. One can use the infinitesimal changes of those inequalities to check if a given LSD is optimal one or not. We saw that one of the properties of the optimal

decomposition, the state $\varrho_s + (1/\mathcal{S} - 1)(\varrho - \rho_p)$ is either non-positive or non-separable for each $\rho_p \neq \varrho$. This property is read as: A given decomposition is optimal if

$$\begin{aligned}\delta \left(A_2 - A_1 + A_0 - 16 \det \left\{ \overline{E} \right\} \right) &\geq 0, \\ \delta \left(2A_2 - A_1 - 16 \det \left\{ \overline{C} \right\} \right) &\geq 0.\end{aligned}\quad (5.10)$$

Now we write these inequalities in explicit forms of δA_2 , δA_1 , δA_0 and $\delta \left(\det \left\{ \overline{C} \right\} \right)$, $\delta \left(\det \left\{ \overline{E} \right\} \right)$.

For this aim, assume that we are given a decomposition of the form,

$$\rho = \lambda \rho_s + (1 - \lambda) \rho_p, \quad (5.11)$$

with

$$\begin{aligned}\rho &= \frac{1}{4}(1 + \vec{s} \cdot \sigma^\downarrow + \vec{\tau} \cdot t^\downarrow + \vec{\sigma} \cdot \overline{C} \cdot \tau^\downarrow), \\ \rho_s &= \frac{1}{4}(1 + \vec{s}_0 \cdot \sigma^\downarrow + \vec{\tau} \cdot t_0^\downarrow + \vec{\sigma} \cdot \overline{C}_0 \cdot \tau^\downarrow), \\ \rho_p &= \frac{1}{4}(1 + \vec{s}_p \cdot \sigma^\downarrow + \vec{\tau} \cdot t_p^\downarrow + \vec{\sigma} \cdot \overline{C}_p \cdot \tau^\downarrow).\end{aligned}\quad (5.12)$$

Appendix C.2, gives the local invariants under the changes of \vec{s}, t^\downarrow and \overline{C} for the first and the second order. Using those invariants together with equations (3.6), one obtains for the first order changes:

$$\begin{aligned}\frac{1}{4}\delta A_2 &= \delta \vec{s}_p \cdot s_0^\downarrow + \vec{t}_0 \cdot \delta t_p^\downarrow + \text{Sp} \left\{ \delta \overline{C}_p^T \cdot \overline{C} \right\}, \\ \frac{1}{8}\delta A_1 &= \delta \vec{s}_p \cdot \overline{C}_0 \cdot t_0^\downarrow + \vec{s}_0 \cdot \overline{C}_0 \cdot \delta t_p^\downarrow + \text{Sp} \left\{ \delta \overline{C}^T \cdot (s^\downarrow \vec{t} - \overline{C}_{\text{sub}}) \right\}, \\ \frac{1}{4}\delta A_0 &= \delta \vec{s}_p \cdot \left[2\overline{C}_0 \cdot \overline{C}_0^T \cdot s_0^\downarrow - 2\overline{C}_{0\text{sub}} \cdot t_0^\downarrow - s^\downarrow \left(\text{Sp} \left\{ \overline{C}_0 \cdot \overline{C}_0^T \right\} + s_0^2 - t_0^2 \right) \right] \\ &\quad + \left[2\vec{t}_0 \overline{C}_0^T \cdot \overline{C} - 2\vec{s}_0 \cdot \overline{C}_{0\text{sub}} - \left(\text{Sp} \left\{ \overline{C}_0^T \cdot \overline{C}_0 \right\} + t_0^2 - s_0^2 \right) \vec{t}_0 \right] \cdot \delta t_p^\downarrow \\ &\quad + \text{Sp} \left\{ \delta \overline{C}_p^T \cdot \left[\overline{C}_0 \left(\text{Sp} \left\{ \overline{C}_0^T \cdot \overline{C}_0 \right\} - s_0^2 - t_0^2 \right) - 2\overline{C}_0 \cdot \overline{C}_0^T \cdot \overline{C}_0 \right. \right. \\ &\quad \left. \left. + s_0^\downarrow \vec{s}_0 \cdot \overline{C}_0 + 2\overline{C}_0 \cdot t_0^\downarrow \vec{t}_0 + 2s_0^\downarrow \times \overline{C}_0 \times \vec{t}_0 \right] \right\},\end{aligned}\quad (5.13)$$

where $\delta \vec{s}_p$, δt_p^\downarrow and $\delta \overline{C}_p$ could be evaluated from (5.3) and (5.12). Using these variations one can obtain the first order response of $A_2 - A_1 + A_0$ and $2A_2 - A_1$

variations as:

$$\begin{aligned}
\frac{1}{4}\delta(A_2 - A_1 + A_0) &= \delta\vec{s}_p \cdot \left[s_0^\downarrow \left(1 - \text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0 \cdot \overleftarrow{\mathcal{C}}_0^T \right\} - s_0^2 + t_0^2 \right) \right. \\
&\quad - 2 \left(\overleftarrow{\mathcal{C}}_0 + \overleftarrow{\mathcal{C}}_{0\text{sub}} \right) \cdot t_0^\downarrow + 2\overleftarrow{\mathcal{C}}_0 \cdot \overleftarrow{\mathcal{C}}_0^T \cdot s_0^\downarrow \left. \right] \\
&\quad + \left[\left(1 - \text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0^T \cdot \overleftarrow{\mathcal{C}}_0 \right\} - t_0^2 + s_0^2 \right) \vec{t}_0 \right. \\
&\quad - 2\vec{s}_0 \cdot \left(\overleftarrow{\mathcal{C}}_0 + \overleftarrow{\mathcal{C}}_{0\text{sub}} \right) + 2\vec{t}_0 \cdot \overleftarrow{\mathcal{C}}_0^T \cdot \overleftarrow{\mathcal{C}}_0 \left. \right] \cdot \delta t_p^\downarrow \\
&\quad + \text{Sp} \left\{ \delta \overleftarrow{\mathcal{C}}_p^T \cdot \left[\overleftarrow{\mathcal{C}}_0 \left(1 + \text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0^T \cdot \overleftarrow{\mathcal{C}}_0 \right\} - s_0^2 - t_0^2 \right) \right. \right. \\
&\quad - 2\overleftarrow{\mathcal{C}}_0 \cdot \overleftarrow{\mathcal{C}}_0^T \cdot \overleftarrow{\mathcal{C}}_0 + 2s_0^\downarrow \vec{s}_0 \cdot \overleftarrow{\mathcal{C}}_0 + 2\overleftarrow{\mathcal{C}}_0 \cdot t_0^\downarrow \vec{t}_0 \\
&\quad \left. \left. + 2s_0^\downarrow \times \overleftarrow{\mathcal{C}}_0 \times \vec{t}_0 - 2s_0^\downarrow \vec{t}_0 + 2\overleftarrow{\mathcal{C}}_{0\text{sub}} \right] \right\}, \\
\frac{1}{8}\delta(2A_2 - A_1) &= \delta\vec{s}_p \cdot \left(s_0^\downarrow - \overleftarrow{\mathcal{C}}_0 \cdot t_0^\downarrow \right) + \left(\vec{t}_0 - \vec{s}_0 \cdot \overleftarrow{\mathcal{C}} \right) \cdot \delta t_p^\downarrow \\
&\quad + \text{Sp} \left\{ \delta \overleftarrow{\mathcal{C}}_p^T \cdot \left(\overleftarrow{\mathcal{C}}_0 + \overleftarrow{\mathcal{C}}_{0\text{sub}} - s_0^\downarrow \vec{t}_0 \right) \right\}. \tag{5.14}
\end{aligned}$$

Also, the infinitesimal changes in $\det \left\{ \overleftarrow{\mathcal{C}} \right\}$ and $\det \left\{ \overleftarrow{E} \right\}$ are

$$\begin{aligned}
\delta \left(\det \left\{ \overleftarrow{\mathcal{C}} \right\} \right) &= \text{Sp} \left\{ \delta \overleftarrow{\mathcal{C}}_p^T \cdot \overleftarrow{\mathcal{C}}_{0\text{sub}} \right\}, \\
\delta \left(\det \left\{ \overleftarrow{E} \right\} \right) &= \text{Sp} \left\{ \left(t_0^\downarrow \times \delta \overleftarrow{\mathcal{C}}_p \times \vec{s}_0 \right) \cdot \overleftarrow{\mathcal{C}}_0 \right\}. \tag{5.15}
\end{aligned}$$

Now, everything is at hand, and one can check the inequalities (5.10). In what follows, two examples are given to see how this procedure works.

5.1.3 Examples

1-First order changes for Werner state: In Appendix C.1, the response of the local invariants for Werner state is derived. One easily uses them to evaluate (5.14) and (5.15). For the first order one gets

$$\begin{aligned}
\delta A_2 &= 4 \text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0^T \cdot \delta_1 \overleftarrow{\mathcal{C}}_p \right\}, \\
\delta A_1 &= -8 \text{Sp} \left\{ \delta_1 \overleftarrow{\mathcal{C}}_p^T \cdot \overleftarrow{\mathcal{C}}_{0\text{sub}} \right\}, \\
\delta A_0 &= 4 \left(\text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0^T \cdot \delta_1 \overleftarrow{\mathcal{C}}_p \right\} \right)^2 - 8 \text{Sp} \left\{ \overleftarrow{\mathcal{C}}_0^T \cdot \overleftarrow{\mathcal{C}}_0 \cdot \overleftarrow{\mathcal{C}}_0^T \cdot \delta_1 \overleftarrow{\mathcal{C}}_p^T \right\}, \tag{5.16}
\end{aligned}$$

where δ_1 is the first order changes. Then the two inequalities (5.10) are

$$\begin{aligned} \delta_1(A_2 - A_1 + A_0 - 16 \det \{\overline{E}\}) &= 4 \text{Sp} \left\{ \overline{C}_0^T \cdot \delta_1 \overline{C}_p \right\} + 4 \left(\text{Sp} \left\{ \overline{C}_0^T \cdot \delta_1 \overline{C}_p \right\} \right)^2 \\ &\quad + 8 \text{Sp} \left\{ \overline{C}_0^T \cdot \overline{C}_0 \cdot \overline{C}_0^T \cdot \delta_1 \overline{C}_p^T \right\}, \\ \delta_1(A_2 - A_1 - 16 \det \{\overline{C}\}) &= 8 \text{Sp} \left\{ \delta_1 \overline{C}_p^T \cdot \left(\overline{C}_0 - \overline{C}_{0\text{sub}} \right) \right\}. \end{aligned} \quad (5.17)$$

For this case, $\delta_1 \overline{C}$ results from varying the associated Bell state, it is given by (5.5). The two-right-hand sides of inequalities (5.17) vanish if the generalized Werner state is barely separable, that is

$$\overline{C} = - \sum_{k=1}^3 e_k^\downarrow c_k \vec{n}_k = \begin{cases} -\overline{O}_{en} \cdot \sum_{k=1}^3 n_k^\downarrow c_k \vec{n}_k \\ - \sum_{k=1}^3 e_k^\downarrow c_k \vec{e}_k \cdot \overline{O}_{en} \end{cases} \quad (5.18)$$

with $c_1 \geq c_2 \geq c_3 \geq 0$ and $c_1 + c_2 + c_3 = 1$.

2-Rank “2+2” case: This case is given by (4.128), it is decomposed to its separable part, which is specified by

$$\begin{aligned} \vec{s}_0 \cdot \sigma^\downarrow &= (\alpha u + \beta v) \sigma_3, \\ \vec{\tau} \cdot t_0^\downarrow &= (\alpha v + \beta u) \tau_3, \\ \vec{\sigma} \cdot \overline{C}_0 \cdot \tau^\downarrow &= (\alpha z_1 + \beta z_2) \sigma_1 \tau_1 + (\alpha z_1 - \beta z_2) \sigma_2 \tau_2 + \beta \sigma_3 \tau_3, \end{aligned} \quad (5.19)$$

where α and β are given by (4.132), while the pure part is defined by

$$\begin{aligned} \vec{s}_p \cdot \sigma^\downarrow &= (u - v) \sigma_3, \\ \vec{\tau} \cdot t_p^\downarrow &= (v - u) \tau_3, \\ \vec{\sigma} \cdot \overline{C}_p \cdot \tau^\downarrow &= (z_1 + z_2) \sigma_1 \tau_1 + (z_1 - z_2) \sigma_2 \tau_2 - \sigma_3 \tau_3. \end{aligned} \quad (5.20)$$

For simplicity let us consider the variance of the infinitesimal changes independently. For example let us consider the changes from \vec{g}_1 only. In this case, (5.3) reduces to

$$\delta \vec{s}_p = \vec{g}_1 \times \vec{s}_p, \quad \delta \vec{t}_p = 0, \quad \delta \overline{C}_p = g_1^\downarrow \times \overline{C}_p. \quad (5.21)$$

Now the variations in A_2, A_1 and A_0 are given by

$$\begin{aligned}
\frac{1}{4}\delta A_2 &= \vec{g}_1 \cdot (s^\downarrow_p \times s_0^\downarrow) + \text{Sp} \left\{ \overline{C}_p \cdot \overline{C}_0 \times \vec{g}_1 \right\}, \\
\frac{1}{8}\delta A_1 &= g_1^\downarrow \cdot (s^\downarrow_p \times \overline{C}_0 \cdot t_0^\downarrow) + \text{Sp} \left\{ \overline{C}_p^T \cdot (t_0^\downarrow \vec{s}_0 - \overline{C}_{0\text{sub}}^T) \times \vec{g}_1 \right\}, \\
\frac{1}{4}\delta A_0 &= \vec{g}_1 \times \vec{s}_p \cdot \left[2\overline{C}_0 \cdot \overline{C}_0^T \cdot s_0^\downarrow - 2\overline{C}_{0\text{sub}} \cdot t_0^\downarrow - s^\downarrow \cdot \left(\text{Sp} \left\{ \overline{C}_0 \cdot \overline{C}_0^T \right\} + s^2 - t^2 \right) \right] \\
&\quad + \text{Sp} \left\{ \overline{C}_p^T \cdot \left[\overline{C}_0 \left(\text{Sp} \left\{ \overline{C}_0^T \cdot \overline{C}_0 \right\} - s_0^2 - t_0^2 \right) - 2\overline{C}_0 \cdot \overline{C}_0^T \cdot \overline{C}_0 \right. \right. \\
&\quad \left. \left. - s_0^\downarrow \vec{s}_0 \cdot \overline{C}_0 + 2\overline{C}_0 \cdot t_0^\downarrow \vec{t}_0 \right] \right\}. \quad (5.22)
\end{aligned}$$

Also, $\delta(\det \left\{ \overline{C} \right\})$ and $\delta(\det \left\{ \overline{E} \right\})$ are

$$\begin{aligned}
\delta(\det \left\{ \overline{C} \right\}) &= \text{Sp} \left\{ \overline{C}_p \cdot \overline{C}_{0\text{sub}}^T \times g_1^\downarrow \right\}, \\
\delta(\det \left\{ \overline{E} \right\}) &= \text{Sp} \left\{ \overline{C}_p \cdot \overline{C}_{0\text{sub}} \times g_1^\downarrow \right\} - \vec{g}_1 \times \vec{s}_p \cdot \overline{C}_{0\text{sub}} \cdot t_0^\downarrow, \\
&\quad + \text{Sp} \left\{ \vec{g}_1 \times \left(\vec{t}_0 \times \overline{C}_0 \times \vec{s}_0 \cdot \overline{C}_0 \right) \right\}. \quad (5.23)
\end{aligned}$$

Using (5.19) and (5.20), one gets

$$\delta A_2 = \delta A_1 = \delta A_0 = 0, \quad \delta \left(\det \left\{ \overline{C} \right\} \right) = \delta \left(\det \left\{ \overline{E} \right\} \right) = 0. \quad (5.24)$$

The same result is obtained if one consider the changes from \vec{g}_2 only or \overline{G} only. Finally one can say that the decomposition of the rank “2+2” case with its separable part (5.19) and its pure part (5.20) is the optimal decomposition.

3-Some special examples

1. Assume that one can decompose a give state ρ of rank-4 into its separable and pure part such that:

$$\rho = \lambda \rho_s + (1 - \lambda) \rho_{\text{Bell}} \quad (5.25)$$

where ρ_s is given by (5.12). One can see that this decomposition obeys the criterion of optimality (5.10) and $\lambda = \mathcal{S}$. The same result is true for rank-3 state. This coincides with the remarks of [43, 44].

2. If one has a decomposition such that ρ_s is of rank-3 and the pure part is not a Bell state. In this case $\rho_s^{\text{T}2}$ may be of rank-2 or rank-3 so one cannot say that this decomposition is optimal or not. In Chapter 4, we give two examples satisfying this property. Consider the particular state which is defined by

(4.136) and (4.144). The final decomposition of this state is specified by its separable part (4.158) and the pure state of (4.154). A straightforward calculation shows that this decomposition obeys the two inequalities (5.10), so it is the optimal one. The other particular example is of rank-4. In this case the final decomposition is defined by its separable part (4.167) and the pure part of (4.164). One can check that this decomposition obeys the optimality conditions

Chapter 6

Purification and degree of separability

In this chapter, the dynamical variables are used to describe the IBM and Oxford protocols at the relevant example of the so-called “generalized Werner state of the first kind” [19] or Bell-diagonal states or “self transposed state” [32]. An alternative version of the Oxford protocol is introduced, which is more efficient than the original one. The two variants of the Oxford protocol are investigated for states of two kinds, binary states and the more general Bell-diagonal states.

6.1 Introduction

Some quantum communication proposals require maximally entangled qubit pairs to perform them. Due to the noisy channels between the sender station and the receiver station, the pairs lose their fidelity partially; dissipative effects of the environment turn pure states into mixed states. Fidelity is defined as the maximum overlap of the density operator of a pair of qubits with the wanted maximally entangled state. Consequently there is no guarantee that the transmission process of information between the two stations is performed faithfully. The aim is then to purify these states to obtain maximally entangled states. The entanglement purification is often required. It distills a small number of strongly entangled pairs of qubits from a larger number of weakly entangled pairs, by using local quantum operations, classical communications, and measurements.

The first entanglement purification protocol, called IBM protocol, has been given by Bennett *et al.* [10, 14]. It enables one to distill from a large ensemble of entangled states with fidelity greater than 0.5 a smaller ensemble of pairs with fidelity close to unity. Those purified pairs could be used for faithful teleportation [14]. Also Deutsch *et al.* [53] have formulated another protocol designed for cryptographic purposes; it is called “quantum privacy amplification”, or “Oxford protocol” for short.

If one starts with an infinite number of non-separable states, then the purified pairs are maximally entangled states, if all local operations and measurements are perfect. Purification under imperfect operations is studied by Giedke *et al.* [54], who obtain the lower bound for the fidelity, such that purification is possible in the presence of noise.

6.2 Local unitary transformation

Before performing the IBM and Oxford protocols in terms of dynamical variables, one needs to describe the operations available to Alice and Bob [55]. It turns out that there are three types of operations:

1. Unilateral rotations: These operations map the Bell state onto another leaving no Bell state unchanged. It is a rotation by π about x, y or z axis, namely

$$\begin{aligned} U_{1x} &= \sigma_x, & U_{1y} &= \sigma_y, & U_{1z} &= \sigma_z, \\ U_{2x} &= \tau_x, & U_{2y} &= \tau_y, & U_{2z} &= \tau_z, \end{aligned} \quad (6.1)$$

where U_1 and U_2 for the first and second qubit respectively.

2. Bilateral rotations: Those operations are performed on both particles in a pair about x, y and z axis. In this case Alice and Bob both perform the same rotations on their qubit. These operations are defined by the unitary operators

$$\begin{aligned} B_x &= \frac{1}{2}(1 + i\sigma_x)(1 + i\tau_x), \\ B_y &= \frac{1}{2}(1 + i\sigma_y)(1 + i\tau_y), \\ B_z &= \frac{1}{2}(1 + i\sigma_z)(1 + i\tau_z). \end{aligned} \quad (6.2)$$

3. Bilateral controlled NOT (BCNOT): In this operation, both members of one pair are used as source qubits and both qubits from another pair are used as target qubits. In dynamical variables it is defined by

$$\begin{aligned} BCNOT(\sigma_\mu^{(1)}\sigma_\nu^{(2)}) &= \frac{1 + \sigma_z^{(1)}}{2}\sigma_\mu^{(1)}\frac{1 + \sigma_z^{(2)}}{2}\sigma_\nu^{(2)} \\ &+ \frac{1 + \sigma_z^{(1)}}{2}\sigma_\mu^{(1)}\frac{1 - \sigma_z^{(2)}}{2}\sigma_x^{(2)}\sigma_\nu^{(2)} \\ &+ \frac{1 - \sigma_z^{(1)}}{2}\sigma_\mu^{(1)}\frac{1 + \sigma_z^{(2)}}{2}\sigma_\nu^{(2)}\sigma_x^{(2)} \\ &+ \frac{1 - \sigma_z^{(1)}}{2}\sigma_\mu^{(1)}\frac{1 - \sigma_z^{(2)}}{2}\sigma_x^{(2)}\sigma_\nu^{(2)}\sigma_x^{(2)} \end{aligned} \quad (6.3)$$

where the suffixes 1 and 2 refer to the first and the second qubit. Table 6.1 shows the effect of the BCNOT operation on the two qubits, that specify $\sigma_\mu^{(1)}$ and $\sigma_\mu^{(2)}$.

	$1^{(2)}$	$\sigma_x^{(2)}$	$\sigma_y^{(2)}$	$\sigma_z^{(2)}$
$1^{(1)}$	1	$\sigma_x^{(1)} \sigma_x^{(2)}$	$\sigma_y^{(1)} \sigma_x^{(2)}$	$\sigma_z^{(1)}$
$\sigma_x^{(1)}$	$\sigma_x^{(2)}$	$\sigma_x^{(1)}$	$\sigma_y^{(1)}$	$\sigma_z^{(1)} \sigma_x^{(2)}$
$\sigma_y^{(1)}$	$\sigma_z^{(1)} \sigma_y^{(2)}$	$\sigma_y^{(1)} \sigma_z^{(2)}$	$-\sigma_x^{(1)} \sigma_z^{(2)}$	$\sigma_y^{(2)}$
$\sigma_z^{(1)}$	$\sigma_z^{(1)} \sigma_z^{(2)}$	$-\sigma_y^{(1)} \sigma_y^{(2)}$	$\sigma_x^{(1)} \sigma_y^{(2)}$	$\sigma_z^{(2)}$

Table 6.1: Bilateral CNOT operation between the two qubits which define $\sigma_\mu^{(1)}$ and $\sigma_\nu^{(2)}$. The same table applies for the two qubits $\tau_\mu^{(1)}$ and $\tau_\nu^{(2)}$, where $\mu, \nu = x, y$ and z .

6.3 IBM protocol

This protocol, which is known also as BBPSSW protocol, still remains the most transparent example of distillation. It works for the two-qubit states where it allows one to distill from a large ensemble of entangled states with fidelity greater than $1/2$, a smaller ensemble of pairs with fidelity arbitrarily close to unity. Each state in this ensemble takes the following form

$$\rho = \frac{1}{4} \left[1 + \frac{1-4F}{3} (\sigma_x \tau_x + \sigma_y \tau_y + \sigma_z \tau_z) \right], \quad (6.4)$$

with a fidelity $F = \text{tr} \{ \rho \rho_{\psi^-} \}$, where

$$\rho_{\psi^-} = \frac{1}{4} (1 - \sigma_x \tau_x - \sigma_y \tau_y - \sigma_z \tau_z). \quad (6.5)$$

To perform this protocol Alice and Bob do the following steps:

1. Alice and Bob pick up two states from this ensemble. Then one of them Alice (or Bob) applies a unilateral transformation on each her (his) pairs of qubits. This operation transform the state (6.4), to an equivalent one with fidelity $F = \text{tr} \{ \rho \rho_{\text{ideal}} \}$ where

$$\rho_{\text{ideal}} = \frac{1}{4} (1 + \sigma_x \tau_x - \sigma_y \tau_y + \sigma_z \tau_z). \quad (6.6)$$

After this operation the two states are,

$$\begin{aligned}\rho_1 &= \frac{1}{4} \left[1 - \frac{1-4F}{3} (\sigma_x^{(1)}\tau_x^{(1)} - \sigma_y^{(1)}\tau_y^{(1)} + \sigma_z^{(1)}\tau_z^{(1)}) \right], \\ \rho_2 &= \frac{1}{4} \left[1 - \frac{1-4F}{3} (\sigma_x^{(2)}\tau_x^{(2)} - \sigma_y^{(2)}\tau_y^{(2)} + \sigma_z^{(2)}\tau_z^{(2)}) \right].\end{aligned}\quad (6.7)$$

2. They perform the BCNOT from one pair to the other, followed by measuring the target qubits in the computational basis. If the outcomes coincide i.e., both spin up or both spin down, they keep the control pairs and discard the target pair, but if the outcomes do not coincide both pairs are discarded. Finally,

$$\rho_{\text{new}} = \frac{1}{4} \left[1 + 2\frac{y^2}{N}\sigma_x\tau_x - 2\frac{y^2}{N}\sigma_y\tau_y - 2\frac{y}{N}\sigma_z\tau_z \right] \quad (6.8)$$

with $y = \frac{1-4F}{3}$ and $N = 1 + y^2$. The new fidelity is given by

$$F_{\text{new}} = \text{tr} \{ \rho_{\text{new}} \rho_{\text{ideal}} \} = \frac{1 - 2y + 5y^2}{4(1 + y^2)}, \quad (6.9)$$

which is the same as in the original protocol.

Since the function $F(F_{\text{new}})$ is continuous, $F_{\text{new}} > F$ for $F > \frac{1}{2}$ and $F_{\text{new}}(1) = 1$, one obtains that, by iterating the procedure, Alice and Bob can obtain states with arbitrarily high fidelity F . It is clear that the larger F is required, the more pairs must be sacrificed and the smaller is the probability of success.

6.4 Oxford Protocol

In this protocol the users Alice and Bob have a supply of qubit pairs, each pair being in the pure maximally entangled state (6.6). Because of the noise along the transmission channel, the pairs interact with the environment so they lose their purity. Assume that Alice and Bob are given an ensemble that consists of two subensembles. Each of those subensembles is made of Bell-diagonal states,

$$\rho_{\text{Bell-diag}} = \frac{1}{4} (1 - c_x \sigma_x \tau_x - c_y \sigma_y \tau_y - c_z \sigma_z \tau_z), \quad (6.10)$$

where

$$1 \geq |c_x| \geq |c_y| \geq |c_z| \geq 0, \quad (6.11)$$

the order being a matter of convention. This state is separable if it has a positive partial transpose [19, 32], which is the case if either $|c_x| + |c_y| + |c_z| \leq 1$ or

$c_x c_y c_z \leq 0$. Otherwise, that is: if $|c_x| + |c_y| + |c_z| > 1$ and $c_x c_y c_z > 0$, the state is non-separable and

$$\mathcal{S} = \frac{3}{2} - \frac{1}{2}(|c_x| + |c_y| + |c_z|) \quad (6.12)$$

is its degree of separability [19, 32]. Let Alice and Bob pick two different pairs, one from each subensemble,

$$\begin{aligned} \rho^{(1)} &= \frac{1}{4}(1 + c_x \sigma_x^{(1)} \tau_x^{(1)} - c_y \sigma_y^{(1)} \tau_y^{(1)} + c_z \sigma_z^{(1)} \tau_z^{(1)}), \\ \rho^{(2)} &= \frac{1}{4}(1 + c'_x \sigma_x^{(2)} \tau_x^{(2)} - c'_y \sigma_y^{(2)} \tau_y^{(2)} + c'_z \sigma_z^{(2)} \tau_z^{(2)}), \end{aligned} \quad (6.13)$$

with fidelities

$$\begin{aligned} F_1 &= \text{tr} \left\{ \rho^{(1)} \rho_{\text{ideal}}^{(1)} \right\} = \frac{1}{4}(1 + c_x + c_y + c_z), \\ F_2 &= \text{tr} \left\{ \rho^{(2)} \rho_{\text{ideal}}^{(2)} \right\} = \frac{1}{4}(1 + c'_x + c'_y + c'_z). \end{aligned} \quad (6.14)$$

In the original protocol, Ox₁, Alice and Bob perform the transformation $U_{12x} = e^{i\pi(\sigma_x - \tau_x)/4}$ on all pairs. This operator changes the positions of c_y and c_z in (6.13). Then Alice and Bob perform BCNOT operations on the pairs $\rho^{(1)}$ and $\rho^{(2)}$, followed by measuring the target qubits in the computational basis. For example, they measure the z components of the targets spin, $\sigma_z^{(2)}$ and $\tau_z^{(2)}$. They keep those first pairs for which they get the same measurement results, and discard the others. The target pairs are always consumed in the process. In the alternative protocol, Ox₂, one exploits the order specified in (6.11) and performs BCNOT directly, without first applying U_{12x} . The resulting subensemble of good first pairs is characterized by

$$\rho_{\text{new}} = \frac{1}{4} \left[1 + \frac{c_x c'_x + c_y c'_y}{1 + c_z c'_z} \sigma_x \tau_x - \frac{c_x c'_y + c_y c'_x}{1 + c_z c'_z} \sigma_y \tau_y + \frac{c_z + c'_z}{1 + c_z c'_z} \sigma_z \tau_z \right]. \quad (6.15)$$

This is another Bell-diagonal state.

In the standard description of Ox₁ [53, 8], certain parameters A , B , C , and D play a central role. Their change under Ox₂ is given by

$$\begin{aligned} A &= \left\{ \begin{array}{l} \frac{1}{4}(1 + c_x + c_y + c_z) \\ \frac{1}{4}(1 + c'_x + c'_y + c'_z) \end{array} \right\} \\ &\rightarrow \frac{1}{4N} \left[(1 + c_z)(1 + c'_z) + (c_x + c_y)(c'_x + c'_y) \right], \end{aligned} \quad (6.16)$$

for example, and corresponding expressions apply for B , C , and D . Here $N = \frac{1}{2}(1 + c_z c'_z)$ is the probability that Alice and Bob obtain coinciding outcomes in the measurements of the target pair. If one changes the positions of c_y and c_z and also of c'_y and c'_z in (6.16), one gets the A , B , C and D values for Ox₁.

If the two subensembles in (6.13) are identical, then the protocol works if $F_1 = F_2 > \frac{1}{2}$. In terms of the parameters of (6.13), this means

$$|c_x| + |c_y| + |c_z| > 1. \quad (6.17)$$

So, at every step Alice and Bob must check this property. In particular, they need

$$(|c_x| + |c_y|)^2 - (1 - |c_z|)^2 > 0 \quad (6.18)$$

for the first step to be successful.

If the given ensemble does not obey the ordering required by (6.11), then Alice and Bob use unilateral rotations to bring the state into the wanted form. In fact, it is only necessary to ensure that $|c_z|$ is smaller than $|c_x|$ and $|c_y|$; the relative size of $|c_x|$ and $|c_y|$ does not matter.

6.4.1 Separability and purification

In this section the degree of separability is used as a purification parameter instead of the fidelity. Also, the behavior of the degree of separability under imperfect operations is investigated. Two cases are considered: Binary states and the more general Bell-diagonal states.

1. **Binary state with perfect operations:** In this case,

$$\rho_{\text{bin}} = \frac{1}{4} [1 + \sigma_x \tau_x - (2f - 1) \sigma_y \tau_y + (2f - 1) \sigma_z \tau_z], \quad (6.19)$$

with the initial degree of separability

$$\mathcal{S}_0 = \begin{cases} 1 & \text{for } 0 < f \leq \frac{1}{2}, \\ 2(1 - f) & \text{for } \frac{1}{2} < f < 1. \end{cases} \quad (6.20)$$

Assume that Alice and Bob are given an ensemble of states (6.19), and they are asked to purify this ensemble. They perform the Ox_2 protocol and after one step they get

$$\rho'_{\text{bin}} = \frac{1}{4} \left[1 + \sigma_x \tau_x - \frac{2f - 1}{2f^2 - 2f + 1} \sigma_y \tau_y + \frac{2f - 1}{2f^2 - 2f + 1} \sigma_z \tau_z \right]. \quad (6.21)$$

The corresponding degree of separability is

$$\mathcal{S}_1 = \frac{\mathcal{S}_0^2}{1 + (1 - \mathcal{S}_0)^2}. \quad (6.22)$$

After repeating the protocol n times one gets \mathcal{S}_n as a function of the initial degree of separability \mathcal{S}_0 ,

$$\mathcal{S}_n = \frac{2}{(2/\mathcal{S}_0 - 1)^{2^n} + 1}. \quad (6.23)$$

From this relation it is clear that $\mathcal{S}_n = 1$ if $\mathcal{S}_0 = 1$ and $\mathcal{S}_n \rightarrow 0$ if $\mathcal{S}_0 < 1$.

2. **Binary state with imperfect operations:** In this case the operations are subjected to noise, so that states of two qubit pairs suffer a non-unitary evolution such that [15]

$$\rho_{12} \rightarrow p\rho_{12} + (1-p)\frac{1}{2}\text{tr}_1\{\rho_{12}\}, \quad (6.24)$$

where p is called reliability of the imperfect operation. The limit $p \rightarrow 0$ corresponds to a very noisy channel, while $p \rightarrow 1$ describes a channel with very little noise. For two pairs in the binary state (6.19), the map (6.24) produces

$$\rho_{\text{bin}}^{\text{noise}} = \frac{1}{4} [1 + p\sigma_x\tau_x - p(2f-1)\sigma_y\tau_y + p(2f-1)\sigma_z\tau_z] \quad (6.25)$$

for the “first” pairs. Rather than (6.3) the initial degree of separability is now

$$\mathcal{S}_0 = \frac{1}{2} [3 - p(4f-1)]. \quad (6.26)$$

Further, the ideal BCNOT operation of (6.3) is replaced by $\text{BCNOT}_{\text{noise}}$,

$$\text{BCNOT}_{\text{noise}}(\cdot) = p^2 \text{BCNOT}(\cdot) + \frac{1-p^2}{16}, \quad (6.27)$$

where (\cdot) is $\rho^{(1)}\rho^{(2)}$. Alice and Bob perform the Ox_2 protocol, and after the measurement of the target qubits and discarding of the “bad” first pairs they obtain

$$\begin{aligned} \rho = & \frac{1}{4} \left[1 + p^2 \frac{2f^2 - 2f + 1}{1 - 2p^2 f(1-f)} \sigma_x \tau_x - p^2 \frac{2f-1}{1 - 2p^2 f(1-f)} \sigma_y \tau_y \right. \\ & \left. + p^2 \frac{2f-1}{1 - 2p^2 f(1-f)} \sigma_z \tau_z \right], \end{aligned} \quad (6.28)$$

for the “good” first pairs. The new degree of separability is

$$\mathcal{S}_{\text{new}} = \frac{1}{2} \left[3 - p^2 \frac{2f^2 + 2f - 1}{1 - 2p^2 f(1-f)} \right]. \quad (6.29)$$

3. **Bell-diagonal state:** Now consider the ensemble (6.13) consisting of Bell-diagonal states. In this case the initial degrees of separability are given by

$$\begin{aligned} \mathcal{S}_0 &= \frac{3}{2} - \frac{1}{2} (|c_x| + |c_y| + |c_z|), \\ \mathcal{S}'_0 &= \frac{3}{2} - \frac{1}{2} (|c'_x| + |c'_y| + |c'_z|). \end{aligned} \quad (6.30)$$

Alice and Bob perform the Ox_2 protocol, and after one step they get

$$\mathcal{S}_1 = \frac{3}{2} - \frac{1}{2N} [(|c_x| + |c_y|)(|c'_x| + |c'_y|) + |c_z| + |c'_z|] \quad (6.31)$$

for the “good” first pairs with N as in (6.16), or in the presence of noise,

$$N_{\text{noise}} = \frac{1}{4p^2} [1 + p^2(1 + 2|c_z c'_z|)]. \quad (6.32)$$

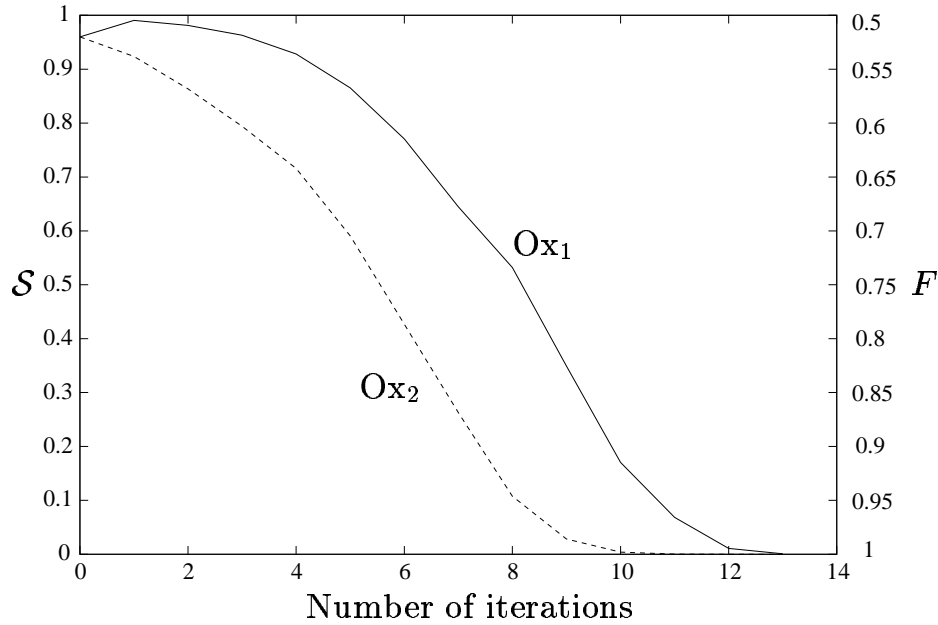


Figure 6.1: The degree of separability \mathcal{S} and fidelity F for the two variants of the Oxford protocol. Solid line: original protocol Ox_1 ; dashed line: alternative protocol Ox_2 .

6.4.2 Discussion

In Figure 6.1, the separability \mathcal{S} and the fidelity F are plotted as a function of the number of iterations, both for the original protocol Ox_1 and for the alternative protocol, Ox_2 , where one enforces the ordering of (6.11) in each step. The figure refers to the initial values $(c_x, c_y, c_z) = (0.16, 0.08, 0.84)$ for which $F = 0.52$ is the initial fidelity and $2F + \mathcal{S} = 2$ holds for all iterations.

In this case Alice and Bob use the bilateral rotations to rearrange these three numbers such that $(c_x, c_y, c_z) = (0.84, 0.16, 0.08)$. The figure clearly shows that for Ox_2 , the fidelity reaches unity much faster than that for Ox_1 . Moreover, for Ox_1 the fidelity decreases and then increases [56], but for Ox_2 it increases in each iteration.

The importance of (6.11) is particularly apparent when one treats the binary state (6.19), for which two of the A, B, C, D parameters of [53, 8] are positive and the other two vanish. To perform Ox_1 successfully, one needs $A, C > 0$ and $B = D = 0$; then Ox_1 works and the fidelity increases monotonically. But if one enforces (6.11), Ox_2 works directly, and one does not have to worry which of the four parameters are non-zero.

In Figure 6.2, Ox_1 and Ox_2 are performed in the presence of noise. The importance of the property (6.11) is clear: the degree of separability becomes constant faster for Ox_2 than for Ox_1 .

The log-log plot of Figure 6.3 shows the number of initial pairs needed to

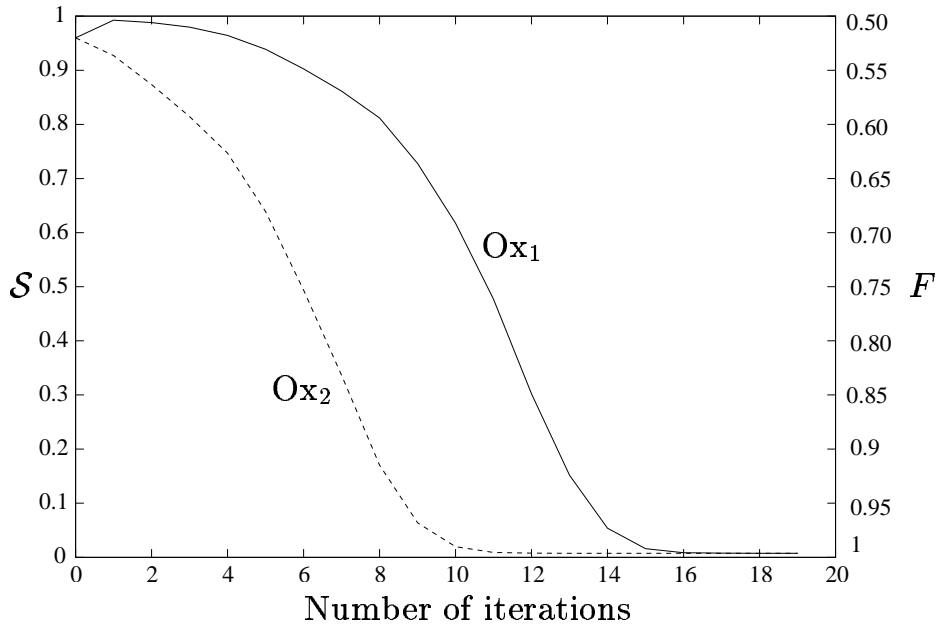


Figure 6.2: Like Figure.1, but with noise of strength $p = 0.994$.

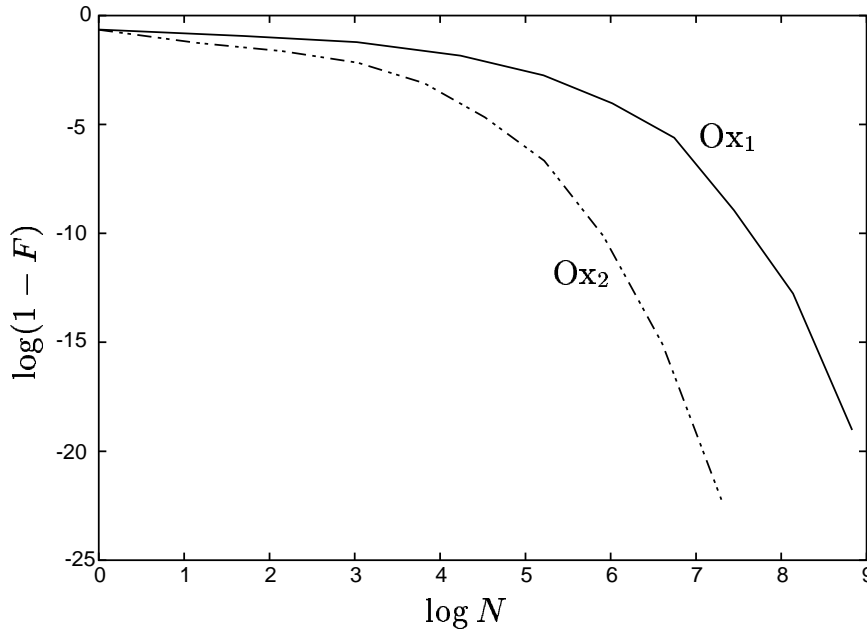


Figure 6.3: Number N of pairs needed to create one pair with fidelity F , displayed as $\log(1 - F)$ vs. $\log N$. The initial state of the pairs has fidelity $F_0 = 0.62$.

create one pair with fidelity F . We see that Ox_2 uses up less qubit pairs than Ox_1 . In addition, Ox_2 needs fewer iterations, so that both advantages taken together make Ox_2 much more efficient than Ox_1 .

In summary, in this chapter an alternative form of the IBM and Oxford pro-

ocols are described for Bell-diagonal states. In the alternative version of the Oxford protocol Ox_1 , the final fidelity is obtained as a function of three numbers, c_x , c_y and c_z . The improvement over the original Oxford protocol is due to the arrangement of these three numbers in decreasing order. The parameter of the degree of separability is considered as a purification parameter. As the number of iterations increases, the degree of separability decreases.

Chapter 7

Summary

The aim of this dissertation is to study the kinematics of 2-qubit pairs. A 2-qubit state is specified by the Bloch vectors for each qubit and a 3×3 dyadic, representing the expectation values of the joint observables. In what follows the main results are listed.

- The behaviour of a 2-qubit state under a local transformation is investigated, where we obtain a set of 9 quantities, constructed from the Bloch vectors and the cross dyadic, which are invariant under local transformation. We establish a generic form for a 2-qubit state, which helps us decide if given two 2-qubit states belong to the same family or not. Using this form, which depends on the characteristic values of the cross dyadic, one can distinguish between all two-qubit families, where we obtain six classes of families of locally equivalent states. Those families classify all 2-qubit states, four of them consist of two subclasses each.
- A simple criterion is obtained to check if a 2-qubit state is separable or not. This criterion does not depend on the eigenvalues of the partial transposition of the state in question but only on three numbers, those are the coefficients of the eigenvalue equation. These numbers are written as a function of the Bloch vectors and the cross dyadic. Also using the characteristic values of the cross dyadic, one can decide if the CHSH inequality is obeyed or violated.
- The properties of Lewenstein-Sanpera decompositions are employed to split a given state into its optimal separable and pure parts. The degree of separability is an important part in this decomposition, where a state is more useful for quantum information purposes, the smaller its degree of separability. The optimal degree of separability is obtained analytically for some important cases as a function of the Bloch vectors and the cross dyadic of the state in question: For the simple Werner state, where our result

coincides with that obtained numerically. Also for the self-transposed states, the generalized for Werner states and rank-2 states.

- The technique of the rank-2 case is employed to study the case of rank-3 and the full rank, where we obtain all possible decompositions. Among them, we choose the one which has the largest splitting parameter. In this situation a numerical procedure could help in obtaining the optimal decomposition. Given a density matrix, one obtains its eigenvalues and corresponding eigenvectors. Using the rank-2 method to obtain all the possible decompositions, then choose the one corresponding to the largest degree of separability. If this decomposition is the optimal one, a technique is used to check the optimality. If it is not optimal, an optimization procedure is performed.
- There is an important relation between the degree of separability \mathcal{S} and what is the so called *concurrence* \mathcal{C} which appears in the definition of the entanglement of formation. In general, the sum of the degree of separability and the concurrence is less than one, but equal to one for states with vanishing Bloch vectors. On the other hand both of them run from 0 to 1.
- A criterion is introduced to decide if a given decomposition is the optimal one or not. Two inequalities are obeyed if the decomposition in question is the optimal one and are violated if it is not.
- The effect of the unitary operators and BCNOT operations are described on the dynamical variables. An alternative presentation of the IBM and Oxford purification protocols is obtained by using these variables. One could introduce the degree of separability as a purification parameter, where the purified state has a smaller degree of separability than the initial one. Employing the properties of the characteristic values of the cross dyadic, makes the Oxford protocol much faster.

Appendixes

Appendix A

Some separability criteria

For **pure states**, there is a very simple necessary and sufficient criterion for separability, the *Schmidt decomposition*. A pure state has Schmidt rank $r \leq M$ if it can be decomposed as the bi-orthogonal sum

$$|\psi^r\rangle = \sum_{i=1}^r a_i |e_i\rangle |f_i\rangle \quad (\text{A.1})$$

where $a_i > 0$, $\sum_{i=0}^r a_i^2 = 1$ and $\langle e_i | e_j \rangle = \delta_{ij} = \langle f_i | f_j \rangle$. These a_i are the eigenvalues of the reduced density matrices. A given pure state $|\psi\rangle$ is separable iff $r = 1$ [39]. For **mixed states** the situation is less simple, there are several separability criteria for this case. In the following sections, some of them are described.

A.1 Bell inequalities

One can say that Bell's inequalities are the first separability criterion. Bell used them to evaluate the power of local-hidden-variables theories in describing local measurement outcomes on quantum mechanical systems. These inequalities are obeyed by any local-hidden-variables theory. So, they must be obeyed by all separable states and are surely violated by some non-separable states. Thus the violation of Bell inequalities is a manifestation of quantum entanglement. A state ρ is said to satisfy these Bell inequalities if, for any choice of operators A_i, A'_i in the Hilbert space \mathcal{H}_i ($i = 1, 2$) with $-1 \leq A_i, A'_i \leq 1$, we have

$$\text{tr} \{ \rho [A_1 \cdot (A_2 + A'_2) + A'_1 \cdot (A_2 - A'_2)] \} \leq 2. \quad (\text{A.2})$$

This kind of Bell inequalities is called Clauser-Horne-Shimony-Holt (CHSH) inequality [35].

Werner first pointed out that separable states must satisfy all possible Bell inequalities [41]. It has been shown by Gisin [36], that any entangled pure state of

two spin $-\frac{1}{2}$ particles violates a Bell inequality of the CHSH type. This result was extended to pairs of systems of arbitrary dimension [57]. Popescu and Rohrlich [37] have extended this result further to any number of systems. They showed that although any entangled pure state of two systems violates the CHSH inequality, the same is not true for mixtures of entangled states. There are some classes of mixed entangled states which do not violate any of Bell's inequalities. As an example, the two spin- $\frac{1}{2}$ in a mixture of entangled states $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, with equal probability, which does not violate Bell's inequality.

A.2 Rení inequalities

Another approach originated by Schrödinger is the observation that an entangled states gives more information about the total system than about the subsystems. This gives rise to a series of entropic inequalities of the form

$$S(\rho_A) \leq S(\rho), \quad S(\rho_B) \leq S(\rho), \quad (\text{A.3})$$

where $\rho_A = \text{tr}_B \{\rho\}$ and similarly for ρ_B . The above inequalities were proven in [45, 46, 47, 48, 60] to be satisfied by separable states for four different “entropies” being particular cases of the so-called Rení quantum entropy $S_\alpha = (1 - \alpha)^{-1} \log \text{tr} \{\rho^\alpha\}$, for which

$$\begin{aligned} S_0 &= \log R(\rho), & S_1 &= -\text{tr} \{\rho \log \rho\} \\ S_2 &= -\text{tr} \{\rho^2\}, & S_\infty &= -\log \|\rho\|, \end{aligned} \quad (\text{A.4})$$

are particular examples. Here, $\|\rho\|$ is the largest eigenvalue of ρ and $R(\rho)$ is its rank. The violation of these inequalities is a manifestation of some non-classical feature of a compound system resulting from its inseparability.

A.3 The reduction criterion

Horodeccy [24] gave a general necessary and sufficient condition for the separability in arbitrary dimensions. It states that ρ is separable if and only if the tensor product of any positive map acting on the subsystem A and the identity acting on the subsystem B maps ρ into a positive map, see Section 1.4. This criterion is hard to use, because it involves the characterization of the set of all positive maps. Cerf *et al.* [59], and M., P. Horodeccy [60] independently, introduced a map $\Gamma : \rho \rightarrow \text{tr}_A \{\rho_{AB}\} - \rho_{AB}$, which gives rise to a simple necessary condition for separability in arbitrary dimensions. According to the reduction criterion, state ρ is separable iff:

$$I_A \otimes \rho_B - \rho_{AB} \geq 0 \text{ and } \rho_A \otimes I_B - \rho_{AB} \geq 0, \quad (\text{A.5})$$

where ρ_A is Alice's reduced density operator, and ρ_B is Bob's. As an example consider the arbitrary state of a two-dimensional quantum system $\rho = \frac{1}{2}(1 + \vec{r} \cdot \sigma^\downarrow)$. The map Γ transforms it to $\frac{1}{2}(1 - \vec{r} \cdot \sigma^\downarrow)$. This means that Γ performs a spin flip, a partial transposition. This criterion is simply equivalent to the Peres-Horodeccy criterion for $2 \times n$ composite systems. It is also sufficient for a 2×2 and 2×3 systems. In higher dimensions the reduction criterion is weaker than the Peres-Horodeccy criterion. The advantage of the reduction criterion is that all states violating it can be distilled; see [58] for a recent review.

A.4 Positive partial transpose

For high-dimensional states, the Peres-Horodeccy criterion is only necessary. P. Horodecki [26] has constructed some classes of families of inseparable states with positive partial transposes for 3×3 and 2×4 systems. States of this kind are said to possess bound entanglement (BE).

States supported on $\mathcal{C}^2 \otimes \mathcal{C}^N$ whose partial transposes are positive operators have been investigated by Kraus *et al.* [61]. It has been shown that if the rank $r(\rho) = N$ then ρ is separable and that bound-entangled states have ranks larger than N . Also they introduced a separability criterion for a generic density operator such that $r(\rho^{\text{T}_A}) + r(\rho) \leq 3N$. The previous results have been generalized in [68] to the case of $M \times N$ systems, where $M \leq N$. They showed that any state with $r(\rho) \leq N$ is separable if its partial transpose is positive. Also the generic PPT density matrices with $r(\rho) + r(\rho^{\text{T}_A}) \leq 2MN - M - N + 2$ are separable. All these results are summarized in [62].

A.5 Volume of separable states

The question of the volume of the set of separable or entangled states in the set of all states has been investigated by Życzkowski *et al.* [63]. They have shown that the volume of the set of separable states is non-zero independently of the dimension of the Hilbert space and the number of systems composing it. This means that all states in a sufficiently small neighbourhood of the chaotic state $\rho = 1/N$ are necessarily separable. To show this property, one considers a ball round the chaotic state: one needs a number $p_0 > 0$ such that for any state $\tilde{\rho}$ the state

$$\rho = (1 - p)\frac{1}{N} + p\tilde{\rho} \quad (\text{A.6})$$

is separable for all $0 < p \leq p_0$, where N is the dimension of the total system. In [63] a sufficient condition for separability is given: if the eigenvalues of a given state do not differ too much from the uniform spectrum of the chaotic state, then the state must be separable. Consider for example, 2×2 systems: here one can provide the largest possible p_0 , as there exists the necessary and

sufficient condition for separability, PPT. Assume that the eigenvalues of the partial transposition of (A.6) are given by

$$\lambda_i = \frac{1-p}{N} + p\tilde{\lambda}_i \quad (\text{A.7})$$

where λ_i and $\tilde{\lambda}$ are the eigenvalues of $\rho^{\text{T}B}$ and $\tilde{\rho}^{\text{T}B}$ respectively. The spectrum of the partially transposed density operator must belong to the interval $[-\frac{1}{2}, 1]$. Then if $\frac{1-p}{N} - \frac{p}{2} \geq 0$, then the eigenvalues λ_i are non-negative for arbitrary $\tilde{\rho}$. So, for 2×2 systems one can take $p_0 = \frac{1}{3}$ to obtain a sufficient condition for separability. In case of n -partite systems, each of dimension d , the value of $p_0 = (1 + \frac{2}{d})^{(1-n)}$ [64, 25].

Appendix B

Some entanglement measures

The existence of nonclassical correlations, entanglement, between parts of a composite quantum system is at the heart of the quantum information. Some efforts have been made on the problem of how to define and quantify the entanglement of a given state in a physically meaningful way. There are some conditions that every measure of entanglement has to satisfy. The measure should be zero for separable states, invariant under local unitary transformations, and its expected value cannot increase under local general measurements and classical communications [51, 52]. In the following, some of the most popular entanglement measures for pure and mixed states are noted for the record.

B.1 Measures for pure states

For any bipartite system in a pure state, Bennett *et al.* [11, 10] defined the entanglement of the system as the von-Neumann entropy of either one of its two parts. That is for a pure state $|\psi\rangle$ in a Hilbert space $\mathcal{H}_A \cdot \mathcal{H}_B$ belonging to two parties, Alice and Bob,

$$E = S(\text{tr}_A \{|\psi\rangle\langle\psi|\}) = S(\text{tr}_B \{|\psi\rangle\langle\psi|\}) \quad (\text{B.1})$$

where S is the von Neumann entropy of the density operator [39]. It is given by $S(\rho) = -\text{tr} \{\rho \log \rho\}$. This measure E is unique and it ranges from zero for product (separable) states, to $\log_2 N$ for the chaotic state of two N state particles. $E = 1$ obtains for the Bell state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$, for example.

B.2 Measures for mixed states

For mixed states, entanglement is more complicated and less well understood than that of pure-state entanglement. There is no single parameter completely characterizing mixed state entanglement the way E does for pure states. There

are several proposed measures of entanglement of mixed states. In the following sections, some of the more important measures are reviewed briefly.

B.2.1 Entanglement of formation

It describes the minimal amount of shared pure entanglement in order to create the given mixed entangled state using only local quantum operations and classical communication. It is defined as:

$$E_f = \min \sum_i p_i S(\rho_A^i) \quad (\text{B.2})$$

where $S(\rho_A^i)$ is the von Neumann entropy again. The minimum is taken over all possible realizations of the state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with $\rho_A^i = \text{tr}_B \{|\psi_i\rangle\langle\psi_i|\}$. The entanglement of formation is zero if and only if the state in question could be expressed as a mixture of product states. It reduces to the von Neumann entropy for pure states.

A nice feature of the entanglement of formation is that it could be calculated analytically for a system of two spin- $\frac{1}{2}$ particles. Hill and Wootters [21] derived an analytical formula for all density matrices of two qubits having only non-zero eigenvalues. The entanglement of a pure state $|\psi\rangle$ is

$$E(\psi) = F(\mathcal{C}(\psi)), \quad (\text{B.3})$$

where \mathcal{C} is the *concurrence* of $|\psi\rangle\langle\psi|$,

$$F(\mathcal{C}) = H\left(\frac{1 + \sqrt{1 - \mathcal{C}^2}}{2}\right), \quad (\text{B.4})$$

with $H(x) = -x \log x - (1 - x) \log(1 - x)$. In [21, 22], this formula has been extended to arbitrary states of two qubits, where in this case the concurrence is given by (1.23). Bennett *et al.* [10] evaluated analytically the entanglement of formation for a mixture of Bell states.

B.2.2 Entanglement of distillation:

It measures the amount of pure entanglement that can be extracted from a state ρ , using only local quantum operations and classical communications. It is of central importance in the theory of bipartite entanglement, see [21, 22]. It has been shown by Horodeccy [70] that all non-separable two qubit states are distillable.

Definition: A density operator ρ is distillable, i.e., $D(\rho) > 0$, if and only if there exists an n such that

$$\text{tr} \{ |\psi\rangle\langle\psi| (\rho^{\otimes n})^T \} < 0 \quad \text{for any } |\psi\rangle \in \mathcal{H}_a \cdot \mathcal{H}_B.$$

States which violate the Peres-Horodeccy criterion are distillable [70, 71]. There exists a class of bipartite density matrices for which it is known that even though a state ρ in this class is not separable, the distillable entanglement vanishes, $D(\rho) = 0$ [10]. This class of states is characterized by the fact that the states do not violate the Peres-Horodeccy criterion, i.e., $\rho^{\text{T}_1} \geq 0$. These kind of states are called bound entangled, BE, states. It has been recently conjectured [65, 66] that there exist states with non-positive partial transpose that are non-distillable. For pure states the two measurements, entanglement of formation and entanglement of distillation, are equal, but for mixed states entanglement of distillation is less than the entanglement of formation. This means that one cannot distill more entanglement out of a state than was used in preparing it.

Appendix C

Infinitesimal changes

C.1 Werner state

invariant	1 st order	2 nd order
s^2	0	$\delta_1 \vec{s} \cdot \delta_1 s^\downarrow$
t^2	0	$\delta_1 \vec{t} \cdot \delta_1 t^\downarrow$
$\vec{s} \cdot \vec{C} \cdot t^\downarrow$	0	$\delta_1 \vec{s} \cdot \vec{C} \cdot \delta_1 t^\downarrow$
$\vec{s} \cdot \vec{C}_{\text{sub}} \cdot t^\downarrow$	0	$\delta_1 \vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta_1 t^\downarrow$
$\vec{s} \cdot \vec{C} \cdot \vec{C}^T \cdot s^\downarrow$	0	$\delta_1 \vec{s} \cdot \vec{C} \cdot \vec{C}^T \cdot \delta_1 s^\downarrow$
$\vec{t} \cdot \vec{C}^T \cdot \vec{C} \cdot t^\downarrow$	0	$\delta_1 \vec{t} \cdot \vec{C}^T \cdot \vec{C} \cdot \delta_1 t^\downarrow$
$\text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \right\}$	$2 \text{Sp} \left\{ \vec{C}^T \cdot \delta_1 \vec{C} \right\}$	$2 \text{Sp} \left\{ \vec{C}^T \cdot \delta_2 \vec{C} \right\}$ + $\text{Sp} \left\{ \delta_1 \vec{C}^T \cdot \delta_1 \vec{C} \right\}$
$\text{Sp} \left\{ \left(\vec{C}^T \cdot \vec{C} \right)^2 \right\}$	$4 \text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \cdot \vec{C}^T \cdot \delta_1 \vec{C} \right\}$	$4 \text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \cdot \vec{C}^T \cdot \delta_2 \vec{C} \right\}$ + $2 \text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \cdot \delta_1 \vec{C}^T \cdot \delta_1 \vec{C} \right\}$ + $2 \text{Sp} \left\{ \vec{C} \cdot \vec{C}^T \cdot \delta_1 \vec{C} \cdot \delta_1 \vec{C}^T \right\}$ + $2 \text{Sp} \left\{ \left(\vec{C}^T \cdot \delta_1 \vec{C} \right)^2 \right\}$
$\det \left\{ \vec{C} \right\}$	$\text{Sp} \left\{ \delta_1 \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$	$\text{Sp} \left\{ \delta_2 \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$ + $\text{Sp} \left\{ \vec{C}^T \cdot \delta_1 \vec{C}_{\text{sub}} \right\}$
$\det \left\{ \vec{E} \right\}$	$\text{Sp} \left\{ \delta_1 \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$	$\text{Sp} \left\{ \delta_2 \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$ + $\text{Sp} \left\{ \vec{C}^T \cdot \delta_1 \vec{C}_{\text{sub}} \right\}$ - $\delta_1 \vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta_1 t^\downarrow$

C.2 2-qubit state

invariant	1 st order	2 nd order
s^2	$2\vec{s} \cdot \delta s^\downarrow$	$\delta\vec{s} \cdot \delta s^\downarrow$
t^2	$2\vec{t} \cdot \delta t^\downarrow$	$\delta\vec{t} \cdot \delta t^\downarrow$
$\vec{s} \cdot \vec{C} \cdot t^\downarrow$	$\delta\vec{s} \cdot \vec{C} \cdot t^\downarrow + \vec{s} \cdot \vec{C} \cdot \delta t^\downarrow$ $+ \vec{s} \cdot \delta \vec{C} \cdot t^\downarrow$	$\delta\vec{s} \cdot \vec{C} \cdot \delta t^\downarrow$ $+ \delta\vec{s} \cdot \delta \vec{C} \cdot t^\downarrow + \vec{s} \cdot \delta \vec{C} \cdot \delta t^\downarrow$
$\vec{s} \cdot \vec{C}_{\text{sub}} \cdot t^\downarrow$	$\delta\vec{s} \cdot \vec{C}_{\text{sub}} \cdot t^\downarrow$ $+ \vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta t^\downarrow$ $- s^\downarrow \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot t^\downarrow$	$\delta\vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta t^\downarrow + \vec{s} \cdot \delta \vec{C}_{\text{sub}} \cdot t^\downarrow$ $- \delta\vec{s} \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot t^\downarrow$ $- \vec{s} \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot \delta t^\downarrow$
$\vec{s} \cdot \vec{C} \cdot \vec{C}^T \cdot s^\downarrow$	$2\vec{s} \cdot \vec{C} \cdot \vec{C}^T \cdot \delta s^\downarrow$ $+ 2\vec{s} \cdot \delta \vec{C} \cdot \vec{C}^T \cdot s^\downarrow$	$\delta\vec{s} \cdot \vec{C} \cdot \vec{C}^T \cdot \delta s^\downarrow$ $+ 2\vec{s} \cdot \delta \vec{C} \cdot \vec{C}^T \cdot \delta s^\downarrow$ $+ 2\vec{s} \cdot \vec{C} \cdot \delta \vec{C}^T \cdot \delta s^\downarrow$ $+ \vec{s} \cdot \delta \vec{C} \cdot \delta \vec{C}^T \cdot s^\downarrow$
$\vec{t} \cdot \vec{C}^T \cdot \vec{C} \cdot t^\downarrow$	$2\vec{t} \cdot \vec{C}^T \cdot \vec{C} \cdot \delta t^\downarrow$ $+ 2\vec{t} \cdot \vec{C}^T \cdot \delta \vec{C} \cdot t^\downarrow$	$\delta\vec{t} \cdot \vec{C}^T \cdot \vec{C} \cdot \delta t^\downarrow$ $+ 2\vec{t} \cdot \delta \vec{C}^T \cdot \vec{C} \cdot \delta t^\downarrow$ $+ 2\vec{t} \cdot \vec{C}^T \cdot \delta \vec{C} \cdot \delta t^\downarrow$ $+ \vec{t} \cdot \delta \vec{C}^T \cdot \delta \vec{C} \cdot t^\downarrow$
$\text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \right\}$	$2 \text{Sp} \left\{ \vec{C}^T \cdot \delta \vec{C} \right\}$	$\text{Sp} \left\{ \delta \vec{C}^T \cdot \delta \vec{C} \right\}$
$\text{Sp} \left\{ \left(\vec{C}^T \cdot \vec{C} \right)^2 \right\}$	$4 \text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \cdot \vec{C}^T \cdot \delta \vec{C} \right\}$	$2 \text{Sp} \left\{ \vec{C}^T \cdot \vec{C} \cdot \delta \vec{C}^T \cdot \delta \vec{C} \right\}$ $+ 2 \text{Sp} \left\{ \vec{C} \cdot \vec{C}^T \cdot \delta \vec{C} \cdot \delta \vec{C}^T \right\}$ $+ 2 \text{Sp} \left\{ \left(\vec{C}^T \cdot \delta \vec{C} \right)^2 \right\}$
$\det \left\{ \vec{C} \right\}$	$\text{Sp} \left\{ \delta \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$	$\text{Sp} \left\{ \vec{C}^T \cdot \delta \vec{C}_{\text{sub}} \right\}$
$\det \left\{ \vec{E} \right\}$	$\text{Sp} \left\{ \delta \vec{C}^T \cdot \vec{C}_{\text{sub}} \right\}$ $+ \vec{s} \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot t^\downarrow$ $- \delta\vec{s} \cdot \vec{C}_{\text{sub}} \cdot t^\downarrow$ $- \vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta t^\downarrow$	$\text{Sp} \left\{ \vec{C}^T \cdot \delta \vec{C}_{\text{sub}} \right\}$ $+ \delta\vec{s} \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot t^\downarrow$ $+ \vec{s} \cdot \left\{ \delta \vec{C}, \vec{C} \right\} \cdot \delta t^\downarrow$ $- \delta\vec{s} \cdot \vec{C}_{\text{sub}} \cdot \delta t^\downarrow - \vec{s} \cdot \delta \vec{C}_{\text{sub}} \cdot t^\downarrow$

Note that $\delta \vec{C}_{\text{sub}}$ consists of the sub-determinants of $\delta \vec{C}$ and is 2nd order in $\delta \vec{C}$.

Bibliography

- [1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature **390**, 575(1997).
- [3] D. Boschi, S. Bronce, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **90**, 1211 (1998).
- [4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 281 (1992).
- [5] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
- [6] C. H. Bennett, G. Brassard, and N. D. Meria, Phys. Rev. Lett. **68**, 559 (1992).
- [7] D. Deutsch, Proc. R. Soc. London A, **425**, 73 (1998).
- [8] D. Bouwmeester, A. Ekert, and A. Zeilinger “*The physics of quantum information*” (Springer 2000).
- [9] H. -K. Lo, S. Popescu, and T. Spiller “*Introduction to quantum Computation and information*” (World Scientific 1998).
- [10] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [11] C. H. Bennett, D. P. Di Vincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [12] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [13] N. Gisin, Phys. Lett. **A210**, 151 (1996).
- [14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

-
- [15] H. -J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
- [16] P. D. D. Schwindt, P. G. Kwiat, and B. -G. Englert, Phys. Rev. A **60**, 4285 (1999).
- [17] B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. A **63**, 032303 (2001).
- [18] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, LANL eprint quant-ph/0101066 (2001).
- [19] B.-G. Englert and N. Metwally, J. Mod. Opt. **47**, 221 (2000).
- [20] B.-G. Englert and N. Metwally, Appl. Phys B **72**, 35 (2001).
- [21] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
- [22] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
- [23] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [24] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. **A222**, 1 (1996)
- [25] M. Horodecki, P. Horodecki and R. Horodecki, LANL eprint quant-ph/0109124 (2001).
- [26] P. Horodecki, Phys. Lett. **A232**, 333 (1997).
- [27] W. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).
- [28] U. Fano, Rev. Mod. Phys. **55**, 8559 (1983).
- [29] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).
- [30] H. Lutkephol, “*Handbook of Matrices*” (John Wiley and Sons 1996).
- [31] J. Gilbert and L. Gilbert “*Linear Algebra matrix theory*” (Academic Press 1995).
- [32] B.-G. Englert and N. Metwally, “*Kinematics of qubit pairs*” in “*Mathematics of Quantum Computation*”, edited by R. Bryinski, and G. Chen, (CRC publisher 2002).
- [33] Y. Makhlin, LANL quant-ph/0002045 (2000).
- [34] M. Grassl, N. Rötteler, and T. Beth, Phys. Rev. A **58**, 1833 (1998).
- [35] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

-
- [36] N. Gisin, Phys. Lett. **A154**, 201 (1991).
- [37] S. Popescu and D. Rohrlich, Phys. Lett. **A166**, 293 (1992).
- [38] Leslie E. Ballentine, “Quantum Mechanics” (Prentice Hall 1990).
- [39] A. Peres “*Quantum theory: Concepts and methods*”, (Kluwer 1993).
- [40] D. V. Michael “*Quantum chance and non-locality: Probability and non-locality of quantum mechanics*” (Cambridge University Press 1998).
- [41] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [42] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
- [43] S. Karnas and M. Lewenstein, J. Phys A **34**, 6919 (2001).
- [44] T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001).
- [45] R. Horodecki and P. Horodecki, Phys. Lett. **A194**, 147 (1994).
- [46] R. Horodecki and M. Horodecki. Phys. Rev. A **54**, 1838 (1996).
- [47] R. Horodecki P. Horodecki, and M. Horodecki, Phys. Lett. **A210**, 377 (1996).
- [48] B. M. Terhal, LANL eprint quant-ph/0101032 (2001).
- [49] S. Karnas and M. Lewenstein, Phys. Rev. A **64**, 042313 (2001).
- [50] J. Eisert and H.-J. Briegel, Phys. Rev. A **64**, 022306 (2000).
- [51] V. Vedral and M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
- [52] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
- [53] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [54] G. Giedke, H. -J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).
- [55] N. Metwally, LANL eprint quant-ph/0109051 (2001).
- [56] C. Macchiavello, Phys. Lett. **A246**, 385 (1998).
- [57] N. Gisin and A. Peres, Phys. Lett. **A162**, 15 (1992).

- [58] M. Horodecki, P. Horodecki, and R. Horodecki, LANL eprint quant-ph/0109124. The article is part of a book entitled *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*, edited by G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, published in *Springer Tracts in Modern Physics*, (2001).
- [59] N. J. Cerf, C. Adami, and R. M. Gingrich, *Phys. Rev. A* **60**, 898 (1999).
- [60] M. Horodecki and P. Horodecki, *Phys. Rev. A* **54**, 2406 (1999).
- [61] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, *Phys. Rev. A* **61**, 062302 (2000).
- [62] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, *J. Mod. Opt.* **47** 2481 (2000).
- [63] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, *Phys. Rev. A* **58**, 883 (1998).
- [64] G. Vidal and R. Tarrach, *Phys. Rev. A* **59**, 141 (1999).
- [65] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, *Phys. Rev. A* **61**, 062313 (2000).
- [66] D. P. DiVincenzo, P. Shor, J. Smolin, B. Terhal, and A. Thapliyal, *Phys. Rev. A* **61**, 062312 (2000).
- [67] G. Ghirardi, L. Marinatto, T. Weber, LANL eprint quant-ph/0109017 (2001).
- [68] P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, *Phys. Rev. A* **62**, 032310 (2000).
- [69] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett.* **A383**, 1 (2001).
- [70] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997).
- [71] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **80**, 5239 (1998).

Acknowledgements

In the first place I would like to express my deep gratitude and sincere appreciation to my supervisor Prof. Dr. B.-G. Englert not only for introducing me to this field, but also for teaching me step by step. I am indebted to him for his patience, encouragement and for all the time he gives me. I am very pleased to thank Prof. Dr. Axel Schenzle for the motivating atmosphere at his group. My deepest thanks to Dr. H.-J. Briegel for his important discussions and encouragement. I am very grateful to Prof. Dr. A. Kihder, the head of Mathematics department, Aswan, for his kindly encouragement. I am indebted to Prof. Dr. Obada, the head of mathematics department, Al-Azhar university, who teach me the fundamental of the quantum mechanics. Warm thanks to Mr. Hans Aschauer for more discussions and for his kind cooperation. Special thanks to Dr. Sigmund Stintzing, Dr. Ulrich Martini and Dr. Claus Beisbart for their kindly help. My thanks to all my colleagues in the theoretical physics department at the LMU. I would like to express my appreciation to the Egyptian Embassy for the scholarship during this dissertation. Finally I wish to thank my family who provides the proper conditions to finish this study.

Curriculum Vitae

Personal details

Name: Nasser Metwally.

Date of birth: 31-12-1965.

Place of birth: Aswan, Egypt.

Nationality: Egyptian

Single/Married: Married.

Children: Two.

Education

1980-1983 Secondary school.

1983 Abitur *Mathematics and physics.*

1984-1987 Faculty of Science, Aswan, Assuit University.

B. Sc. Mathematics.

1989-1990 Faculty of Science, Aswan Assuit University.

Preliminary Courses of M. Sc.

1990-1994 Faculty of Science, Aswan, Assuit University.

*M. Sc. : Classical treatment of Atomic Hydrogen
in Electromagnetic field.*

1998-2002 Scholarship from the Egyptian Embassy, this *Dissertation.*

Employments

1989-1994 Faculty of Science, Aswan, Assuit University.

Demonstrator in Mathematics department.

1995-1997 Faculty of Science, Aswan, South Valley University.

Assistant lecturer in Mathematics department.